Description of document:	Board of Governors of The Federal Reserve System notes, memos, correspondence, and other materials concerning the Federal Reserve OIG audit report: 2015-MO-B-006 March 31, 2015, entitled: The Board Can Enhance Its Diversity and Inclusion Efforts, exclusive of the audit report itself
Requested date:	31-May-2017
Release date:	10-July-2020
Posted date:	09-November-2020
Source of document:	Information Disclosure Section Board of Governors of the Federal Reserve System 20th & Constitution Avenue, NW, Washington, DC 20551 Fax: (202) 872-7565 Electronic Request Form

BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

ADDRESS OFFICIAL CORRESPONDENCE
TO THE BOARD

July 10, 2020

Re: Freedom of Information Act Request No. F-2017-00188

This is in response to your email message dated and received by the Board's Information Disclosure Section on May 31, 2017. Pursuant to the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, you seek:

> [a] copy of all notes, memos, correspondence, and other materials concerning the Federal Reserve OIG audit report: 2015-MO-B-006 March 31, 2015, entitled: The Board Can Enhance Its Diversity and Inclusion Efforts. [You are] not requesting a copy of the audit report itself, since that document is posted online.

Staff searched Board records and located information responsive to your request. I have determined, however, that certain portions of the responsive information consists of non-public proprietary materials of a consultant (e.g., vendor reports and presentation materials for Board diversity efforts); internal pre-decisional deliberations and recommendations (e.g., memoranda, presentations, and the deliberative portions of staff emails); and personally identifiable information (e.g., staff performance reviews, promotions records, and compensation information). This information is subject to withholding and will be withheld pursuant to exemptions 4, 5, and 6 of the FOIA, 5 U.S.C. §§ 552(b)(4), (b)(5), and (b)(6), respectively. I have also determined that the information should be withheld because it is reasonably foreseeable that disclosure would harm an interest protected by an exemption described in subsection (b) of the FOIA, 5 U.S.C. § 552(b). The responsive documents have been reviewed under the requirements of subsection (b) and all reasonably segregable nonexempt information will be provided to you. The documents being provided to you will indicate the amount of information that has been withheld and the applicable exemptions. Approximately 4,306 pages will be released to you in full or in part, and approximately 4,106 pages are being withheld in full.

Accordingly, your request is granted in part and denied in part for the reasons cited above. The Board's Information Disclosure Section will provide you with copies of the documents being made available to you under separate cover. If you believe you have a legal right to any of the information that is being withheld, you may appeal this determination by writing to Board of Governors of the Federal Reserve System, Attn: FOIA Appeals, 20th Street & Constitution Avenue NW, Washington, DC 20551; by facsimile to 202-872-7565; or electronically to FOIA-Appeals@frb.gov. Your appeal must be postmarked or electronically transmitted within 90 days of the date of the response to your request.[1]

Very truly yours,

Margaret McCloskey Shanks
Deputy Secretary of the Board

[1]As an alternative to an administrative appeal, you may contact the Board's FOIA Public Liaison, Ms. Candace Ambrose, at 202-452-3684 for further assistance. Additionally, you may contact the Office of Government Information Services ("OGIS") at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, MD 20740-6001; email at ogis@nara.gov; telephone at 202-741-5770 or toll free at 1-877-684-6448; or facsimile at 202-741-5769.

Strategic Framework 2012–15

February 2013

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

Strategic Framework 2012–15

February 2013

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

This and other Federal Reserve Board reports and publications are available online at
www.federalreserve.gov/publications/default.htm.

To order copies of Federal Reserve Board publications offered in print,
see the Board's Publication Order Form (www.federalreserve.gov/pubs/orderform.pdf)
or contact:

Publications Fulfillment
Mail Stop N-127
Board of Governors of the Federal Reserve System
Washington, DC 20551
(ph) 202-452-3245
(fax) 202-728-5886
(e-mail) Publications-BOG@frb.gov

Contents

Preface

In anticipation of the expiration of its 2008–12 Strategic Plan, the Federal Reserve Board launched an enhanced strategic review process that involved the leadership and senior staff in the Board's divisions and offices.

More than 40 directed meetings were conducted at multiple levels of the organization, and the Executive Committee of the Board (ECB)—a body that includes all division and office directors, the chief operating officer, and the administrative governor—held working sessions over the course of several months. These sessions focused on what it would take to meet the mandates of the Wall Street Reform and Consumer Protection Act of 2010 (the Dodd-Frank Act), address the challenge of financial stability more generally, attempt to close cross-disciplinary knowledge gaps, develop appropriate policy, and continue effectively addressing the recovery of a fragile global economy.

The ECB identified and framed the most critical organizational challenges, developed potential options for addressing them, and clarified the tradeoffs. This strategic framework is the result.

The Board releases this strategic framework—which was approved on June 26, 2012—in the spirit of the Government Performance and Results Act (GPRA) of 1993, which requires that federal agencies, in consultation with Congress and outside stakeholders, prepare a strategic plan covering a multiyear period and submit an annual performance plan and performance report. The GPRA Modernization Act of 2010 refines those requirements to include quarterly performance reporting. Although the Board is not covered by GPRA, the Board follows the spirit of the act and prepares and publicizes these regular plans and performance reports.

This strategic framework is one of the reports published by the Board in the spirit of GPRA. Others include the

- *Annual Performance Plan.* This document includes specific targets for some of the Board's performance measures identified in the strategic plan and describes the operational processes and resources needed to meet those targets. It also discusses validation of data and verification of results.
- *Annual Performance Report.* This document discusses the Board's performance in relation to strategic themes and objectives.

Several other documents provide further information about the planning, budgeting, operations, and performance of the Federal Reserve System. As required by the Federal Reserve Act, the Board annually submits to the Congress a report describing in detail the operations of the System for the previous year. Since 1985, the System has also provided the Congress with a supplement, the *Annual Report: Budget Review*, which provides a detailed explanation of the plans and resources discussed in the approved budgets of the Board and Reserve Banks.

All these reports are available on the Board's website, at www.federalreserve.gov/publications.

Executive Summary

The 2007–09 financial crisis and the resulting statutory changes called for fundamental changes in the way the Board conducts its operations.

To meet its responsibilities, the Board must make strategic investments in its people, data, and facilities, and enhance its management processes to boost productivity and make coordination more effective across the organization. At the same time, the Board must also continue to manage its resources effectively by capturing cost savings and operational efficiencies.

The Board has defined its priorities for the next four years within the scope of its strategic plan:

- continue building a robust interdisciplinary infrastructure for regulation, supervision, and financial stability
- redesign data governance and management processes to enhance the Board's data environment
- establish a modern, safe work environment that emphasizes the need to maintain data quality and integrity and the importance of enhanced collaboration within the organization and with the public
- create a work environment built on market-oriented compensation and support for academic and personal achievement that attracts and retains top talent, while maintaining a highly collegial atmosphere
- strengthen management processes to enable effective implementation of strategic themes, increase operating efficiencies, and reduce administrative burden
- establish a cost-reduction approach and a budgetary growth target that maintains an effective and efficient use of financial resources

Achieving these strategic goals will improve the way the Board functions and will require more active collaboration across the divisions at the Board and the System. Such an effort will, furthermore, serve to ensure employees are able to focus on the policy work and research required to anticipate and address emerging risks to U.S. financial stability; it will also support the Federal Reserve's congressionally mandated goals of achieving price stability and maximum sustainable employment in the U.S. economy.

The Board will use this framework to align resources and to implement changes through 2015. Throughout the implementation, priorities will be reassessed to take into account changing circumstances, environmental factors, and trends. Likewise, funding for these initiatives will be reviewed and offset, to the extent possible, by savings initiatives and efficiency gains.

As the Board implements this framework and makes the necessary investments in people, data, and facilities, the Board recognizes the importance of its longstanding efforts to promote equal employment opportunity and diversity and to foster diversity in procurement.

Introduction

Overview of the Federal Reserve System

The Federal Reserve System is the central bank of the United States, established by the Congress to provide the nation with a safer, more flexible, and more stable monetary and financial system. Over the years, Congress has expanded the System's role in banking and the economy, and today the Federal Reserve System has numerous, varied responsibilities, including

- conducting the nation's monetary policy by influencing the money and credit conditions in the economy in pursuit of maximum employment, stable prices, and moderate long-term interest rates;
- helping maintain the stability of the financial system and containing systemic risks that may arise in financial institutions and markets;
- supervising and regulating a variety of financial institutions and activities to ensure the safety and soundness of the nation's banking and financial systems and to protect certain rights of consumers;
- providing certain financial services to depository institutions, the U.S. government, and foreign official institutions; and
- promoting consumer protection, fair lending, and community development.

The System was created on December 23, 1913, when the Federal Reserve Act was signed into law by President Woodrow Wilson "to provide for the establishment of Federal reserve banks, to furnish an elastic currency, to afford means of rediscounting commercial paper, to establish a more effective supervision of banking in the United States, and for other purposes."

In a 1977 amendment to the Federal Reserve Act, the Congress defined the primary objectives of national economic policy by directing the Board and the Federal Open Market Committee to "maintain long run growth of the monetary and credit aggregates commensurate with the economy's long run potential to increase production, so as to promote effectively the goals of maximum employment, stable prices, and moderate long-term interest rates."

As time has passed, further legislation has clarified and supplemented the System's original purposes. Key laws affecting the Federal Reserve include the Bank Holding Company Act of 1956 and its amendments; the Financial Institutions Reform, Recovery, and Enforcement Act of 1989; the Federal Deposit Insurance Corporation Improvement Act of 1991; the Gramm-Leach-Bliley Act of 1999; the Check Clearing for the 21st Century Act of 2004; and the Dodd-Frank Act.

Background: The Dodd-Frank Act and Its Impact on the U.S. Regulatory Framework

The passage of the Dodd-Frank Act was a significant event for the Federal Reserve and other U.S. regulators of financial institutions and entities.

The act was designed to address critical gaps and weaknesses in the U.S. regulatory framework that were revealed during the course of the financial crisis. For example, the act created an interagency council to monitor and coordinate responses to emerging threats to the financial system, required that large bank holding companies and systemically important financial firms be subject to enhanced prudential standards to reduce the risks they may present to the financial system, and provided for the consolidated supervision of all systemically important financial institutions.

It also provided a mechanism for resolving financial firms whose failure could pose a threat to U.S. financial stability, and provided for the strengthened

supervision of systemically important financial market utilities that provide payment, settlement, and clearing services. Moreover, the act enhanced the transparency of the Federal Reserve while preserving its independence, a feature crucial to its ability to implement monetary policy effectively.

In January 2011, pursuant to section 342 of the Dodd-Frank Act, the Board established an Office of Diversity and Inclusion (ODI). The Board has welcomed the new requirements under section 342 of Dodd-Frank as a complement to, and strengthening of, its existing efforts. ODI is working with Human Resources and Procurement staff at the Board to (1) ensure a commitment to recruit and retain a staff that is diverse and inclusive and (2) develop standards and procedures to ensure, to the extent possible, the fair inclusion and utilization of minority- and women-owned businesses in the Board's procurements.

Structure of the System

The Federal Reserve System is considered to be an independent central bank because its decisions are not ratified by other branches of government. The System is, however, subject to oversight by the Congress, and must work within the framework of the overall objectives of economic and financial policy established by its enabling statutes.

Congress designed the structure of the Federal Reserve System to ensure it maintained a broad perspective on the economy and on economic activity in all parts of the nation. It is a federated system, composed of a central, governmental agency—the Board of Governors—in Washington, D.C., and 12 regional Federal Reserve Banks.

A major component of the System is the Federal Open Market Committee (FOMC), a deliberative body consisting of the members of the Board of Governors, the president of the Federal Reserve Bank of New York, and presidents of four other Federal Reserve Banks (who serve on a rotating basis). The FOMC oversees open market operations, the main tool used by the Federal Reserve to influence overall monetary and credit conditions in the United States.

Board of Governors

The Board of Governors of the Federal Reserve System (the Board) is a federal government agency. The Board is composed of seven members, each of whom is appointed by the President and confirmed by the Senate. The full term of a Board member is 14 years, and the appointments are staggered so that one term expires on January 31 of each even-numbered year.

The Chairman, Vice Chairman, and the Vice Chairman for Supervision of the Board are also appointed by the President and confirmed by the Senate. The nominees to these posts must already be members of the Board or must be simultaneously appointed to the Board. The terms for these positions are four years.

Mission and Values of the Board of Governors

The Board's longstanding mission is to foster the stability, integrity, and efficiency of the nation's monetary, financial, and payment systems in pursuit of optimal macroeconomic performance. This mission is rooted in the Federal Reserve System's statutory mandates, and on a set of core institutional values.

- **Public interest.** In its actions and policies, the Board seeks to promote the public interest; it is accountable and responsive to the general public, the U.S. government, and the financial community.
- **Integrity.** The Board adheres to the highest standards of integrity in its dealings with the public, the financial community, and its employees.
- **Excellence.** The conduct of monetary policy, responsibility for bank supervision, and maintenance of the payment system demand high-quality analysis, high performance standards, and a secure, robust infrastructure. The pursuit of excellence drives the Board's policies concerning recruitment, selection, and retention of Board employees.
- **Efficiency and effectiveness.** In carrying out its functions, the Board is continually aware that its operations are supported primarily by public funds, and it recognizes its obligation to manage resources efficiently and effectively.

- **Independence of views.** The Board values the diversity of its employees, input from a variety of sources, and the independent professional judgment that is fostered by the System's regional structure. It relies on strong teamwork and consensus-building to mold independent viewpoints into coherent, effective policies.

Board Division Responsibilities

The Board is organized along divisional lines, with each division having specific functions.

Office of Board Members

The Office of Board Members—including the seven Governors—provides overview, direction, and supervision for System goals, objectives, and projects involving monetary policy, supervision and regulation policy, and managerial policy.

Within the office, the public affairs unit provides the public with information concerning Federal Reserve actions and works to increase the public's understanding of the System's functions, responsibilities, and policy goals. The congressional liaison program facilitates effective communication between the Board and the Congress and other government agencies.

Office of the Secretary

The Office of the Secretary provides corporate secretary and governmental services to Board members, Board staff, and the public.

The division maintains electronic information systems (Board records management and distribution/voting applications), oversees Board meetings and agendas, prepares minutes of Board meetings and notation voting summaries, and administers the Freedom of Information Act program. Specialty services include managing the Reserve Bank directors program (providing guidance on selection of directors and applicable regulations and conducting orientation programs and conferences for Reserve Bank directors and chairs), securing official passports for Board and System staff, planning official conferences and events, and providing temporary executive assistants for Board members.

The division also serves as liaison to the Federal Advisory Council and the Community Depository Institutions Advisory Council and acts as the Board's Ombudsman.

Research and Statistics

The Division of Research and Statistics (R&S) focuses on the domestic economy, and provides the Board, FOMC, and other System officials with analysis and research pertaining to current and prospective economic conditions, and supplies data and analyses for public use. The division also provides analysis and research pertaining to supervision and regulation, payment system policy and oversight, and consumer affairs.

International Finance

The Division of International Finance (IF) focuses on the global economy and provides the Board, the FOMC, and other System officials with assessments of current and prospective international, economic, and financial developments. The division evaluates and forecasts major economic and financial developments abroad, developments in foreign exchange and other international asset markets, and U.S. international transactions.

The division maintains close contacts with international organizations and foreign official institutions and supports the Board's participation in international meetings. The division also provides support for the Board's financial supervision and regulation activities and supplies data on international financial positions for public use.

Monetary Affairs

The Division of Monetary Affairs (MA) supports the Board and the FOMC in the formulation of U.S. monetary policy and on matters pertaining to financial stability.

The division serves as secretariat of the FOMC and contributes to the communication of policy through vehicles such as the FOMC statement and the minutes of FOMC meetings. The division also oversees the implementation of monetary policy through open market operations, discount rates and the operations and administration of the discount window, and reserve requirements.

It coordinates with the Open Market Desk at the Federal Reserve Bank of New York in the conduct of open market operations. The division produces data

series on related financial elements of the economy and analyses developments in money, reserves, bank credit and profits, and interest rates, and forecasts movements in money, reserves, and bank credit. Staff in the division, working with colleagues in other divisions, conducts analysis of topics related to financial stability, assists in the implementation of the Dodd-Frank Act, and provides support for the Board's financial supervision and regulation activities (including "stress-testing" of financial institutions and helping in the development of regulations related to liquidity issues). The division also oversees the Term Deposit Facility and the Statistics and Reserves business function for the System.

Office of Financial Stability Policy and Research

The Office of Financial Stability Policy and Research (OFS) coordinates staff support to the Board and FOMC on financial stability policy. Together with staff in other divisions and the Reserve Banks, it analyzes risks to the financial system by monitoring key financial institutions, markets, and infrastructures, and conducts research on the causes and consequences of financial disruptions.

The office also develops and evaluates alternative macroprudential supervisory and regulatory policy responses, and presents them for consideration to policymakers in order to mitigate emerging and structural vulnerabilities. In addition, the office coordinates the Federal Reserve's involvement in interagency and international financial stability policymaking groups, including the Financial Stability Oversight Council (FSOC) and the Financial Stability Board (FSB).

Banking Supervision and Regulation

The Division of Banking Supervision and Regulation (BS&R) is responsible for informing the Board on current and anticipated developments in bank supervision and banking structure. The division also coordinates and directs the System's bank supervision and examination activities; in this role, the division develops and ensures implementation of policy for these activities, and it develops requirements for data collection, supervisory automated systems and related technology, and training. The division has a leading role in the implementation of the Dodd-Frank Act provisions across the Federal Reserve System. In addition to these responsibilities, the division also processes applications for prior consent to form or expand bank holding companies or make other changes in banking structure.

Consumer and Community Affairs

The Division of Consumer and Community Affairs (C&CA) informs the Board on the concerns of consumers and communities and coordinates the System's consumer compliance supervision and examination activities, including policy development and examiner training. The division also conducts consumer focused research and policy analysis, implements requirements for consumer protection statutes, and promotes community development in traditionally underserved neighborhoods.

Legal Division

The Legal Division provides legal advice and services to the Board to meet its responsibilities in all aspects of its duties, including the Board's bank supervisory and regulatory responsibilities. The division also provides legal support for the Board's role in developing and implementing monetary policy, employing its financial stability tools, and all aspects of the Board's operations, including the Board's procurement and personnel functions, ethics, and information disclosure.

The Legal Division represents the Board in litigation in federal and state court, and pursues enforcement actions against individuals and companies over which the Board has supervisory authority. The Legal Division also drafts regulations and proposes statutory changes to advance the Board's mission.

Reserve Bank Operations and Payment Systems

The Division of Reserve Bank Operations and Payment Systems (RBOPS) oversees the Federal Reserve Banks' provision of financial services to depository institutions, fiscal agency services to the Treasury and other entities, and emergency liquidity facilities.

The division also has oversight responsibility for Reserve Bank support functions, such as information technology, human resources, financial and cost accounting, operating and capital budgets, facilities management, and internal audit. In addition, it develops and recommends to the Board policies and regulations governing payment, clearing, and settlement systems; works collaboratively with other central banks and market regulators to set standards to

promote the safety and efficiency of payment, clearing, and settlement systems globally; and conducts research regarding payment and settlement matters.

Office of the Chief Operating Officer

The Office of the Chief Operating Officer works with all division directors to establish, implement, and measure performance against the Board's strategic direction, and provides analysis and counsel to the administrative governor regarding the overall operation of the Board's administrative functions, technology services, and short- and long-term strategic planning goals.

The chief operating officer provides oversight to the Division of Information Technology, the Management Division, the Division of Financial Management, the Office of Diversity and Inclusion, and the chief data officer function.

Division of Financial Management

The Division of Financial Management (DFM) is responsible for providing effective financial and risk management activities across the organization, including (1) overseeing implementation of the recommendations resulting from the ongoing strategic planning effort and (2) ensuring that the investment requirements outlined in the strategic plan are aligned with the Board's budget process.

Information Technology

The Division of Information Technology (IT) provides infrastructure support to all Board divisions, including mainframe operations and distributed processing, applications development, central automation and telecommunication support, data and communications security, local area network administration, and technology reviews of all Board functions.

Management Division

The Management Division (MGT) provides the full spectrum of personnel management, facility, and logistical support for the Board's day-to-day operations, including managing office space and property and providing food services and physical security. The division also provides continuity-of-operations services and business-resumption services.

Office of the Inspector General

The Office of the Inspector General (OIG) conducts independent and objective audits, inspections, evaluations, investigations, and other reviews related to the program and operations of the Board and the Consumer Financial Protection Bureau. Through this work, OIG promotes integrity, economy, efficiency, and effectiveness; helps prevent and detect fraud, waste, and abuse; and strengthens the agencies' accountability to Congress and the public.

The Impact of the 2007–09 Financial Crisis and the Dodd-Frank Act on the Board

While the Federal Reserve's broad mission and functions remain essentially unchanged, the 2007–09 financial crisis fundamentally changed how the Board operates within its functional disciplines.

Changes in the Board's approach to monetary policy, supervision, and financial stability are expected to prove particularly critical, and will drive an evolution in Board capabilities begun after the crisis and in response to the provisions of the Dodd-Frank Act. This operational evolution will prove central to the Board's effort to continue to build its capabilities in key areas over the next four years covered under this strategic plan:

- **Elevating financial stability.** First and foremost, the review of the financial crisis of 2007–09 elevated the importance of designing the operational capabilities in the Federal Reserve System to help identify threats to the stability of the U.S. financial system. Today, financial stability issues are prominent in discussions of monetary policy, and the Board is providing a robust policy infrastructure to support financial stability. When completed, this new infrastructure will include new capital and liquidity requirements to strengthen the financial sector, a more robust monitoring system for markets and institutions, an ambitious research agenda to establish context for policymakers, and more effective tools for addressing future financial crises.
- **Enhancing supervision.** The crisis highlighted gaps in the regulatory structure imposed by statute to supervise financial institutions. In particular, it

became clear that various entities exerting potential impact on the nation's monetary, financial, and payment systems were inadequately supervised at the federal level. In addition, the crisis revealed that existing supervisory policies did not fully address issues raised by complex and interrelated financial structure.

While broader government-wide improvements and changes are needed to address these issues, the Board, for its part, has adopted an enhanced supervisory approach that takes a more systemic approach to understanding the risks posed by the combined actions of institutions rather than focusing on the health of individual firms; this includes business drivers, new industry practices, new products, and the potential risk implications of such developments in financial markets and the economy. The more proactive approach to supervision reflected in the Dodd-Frank Act has meant re-thinking the type of skills required at the Board, and improving coordination of new and existing skill sets across the System.

- **Developing and refining new tools for monetary policy.** The financial crisis tested the limits of traditional monetary policy tools, and triggered a re-examination of standard monetary policy assumptions.

Looking ahead, the Board will focus significant efforts on research regarding the evaluation of tools introduced during the crisis, such as large-scale asset purchases and emergency liquidity provision. The organizational challenge will include ensuring the right balance between, on one hand, resources devoted to designing monetary policy and, on the other hand, resources needed to support crisis prevention or containment.

- **Integrating the way monetary policy and financial stability decisions are made.** The Dodd-Frank Act gives the Federal Reserve an important role in areas of financial stability policy (such as macroprudential supervisory oversight), defining the conditions that can result in financial instability, identifying policy strategies that can prevent such outcomes, and providing oversight of systemically important financial institutions and financial market infrastructures. The Federal Reserve's role in financial stability also recognizes that the analysis and data required for supervision is useful in conducting monetary policy and vice versa. It will take time and effort to establish the processes and procedures that best exploit these synergies.

Meeting the Strategic Challenges

Meeting the challenges in the four areas described in the previous section requires appropriate levels of Board resources and investments in people, data, and facilities. Meeting these challenges also requires management processes for hiring, developing, and re-allocating expertise and coordination across the organization.

The following six themes will guide investment and action over the 2012–15 planning period:

- continuing to build a robust infrastructure for regulation, supervision, and monitoring risks to financial stability
- redesigning data governance and management processes to enhance the Board's data environment
- ensuring a modern, safe work environment that emphasizes the need to maintain data quality and integrity and the importance of enhanced collaboration within the organization and with the public
- creating a work environment built on market-oriented compensation and support for academic and personal achievement that allows the Board to attract and retain top talent while reinforcing collegiality
- strengthening management processes to enable effective implementation of strategic themes, increasing operating efficiencies, and reducing administrative burden
- establishing a cost-reduction approach and a budgetary growth target that maintains an effective and efficient use of financial resources

Strategic investments in these areas above those required for day-to-day operations are necessary for the Board to meet the supervisory expectations of it under the Dodd-Frank Act while continuing to enhance its ability to promote stable prices, full employment, and financial stability. The strategic investments are also accompanied by an agenda of management process changes that will keep major investments on track, identify additional opportunities for cost savings, and improve overall operations.

Strategic Themes

Strategic Theme 1

Continue Building a Robust Infrastructure for Regulation, Supervision, and Monitoring Risks to Financial Stability

The financial crisis of 2007–2009 has resulted in an enhanced approach to supervision and regulation, which places a heightened emphasis on the health of both individual institutions and the financial system as a whole. As a result, the Board has emphasized its interdisciplinary approach to regulation and supervision, regularly involving economists, legal experts, and regulatory experts in supervisory exercises and in rulewriting.

In addition, the Board has increased its base of knowledge and experience concerning fundamental business drivers, related risks, the interconnectedness of the modern financial landscape, and potential outcomes in a complex and dynamic market environment.

Finally, the Board's role in the supervisory oversight of systemically important firms has expanded. The Dodd-Frank Act gives the Federal Reserve responsibilities and powers to oversee additional financial institutions that the interagency council (FSOC) designates as systemically important. The act also formalized several of the macroprudential tools that supervisors and regulators use, including stress tests, resolution and recovery planning, source-of-strength guarantees, and early remediation requirements.

With the new legal authority in place, the Board has begun to design and build a new policy infrastructure to support its financial stability and prudential supervisory strategies. The Board is coordinating supervision across systemically important firms and leading the development and execution of supervisory efforts. As a coordinator directly participating in supervisory exercises, the Board is uniquely positioned to bring a horizontal perspective concerning systemically important institutions—particularly how changing market conditions are affecting individual firms and financial stability as a whole.

Strategic Objectives

Strategic objective 1: Strengthen the stability of the financial sector through the development of policies, tools, and standards.

Strategic objective 2: Monitor financial markets and industry practices and structures.

Strategic objective 3: Monitor and supervise individual financial institutions and infrastructures.

Strategic objective 4: Ensure that sufficient crisis management tools are in place.

Strategic objective 5: Analyze for the Board and FOMC the role that financial stability concerns should play in setting monetary policy.

Strategic objective 6: Pursue research on stress tests, macroprudential regulation and tools, and other financial stability topics.

Roles and Responsibilities

The policy infrastructure for financial stability will bring resources and expertise together from multiple Board divisions. Three economics divisions (IF, MA, and R&S) and the OFS will continue to drive the Board's research agenda, participate in market monitoring, and collaborate with BS&R and the Federal Reserve Banks on stress tests and cross-institutional reviews focused on particular practices in the financial industry as a whole (horizontal reviews).

These functional areas will also participate and support the Large Institution Supervision Coordinating Committee (LISCC) activities, as required, and develop crisis management tools. OFS will coordinate much of the Federal Reserve's involvement in

interagency and international financial stability policymaking groups, including FSOC and the FSB. The Legal Division will lead some Dodd-Frank Act implementation initiatives and review all new rules. Legal will also continue to provide advice to the banking supervision function.

Potential Risks and Challenges

The success of the Board's financial stability and supervisory strategy depends on retaining the right mix of skills and expertise, developing sufficient Federal Reserve System capacity, and ensuring high levels of coordination across divisions and across the System.

Without these additional resources, the Board risks delaying its expanded mandate for institutional regulation and financial stability. Failure to fully implement new supervisory rules, activities, and processes could jeopardize the soundness of individual institutions and the financial system at large.

The Board also faces risks to its operational capabilities through staff turnover, as some staff continue to labor under crisis-levels demands on their time and functional capacity. They may leave the Board due to the demanding pace of work, and the Board would have difficulty replacing their specialized skills.

Strategic Theme 2

Redesign Data Governance and Management Processes to Enhance the Board's Data Environment

Data and data management play a critical role in fulfilling the Board's mission. As the Board's mandate has expanded in the wake of the financial crisis and the passage of the Dodd-Frank Act, so has the need for data to meet the breadth and depth of analytical issues that staff are now addressing.

The Board's current process for managing data served the organization well when the Board managed relatively small and predictable data sets that required limited sharing across divisions and within the System. However, the Board and the System now require a data governance and management structure that supports a growing quantity of data and an increased need to share data more broadly while ensuring the operational flexibility required by the Board's data users.

The success of the Board's strategy concerning financial system stability and supervisory strategy depends on proper data management. Implementing a data governance framework will be an important complement to the Board's investment in enhanced research capability. Effective and efficient data management will enhance staff's ability to obtain, interpret, and analyze the large volume of data that new supervisory responsibilities will require. As supervision is a delegated function that is coordinated by the Board, data management for the supervision function will require a System perspective.

Strategic Objectives

Strategic objective 1: Improve data governance by establishing a new Office of the Chief Data Officer and ensuring that there are clear roles and responsibilities among the chief data officer, the Board Data Council, and data users.

Strategic objective 2: Ensure that all enterprise data are handled, processed, stored, and disseminated by professional data management groups.

Strategic objective 3: Strengthen the Board's data environment by establishing an infrastructure to share data and improve opportunities for data integration that supports the Board's research and analytical capabilities.

Roles and Responsibilities

Economists and analysts across the Board's economics divisions, OFS, BS&R, RBOPS, and C&CA will provide input on the development of data policies, including the types of data needed, consistency of policies, and the degree of coordination across the System.

The Board's IT division will play a critical role in designing the overall data environment, including providing the supporting IT infrastructure in coordination with System and Reserve Bank IT partners (as required to support the data needs of Board functions delegated to Reserve Banks). The Board's Legal Division will work closely with the Board's Research Library to develop standards for license-usage agreements with vendors to ensure appropriate use.

Potential Risks and Challenges

The financial crisis and the Board's mandate under the Dodd-Frank Act have created five specific chal-

lenges related to data: quantity, sharing, awareness, access and controls, and quality.

Quantity. Since the financial crisis, the quantity of data required for economic research, policy analysis, and supervisory purposes—both its variety and volume—has increased dramatically, straining current arrangements.

Sharing. The need to share data among Board divisions, the System, and other federal agencies has also increased. There are many more instances where data are already shared, either in an organized manner or informally. However, data sharing has been difficult due to large file sizes and constraints in the existing data environment. The increased need to share data places a burden on the owners of the data since they must serve not only as data managers but also as service providers.

Awareness. Board staff members are not aware either of what data are available or of the full characteristics of such data due to the limitations of available catalogs. In addition, it is important to know the full range of data that the Board collects from the public and regulated parties in order to ensure the Board's continued compliance with the requirements of the Paperwork Reduction Act of 1980.

Controls and access. The Board does not have a uniform set of policies for data security and controls beyond the Federal Information Security Management Act of 2002. This constrains the process of both granting and gaining access to data.

For acquired data, users need to be aware that the data may be subject to a unique set of licensing restrictions. The Board has developed a set of standards for license and usage agreements with vendors to ensure appropriate use; as new license agreements are negotiated, these standards will be implemented for additional data sets.

Quality. Since the onset of the financial crisis, ad hoc data collections have increased; thus, uniformity and guidance are necessary to ensure appropriate data quality.

Strategic Theme 3

Ensure a Modern, Safe Work Environment that Emphasizes the Need to Maintain Data Quality and Integrity and the Importance of Enhanced Collaboration within the Organization and with the Public

Data Center Relocation

The Board's Data Center provides the infrastructure that makes data and servers available to the Board and System for monetary policy, financial supervision, consumer protection, and economic research. Data Center and operational staff are critical in maintaining the Board's computer systems and associated components. Board staff, primarily from its IT and economics divisions, are responsible for determining the infrastructure needs and maintenance requirements of the Data Center.

To be able to meet the increased quantity of data demanded by the economic and supervision function after the financial crisis, the Data Center has had to increase its capacity significantly. In the past two years alone, the Data Center's storage capacity has nearly quadrupled as the number of physical and virtual servers has increased and has also driven the growth of supporting infrastructure. The resulting increased density of storage and computer systems has exceeded the cooling and power capacity of the Data Center.

Strategic Objectives

Strategic Objective 1: Create the capacity for increased data demand.

Strategic Objective 2: Address critical Data Center subsystem requirements.

Roles and Responsibilities

IT, R&S, and MGT will be the primary divisions involved in the Data Center relocation. These divisions will work together to coordinate an agreement,

plan the Data Center relocation, and ensure the continuity of operations during the transition.

Potential Risks and Challenges

The Data Center relocation includes a significant initial investment because of the requirement to build out the associated space. Unintended issues or challenges could result in cost overruns or late delivery, which would impact accomplishment of the Board's mission.

Martin Building Renovation

Ensuring a safe and adequate work environment for individuals and groups to work and meet is a key component of the Board's overall strategy. There have been no significant renovations completed on the Martin Building facility since its construction in 1974.

Short-term upgrades have been made as issues have arisen, but the drive to reduce upfront capital costs has made it more difficult to reduce long-term operating costs. This trade-off has led to an outdated, inefficient building that does not meet the current needs of the Board in fulfilling its missions. Efforts associated with the renovation will focus on security, energy efficiency, meeting and conference space, and physical plant capacity.

Strategic objective 3: Create a safe and secure work environment.

Strategic objective 4: Upgrade physical infrastructure.

Strategic objective 5: Reduce utility consumption and expenses.

Roles and Responsibilities

MGT is responsible for securing sufficient leasing space to accommodate staff during the construction period, overseeing the renovation, and ensuring that the project is completed according to plan while meeting the Board's needs.

Potential Risks and Challenges

A renovation of this scope is a complex undertaking and there are significant implementation risks and transition-oriented challenges that must be managed, particularly as it relates to costs. Risks include disruption to staff during the renovation and ensuring that planning efforts address future space requirements.

Strategic Theme 4

Create a Work Environment Built on Market-oriented Compensation and Support for Academic and Personal Achievement that Attracts and Retains Top Talent While Reinforcing Collegiality

The Board has added almost 400 positions in response to the financial crisis, the implementation of the Dodd-Frank Act, and the general functional support necessary to manage an organization of the Board's complexity and importance to the U.S. financial system and economy.

Over the next four years, the Board will add more full-time employees consistent with the themes described in this strategic framework. Maximizing the value of the Board's human capital will depend on enhancing processes for effective recruitment, development, and retention of qualified staff.

Strategic Objectives

Strategic objective 1: Increase efficiency and effectiveness of the existing performance management process.

Strategic objective 2: Reduce administrative burden associated with the adverse-action process while respecting employees' due-process rights.

Strategic objective 3: Enhance the talent management process (succession planning, development programs, training, etc.).

Strategic objective 4: Increase equitability in compensation and benefits, in closer alignment with the Federal Reserve System and market.

Roles and Responsibilities

MGT, working closely with all Board divisions and offices, will develop and implement the strategic objectives.

Potential Risks and Challenges

Performance Management

The Board will need to ensure that any change it makes to its performance management process does not prevent meaningful distinctions between high and low performers. The Board must also ensure that changes do not make the process more complicated.

Adverse Action

Changes that affect the rights of Board employees must be carefully considered and implemented to ensure compliance with law and to minimize negative effects on morale.

Succession Planning

Lack of a systematic approach to succession planning may lead to concerns that qualified staff are being lost. Moving toward a Board-wide succession-planning process will require significant staff support for governors and division directors as they prepare for talent-assessment sessions. Legal concerns must also be addressed in any succession-planning approach.

Compensation

There are three primary challenges that the Board needs to address in order to increase the effectiveness of its compensation administration system:

- The Board has a fragmented system for administering compensation. Divisions have different standards for writing job descriptions, and because the salary of a position is linked to the job description, the variance in job descriptions allows different salaries for comparable work.
- The current system does not link market rates to Board salaries and benefits for comparable positions. Failing to link market rates to salaries and benefits will limit the Board's ability to attract and retain top talent.
- Variable pay (e.g., cash awards, targeted awards) for staff is limited and too fragmented, making it difficult to adequately distinguish and reward high performers with additional compensation.

Strategic Theme 5

Strengthen Management Processes to Enable Effective Implementation of Strategic Themes, Increase Operating Efficiencies, and Reduce Administrative Burden

The Board defines "management processes" to mean the internal support processes necessary for long-term planning and short-term execution of the Board's priorities. Management processes can include strategic planning, budgeting, identification of cost savings, performance management, risk management, talent management, and knowledge sharing.

Enhancements to the Board's management processes will allow for increased ownership and accountability of leadership decisions, an enhanced ability to prioritize strategic needs, and a potentially reduced administrative burden.

Strategic Objectives

Strategic objective 1: Focus on enterprise issues.

Strategic objective 2: Strengthen financial planning accountability.

Strategic objective 3: Reduce financial management administrative burden.

Roles and Responsibilities

DFM will have primary responsibility for developing the framework to implement the strategic objectives.

Potential Risks and Challenges

Well-designed management processes are essential to driving enterprise-wide decisions, ensuring better coordination, and reducing administrative burden. However, organizational structure and role changes may be equally important, and these changes are difficult to raise and resolve. It is essential to have a single point of accountability for executing and ensuring compliance with these processes.

Another challenge with implementation is the difficulty with defining performance metrics and markers of progress related to strategic outcomes. For example, it is difficult to measure the delivery of high-quality policy insight. As such, it will be important to identify indirect indicators that will show that the Board is on the right track toward achieving desired outcomes.

Finally, the planned changes will require broad commitment from the workforce. To earn that commitment, leaders will need to invest sufficient time to explaining the need for change and what will be different. Appropriate communication of the Board's strategy to both internal and external audiences will be particularly important.

Strategic Theme 6

Establish a Cost-reduction Approach and a Budgetary Growth Target that Maintains an Effective and Efficient Use of Financial Resources

The Board recognizes the importance of continuing to identify opportunities to enhance its operational efficiency and control growth in its operational costs. Implementing these changes will help ensure that the strategic investments remain within a sustainable budgetary range and provide the appropriate level of support so that the Board continues to meet its mandates and builds the capabilities to improve the way it fulfills its mission.

Strategic Objectives

Strategic objective 1: Use financial resources efficiently and effectively.

Strategic objective 2: Achieve budgetary savings and expense growth in line with Board-approved targets.

Roles and Responsibilities

The chief operating officer and the chief financial officer, working with the ECB and other senior staff across the organization, will have primary responsibility for developing the approach, quantifying expected savings, and overseeing implementation.

Potential Risks and Challenges

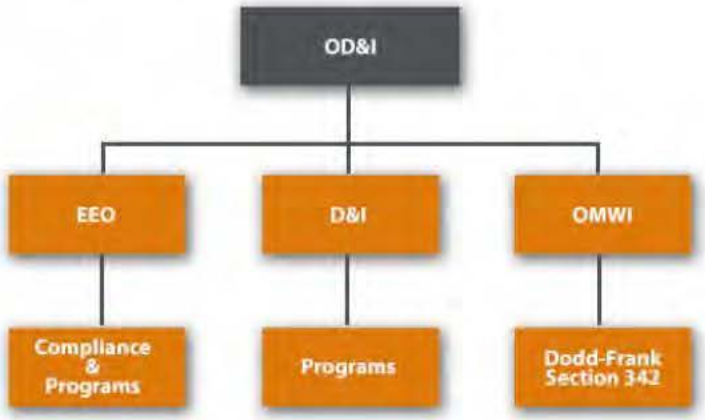
As part of this strategy, the Board expects to capture sufficient savings in its operating budget to offset some of the costs of the strategic priorities. There is inherent risk in trying to establish the proper balance between implementing cost-reduction initiatives and ensuring the appropriate level of resource investment to achieve the goals and objectives outlined in the strategic framework. The Board must ensure that reductions in its administrative and overhead functions do not impede day-to-day operations.

inside the board

PSSC: PRG B.1
Source: ITB - internal Board website

Office of Diversity and Inclusion

Organizational Chart



Source: http://www.federalreserve.gov/careers/salary.htm
Purpose: (b) (5)

Prepared: S. Newman, Auditor
Reviewed: K. Perteet, Sr. Auditor

Careers at the Federal Reserve

Guiding the Nation's Economy

Salary

2014 FR Salary Structures

Exempt and Non-Exempt

Grade	Minimum	Maximum
FR-16	$18,400	$28,400
FR-17	$27,000	$41,400
FR-18	$30,600	$47,000
FR-19	$34,000	$52,200
FR-20	$37,800	$58,200
FR-21	$41,600	$64,800
FR-22	$47,600	$74,800
FR-23	$56,000	$86,000
FR-24	$66,000	$101,400
FR-25	$76,100	$120,900
FR-26	$87,700	$139,300
FR-27	$95,900	$164,700
FR-28	$104,100	$191,300
FR-29	$112,300	$220,800
FR-30	$120,500	$232,000

2014 Wage Employee Salary Structure

Grade	Minimum	Maximum
WE-41	$27,800	$45,600
WE-42	$33,300	$54,700
WE-43	$40,100	$65,700
WE-44	$48,000	$78,800
WE-45	$57,700	$94,500
WE-46	$69,200	$113,400
WE-47	$83,000	$136,200

PRACTICAL Manager
Fall 1990

The Budget Process at the Board

By Kip Livingston

One of the more important tasks facing any manager is the preparation of the budget. At first glance, this strikes some managers as a time-consuming, administrative task rather than a significant managerial function. Most Board managers understand that careful preparation of the program budget is a significant part of their responsibilities and is particularly essential in the Board's budget environment. While preparation of the budget will probably never be fun, it need not be difficult. The purpose of this article is to provide a better understanding of the Board's budget process.

The Board's budget process incorporates the classic budget phases: planning, formulation, implementation, and evaluation. The full process spans two and one half years. Since we begin a new budget each year, there are always two or three budgets in process at any given time.

Formulation

The budget process is the principal element of the planning and management process at the Board. This process begins in the Spring of the year prior to the budget year. Individual divisions conduct strategic planning sessions. During these sessions, divisions develop ideas and plans that will guide them for the years ahead. The division directors present these plans to their respective Board Oversight Committees in May. These meetings provide an opportunity for dialogue between the division directors and Board Members about the general direction the division will follow. The Controller is responsible for scheduling and moderating these meetings.

When the meetings are completed, the Controller's staff prepares an analysis of the potential costs of ideas that were presented, together with a current analysis of likely economic assumptions for the period. Based on these analyses, the Controller presents a recommended budget guideline to the Board in early June.

Upon Board approval of a budget guideline, the Controller sends out a budget call memorandum to all divisions advising them of their individual guidelines and budget submission schedules. The divisions submit their proposed budgets to the Controller during September and October. These proposals are reviewed by the Controller, the Staff Director for Management and the appropriate oversight committees. When these reviews are completed, the Controller summarizes the results and prepares a recommended budget for Board approval in the first week in December.

Implementation

Board approval marks the end of the budget formulation stage. Based on the approved budget, the Controller prepares a cash budget and semi-annual assessment of the Federal Reserve Banks for funds. The Banks then transmit these funds quarterly to our account at the FR Bank of Richmond. Implementation of the Board's budget starts on January 1, with the divisions preparing operating plans that project expenses by month. These plans are entered into computerized systems so that actual

Continued on page 2.

Inside . . .

News items of interest to managers of the Federal Reserve Board
Editor: Juana Montgomery, Division of Human Resources Management, ext. 3385, Stop 146

Salary Increase Recommendations

By Barbara Brodell

Promotions and Career Ladder Progressions serve as a means of recognizing and rewarding employees who assume greater responsibility, within their current job (career ladder progression) or in a new job for which they qualify (promotion).

A **promotion** is a grade increase that an employee receives when he or she is selected to fill a vacant position in a new career ladder with a new set of duties and a higher grade. Employees are selected from a competitive pool of qualified employees through the Board's job posting process. Selection is based on past performance, experience, and qualifications.

A **career ladder progression** is a grade increase that recognizes an employee's proven ability to perform satisfactorily at the next higher grade level, up to the **full performance level. The full performance level is the highest grade level of work that is attainable within a career ladder without using competitive methods.**

A career ladder progression to a grade level above the full performance level is permitted when an employee performs duties and responsibilities that exceed those at the full performance level. Opportunities to progress above the full performance level are limited based on the availability of senior level work in the unit. Selection is made by either interviewing all eligible employees or by reviewing their performance appraisal documents.

When an employee receives a grade increase either through a promotion or career ladder progression, it is accompanied by an increase in salary to recognize the greater level of responsibility. Managers recommending an employee for a career ladder progression or a promotion should submit a recommendation to HRM that considers the following guidelines:

- increases the employee's salary at least to the new range minimum (but generally not above the range midpoint);
- emphasizes the level of increased responsibility assumed by the employee;
- recognizes the employee's education and experience relative to the minimum qualifications for the job level; and
- places the employee's salary relative to other employees with similar jobs at that level, both within the section and the division.

The Compensation staff in HRM approves the division's recommended salary increase taking into consideration the following:

- the employee's education and experience relative to the job requirements;
- the division's recommendation; and
- the salaries of employees with comparable experience and qualifications within the section, division, and other divisions throughout the Board.

HRM strives to ensure that salary decisions are consistent with the Division's recommendation and are internally equitable. When differences of opinion occur, the Compensation Specialist will work with the division manager to reach a mutually agreeable solution. These actions are detailed in the Compensation Program Administrative Manual.

For more information on determining increases for career ladder progressions and promotions, the Compensation Specialists are available to discuss the process in more detail. Lisa Hickman, ext. 3748; Barbara Brodell, ext. 3843 and Ali Emran, ext. 3747.

For practice applying the guidelines discussed above, try the case study on page 5.

Case Study

Assume you are the Manager of the Data Analysis Section. You are recommending that one of the section's employees, Sarah Smith, be given a career ladder progression to grade 24.

What is your recommendation for Sarah's salary increase?

Section: Data Analysis

Job Family: Data Analyst

Current Section Staff:

	Salary	Grade	Experience/Education	Performance History
Christine	$39,000	24	Bachelors + 7 yrs. exp.	CMS
Michael	$42,400	24	Associates + 10 yrs. exp.	CFS
Beth	$36,000	24	Bachelors + 5 yrs. exp.	CES
George	$33,500	23	Bachelors + 7 yrs. exp.	CMS
Sarah	**$33,500**	**23**	**MBA + 4 yrs. experience**	**CES**

Career Ladder:

	Minimum Qualifications	Grade	Salary Range
	Bachelors or equivalent	21	$21,090 - $26,360 - $31,630
	Bachelors + 2 yrs.	23	$29,320 - $36,650 - $43,980
(full performance)	Bachelors + 4 yrs.	24	$34,610 - $43,260 - $51,910
(above full performance)	Bachelors + 6 yrs.	25	$40,820 - $51,030 - $61,240

See page 12 for Compensation staff recommendation.

report to request a hearing and a decision from an Equal Employment Opportunity Commission (EEOC) administrative judge or to request a final Board decision without a hearing.

- You may request a hearing before an EEOC administrative judge any time after 180 days have elapsed since the filing of your formal complaint.
- All requests for a hearing before an EEOC administrative judge must be made by submitting a written request to:

EEOC
131 M Street, NE – Fourth Floor, Suite 4NW02F
Washington, DC 20507

- You are required to send a copy of your request for a hearing to:

Sheila Clark, Program Director
Office of Diversity and Inclusion
Stop 156, Room M-3408
20th Street & Constitution Avenue, NW
Washington, DC 20551

- If you request a final Board decision without a hearing, the Board will have 60 calendar days to render its final decision.
- If you request a hearing before an EEOC administrative judge, the EEOC will appoint an EEOC administrative judge to hold the hearing. The administrative judge will make findings of fact and conclusions of law and will issue a decision. The Board will have 40 calendar days from the date of its receipt of the administrative judge's decision to issue a final order informing you whether it will implement the decision. If the Board does not implement the administrative judge's decision, the Board can file an appeal with the EEOC simultaneously with the issuance of the Board's final order.
- As a complainant, you may appeal the Board's dismissal, or its final decision on your formal complaint, to the EEOC within 30 calendar days of your receipt of the Board's dismissal or final decision.
- As a complainant, you may file a civil action in U.S. district court within 90 calendar days of the Board's final decision or the EEOC's decision on appeal. In addition, you may file a civil action in U.S. district court after 180 calendar days have passed since the filing of your formal complaint or since the filing of your appeal with the EEOC.

Important Points to Remember

- **You have the right to be represented at any stage in the presentation of your complaint by a person of your own choosing. This representative may be a Board employee and need not be an attorney. The Board does not, however, provide attorneys. The Board may determine to award attorney fees to a complainant—but only for the services of an attorney—when a finding of discrimination has been entered or when such an award is deemed appropriate under the applicable regulations. Attorney fees are not available for services performed at the administrative level for Age Discrimination in Employment Act (ADEA) or Equal Pay Act (EPA) complaints.**
- **Any person considering filing an EEO complaint must first meet with an EEO counselor within 45 days of the alleged discriminatory act.**
- **Copies of the Board's EEO rules and the Board's internal policy statements on EEO as well as further details on the EEO complaint process, including the Mediation Program for EEO Complaints, are available from the Office of Diversity and Inclusion.**
- **For a work-related problem in which you do not believe discrimination is a factor, you should first seek a resolution through your supervisor and other division management. If that effort fails, you may wish to contact an employee relations specialist in Human Resources.**
- **If a complaint is determined to be appropriate for mediation, mediation can be offered (prior to the hearing) at both the informal and formal complaint processing stages.**

Office of Diversity and Inclusion

You may contact any representative of the Office of Diversity and Inclusion in person, in writing, by e-mail, or by phone for advice or information on all aspects of equal employment opportunity.

(05/14)

The EEO Complaint System and How It Works

An Equal Opportunity Employer

The Board's policy is to provide equal opportunity in employment for all persons. Thus, consistent with applicable law, the Board prohibits discrimination in employment on the basis of race, color, religion, sex, national origin, age, disability, or genetic information and promotes the full realization of equal employment opportunity (EEO) through a continuing affirmative program. In addition, as a matter of policy and although it is not required by law, the Board prohibits discrimination in employment on the basis of sexual orientation.

The Board is committed to complying with the following statutes and any amendments thereof: Civil Rights Act of 1964 (Title VII), section 501 of the Rehabilitation Act of 1973, the Age Discrimination in Employment Act of 1967, the Equal Pay Act of 1963, the Genetic Information Nondiscrimination Act of 2008, and the Uniformed Services Employment and Reemployment Rights Act of 1994. The Board's plan, program objectives, and goals dealing with equal employment opportunity are set forth in the Board's Rules Regarding Equal Opportunity, 12 CFR 268, and in the Annual EEO Program Status Report adopted by the Board. Both of these documents are available from the Board's Office of Diversity and Inclusion.

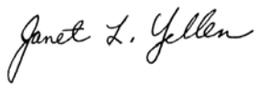
As an essential part of the Board's policy, no one will be subject to retaliation or reprisal for participating in any stage of the administrative or judicial proceedings provided for in the Board's Rules Regarding Equal Opportunity.

The Board has a zero-tolerance policy for discriminatory harassment, which includes sexual harassment. The Board is committed to preventing any discriminatory harassment.

The Board calls on senior management to comply fully with its policy of a work environment that is free from discrimination, hostility, intimidation, reprisal, and harassment. Each manager, at every level, must ensure that the Board's commitment to equality of opportunity is honored.

The following is an overview of the Board's EEO complaint process. For a comprehensive review of the Board's EEO program, employees and applicants for employment are encouraged to review the Board's Rules Regarding Equal Opportunity.

Sincerely,



Janet L. Yellen, Chair

Equal Employment Opportunity (EEO) Designations

The Board designates members of its staff to help carry out the functions described in the Board's Rules Regarding Equal Opportunity.

EEO Counselors		
Johanna C. Bruce	M-3304	ext. 2787
Penny Thompson	M-3310	ext. 2077
Daniel Aranda	M-3303	ext. 3367

EEO counselors are available to counsel any Board employee or applicant who feels that he or she has been discriminated against because of race, religion, color, national origin, sex, age, disability, genetic information, or sexual orientation, or has been subjected to retaliation for engaging in protected activity.

Receipt of Complaints

The following individual is designated to receive formal complaints of discrimination:

Sheila Clark, Program Director
Office of Diversity and Inclusion
Board of Governors of the Federal Reserve System
Stop 156, Room M-3408
20th Street & Constitution Avenue, NW
Washington, DC 20551
Voice: (202) 452-2883

Approaches to Address Complaints

If you believe that you have been discriminated against because of your race, religion, color, national origin, sex, age, disability, genetic information, or sexual orientation, or have been subjected to retaliation for engaging in protected activity, you should contact an EEO counselor.

If you believe that you are a victim of discriminatory harassment, which includes sexual harassment, you may contact an EEO counselor. You may also seek relief by reporting such conduct through the established channels designated in the Board's Discriminatory Workplace Harassment Policy. In this regard, an employee may report discriminatory harassment to (1) the offending individual's supervisor or the harassed employee's supervisor; (2) the offending individual's division director or the harassed employee's division director; (3) the Office of Diversity and Inclusion program director, (4) an employee relations specialist in the Human Resources Function of the Management Division; (5) the officer responsible for Employee Relations, or his or her designee; (6) for employees in Human Resources, the assistant general for Human Resources in the Legal Division.

The EEO Complaint System

The following steps summarize the Board's EEO complaint process for employees and applicants who feel they have been discriminated against because of their race, religion, color, national origin, sex, age, disability, genetic information, or sexual orientation, or have been subjected to retaliation for engaging in protected activity. There are time limits for the filing and resolution of an EEO complaint. Failure of the employee or applicant to meet the time requirements stated for any stage of the complaint process may result in the dismissal of the complaint or the loss of administrative and judicial rights. These steps also apply to complaints of retaliation and equal pay (sex-based wage discrimination).

- You must contact an EEO counselor within 45 calendar days of the date of the matter alleged to be discriminatory or, in the case of a personnel action, within 45 calendar days of the effective date of the action.
- Unless you agree to an extension of time, the EEO counselor has 30 calendar days to inquire into your informal complaint, to attempt a resolution of the matter, and to advise you how to file a formal complaint if the matter is not resolved.
- In the event the Board's alternative dispute resolution process is offered to you and you agree to participate in mediation, the informal complaint processing period will be 90 days. Mediation will be offered on a case-by-case basis, when the program director deems a complaint appropriate for mediation.
- If the EEO counselor cannot resolve your complaint or if your complaint is in mediation and it is not resolved by the 90th day, the EEO counselor will issue you in writing a notice of your right to file a formal complaint with the Board. Should you choose to file a formal complaint, you must do so within 15 calendar days after your receipt of this notice.
- If you file a formal complaint, the Office of Diversity and Inclusion will review that complaint and determine the issues accepted for investigation. The Office of Diversity and Inclusion will then assign an EEO investigator to investigate the issues accepted in your complaint.
- At the conclusion of the investigation, the program director will provide you with the investigative report.
- You will have 30 calendar days from receipt of the investigative

Source: ITV Board Job Postings
Purpose: (b) (5)
Prepared by: S. Newman
Reviewed by: K. Perteet

Sign In to access application status, saved documents and Job Search Agents

Job Details

View Search Results | View Job Cart (0) | View My Account

Executive Recruiter

Job ID #: 10306
Functional Area: Human Resources
Employment Status: Temporary
Position Type: Full-Time
Education Required: Bachelor's or Equivalent Exp.
Salary Grade Low: 27
Salary Grade High: 28
Career Ladder High: 28
Closing Date: FEB 17, 2015

Location: Washington, DC
Facility: Not Indicated
Division: Management Division
Relocation Provided: Yes
Experience Required: 7 years

Apply Now | Add to Job Cart

Position Description

The Executive Recruiter will be a critical member of the Human Resources (HR) team and will have a direct impact on the future success of HR in addressing the leadership and workforce succession planning needs of clients. The Executive Recruiter serves as a strategic internal consultant to clients and manages the full cycle recruitment process for a broad array of official and senior management positions. The Executive Recruiter will provide an impactful combination of business acumen, strategic functional recruitment and HR experience to support clients with the objective of developing and implementing high quality sourcing and screening strategies for senior level and Officer level positions. This person will create applicant flows and a strong pipeline connection of potential candidates. The incumbent will also: act as a strategic partner and talent acquisition advisor influencing senior leadership teams, pro-actively identify the needs and risks of clients and the Board as they relate to the executive recruitment process, ensure programs continuously meet Board and client business objectives and recommend changes for improvement. The Executive Recruiter maintains a high level of discretion and trust and embodies a strong customer service philosophy.

Position Requirements

Incumbent must demonstrate an established network of executive level job candidates and sourcing network. Incumbent must demonstrate complete mastery and successful track record of the executive level sourcing and placement process and will be expected to act as the resident expert on this topic at the Board. At the FR-27, 7 years of experience required; at the FR-28, 8+ years of experience required leading progressively complex senior executive search and recruitment responsibilities in financial services and regulatory organizations. A mastery level knowledge of all Human Resources Management practices and especially Succession Planning and Organizational Design and a mastery level of understanding of Executive Compensation principles as well as current market pricing for Executive level talent. Proficient in working with applicant tracking technology and PeopleSoft. Quickly learns and assimilates complex technical and business requirement information at the Board and has such knowledge from previous work experience. The ability to handle conflicting information and

requirements effectively is important. Demonstrated ability to handle multiple tasks, competing priorities, and challenging situations professionally. Ability to elicit cooperation from a wide variety of sources, including upper management, clients, and other departments. Excellent oral and written communication/presentation skills. Demonstrated commitment to a strong customer service philosophy required. Requires strong human relations and analytical skills typically acquired through completion of a bachelor's degree in management, business administration or related discipline or equivalent experience.

The Federal Reserve Board of Governors is seeking to hire an Executive Recruiter at the Washington DC office. This is a temporary, full-time position for two years with the possibility of an extension.

The Executive Recruiter serves as a strategic internal consultant to clients and manages the full cycle recruitment process for a broad array of official and senior management positions. The Executive Recruiter will provide an impactful combination of business acumen, strategic functional recruitment and HR experience to support clients with the objective of developing and implementing high quality sourcing and screening strategies for senior level and Officer level positions. This person will create applicant flows and a strong pipeline connection of potential candidates. The incumbent will also: act as a strategic partner and talent acquisition advisor influencing senior leadership teams, pro-actively identify the needs and risks of clients and the Board as they relate to the executive recruitment process, ensure programs continuously meet Board and client business objectives and recommend changes for improvement.

The Executive Recruiter will work alongside of the Board recruitment team but with report directly to the Assistant Director for Human Resources.

It is strongly preferred that applicants have at least 5 years tenure as an Executive Recruiter and provide specific examples of successful executive placements, demonstrated success in defining executive level job descriptions, experience requirements and success factors, demonstrated success at driving diverse candidate slates and successful feedback mechanism for the executive level search process.

*****Internal Posting Policy***If an internal Board employee meets the minimum qualifications for this position and applies during the internal job posting preference dates 02/10/2015 to 02/17/2015, then the employee will receive an interview with the hiring manager. Internal Board employees who apply after the internal posting preference period are not guaranteed an interview with the hiring manager.**

We are an Equal Opportunity Employer and do not discriminate against applicants due to race, ethnicity, gender, veteran status, or on the basis of disability or any other federal, state or local protected class.

Back to top

View Search Results | View Job Cart (0) | View My Account

Report to the Congress on the Office of Minority and Women Inclusion

Print

Preface: Implementing the Dodd-Frank Act
Introduction
Equal Employment of Minorities and Women
Inclusion of Minority-Owned and Women-Owned Businesses
Financial Literacy Activities
Diversity Policies and Practices of Regulated Entities
Appendix A

Other Formats
- Full Report (PDF)

Stay Connected
Twitter YouTube
Flickr RSS Feeds
Subscribe

Financial Literacy Activities

During 2013, the Board continued to participate in community and Federal Reserve System outreach events and programs, examples of which are listed below.

- *Congressional Black Caucus Annual Legislative Conference*: In September 2013, the Board, in conjunction with the Federal Reserve System, sponsored a booth at the 43rd Annual Legislative Conference. Financial education materials and information were distributed to conference attendees. The Board also provided support for the Financial Educa ion Youth Summit convened by he Congressional Black Caucus held at the U.S. Capitol Visitor Center and Trinity Washington University.
- *FedEd Program*: During 2013, research assistants from divisions within the Board continued to implement a program developed to work with local high school students to improve their understanding of personal finances and the role of the Federal Reserve System in the economy. Subjects covered include the importance of saving, budgeting, using credit, establishing financial goals, and the impact of Federal Reserve policy on those subjects. More than 40 presentations were made to middle and high school students in the Washington metropolitan area. Presentations were made at ten schools in the District of Columbia: Roosevelt High School; Wilson High School; Coolidge High School; Dunbar High School; Anacos ia High School; Ballou High School; Washington La in Public Charter School; Edmund Burke School; KIPP DC Charter School; and St. Albans School. Presentations were made at two schools in Virginia--Annandale High School and Marshall High School--and one school in Maryland--Stone Ridge School of the Sacred Heart. Presentations were also made at the District of Columbia Public Schools Central Office to preview the FedEd Program for the New Heights Providers Meeting, the Sumner School for the DC Future Business Leaders of America, and the Heights School.
- *Federal Reserve Financial Literacy Day*: On October 23, 2013, the Board and the Federal Reserve System held training programs and seminars around the country on such topics as saving, budge ing, credit use, and the establishment of financial goals. Board research assistants presented the program to classes at two schools in the District of Columbia: Cardozo High School and the Columbia Heights Education Campus.
- *Math x Economics*: On May 23, 2013, the Board hosted the Math x Economics program for a second year in a row. The goal of the program was to introduce students to economics as a potential course of study in college and as a future career option. The Board's recruitment efforts targeted groups who are underrepresented in the field of economics, including minorities and females, especially from underserved schools. A total of 29 students from Washington metropolitan area schools attended. The students completed a survey at the end of the program; all 29 participants said they would recommend the program to other students. The descriptive statistics of the respondents are listed below.

Distribution of participants	Percent
Female	56
Male	44
Juniors	78
Seniors	22
African American	25.9
Hispanic	18.5
Asian	18.5
White	18.5
More than one ethnicity	14.8
Did not specify ethnicity	3.7

- *Education and Training Materials Distribution*: During 2013, the Board continued to provide financial literacy materials to consumer education and financial literacy groups, including the University of Maryland Extension Family and Consumer Sciences Center, the YMCA of Metropolitan Washington, Operation HOPE, and It Takes a Community to Raise a Child (located in New York City).

- *Professional Outreach*: On April 3, 2013, Chairman Bernanke delivered remarks to the 13 h Annual Redefining Investment Strategy Education (RISE) Forum. His remarks highlighted he importance of promoting economic and financial knowledge among people of all ages and walks of life. He stated that the Board and the 12 Federal Reserve Banks are all deeply involved in economic education and in supporting the work of teachers, schools, and national organizations.

  On November 13, 2013, Chairman Bernanke hosted the annual Teacher Town Hall Meeting at the Federal Reserve Board. Federal Reserve Banks also held gatherings around the country to provide educators the opportunity to listen to the Chairman and ask questions. His remarks covered the origins, history, and role of the Federal Reserve, and how it has helped shape the nation's economy and financial system.

Last update: Apr 8, 2014

October 30, 2014
Federal Reserve Board
Washington, D.C.

Sponsored by:
Federal Reserve Board

National Summit on Diversity in the Economics Profession

Print

About | Conference Program

About

The National Summit on Diversity in the Economics Profession, hosted by the Board of Governors of the Federal Reserve System in partnership wi h the American Economic Association, will be held at the Federal Reserve Board on October 30, 2014 in Washington, D.C. This conference brings together presidents and research directors of he Federal Reserve Banks and chairs of economics departments from around the country to open a profession-wide dialogue about diversity. Speakers and panelists will discuss he state of diversity in the economics profession and examples of successful diversity initiatives in academia. A hallmark of the conference will be the opportunity for collegial learning, discussion, and sharing among faculty peers to develop practical ideas about what can be accomplished in our profession.

Please note that attendance at the conference is by invitation only. Conference attendees and media representatives must register in advance.

Watch the online webcast of the event at http://www.ustream.tv/federalreserve

Organizers

- Janice Shack-Marquez
- Amanda Bayer

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
Eighth Annual No FEAR Act Report
Fiscal Year 2011

The Board of Governors of the Federal Reserve System (Board) hereby submits this Eighth Annual Report pursuant to the requirements of Section 203 of the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (No FEAR Act), Public Law 107-174. In accordance with Section 203(a) of the No FEAR Act and its regulations there-under (5 C.F.R. § 724.302), this Eighth Annual Report is being forwarded to the Speaker of the House of Representatives, the President pro tempore of the Senate, the Committee on Governmental Affairs of the Senate, the Committee on Government Reform of the House of Representatives, each committee of Congress with jurisdiction relating to the Board, the Equal Employment Opportunity Commission, and the Attorney General of the United States, and the Director of the Office of Personnel Management.

The Board responds to the items listed in Section 203(a) (1) through (8) of the No FEAR Act and 5 C.F.R. § 724.302 as follows:

(1) The number of cases in Federal court pending or resolved in each fiscal year and arising under each of the respective provisions of the Federal Antidiscrimination Laws and Whistleblower Protection Laws applicable to the agency as defined in 5 C.F.R. § 724.102 in which an employee, former Federal employee, or applicant alleged a violation(s) of these laws, separating data by the provision(s) of law involved;

Fiscal Year 2011	
Basis of Actions	***Total Cases Pending or Resolved***
29 U.S.C.§ 633a (Age)	1
42 U.S.C. § 2000e-16 (Race, Color, Religion, Sex, or National Origin)	2

(2) In the aggregate, for the cases identified in paragraph (1), above, and separated by provision(s) of law involved:

(i) The status or disposition (including resolved);

Fiscal Year 2011	
Status or Disposition:	***Pending***
Basis of Actions	
29 U.S.C.§ 633a (Age)	1
42 U.S.C. § 2000e-16 (Race, Color, Religion, Sex, or National Origin)	2
	Resolved
Basis of Actions	
29 U.S.C.§ 633a (Age)	0
42 U.S.C. § 2000e-16 (Race, Color, Religion, Sex, or National Origin)	0

(ii) The amount of money required to be reimbursed to the Judgment Fund by the agency for payments as defined in 5 C.F.R. § 724.102;

None

(iii) The amount of reimbursement to the Fund for attorney's fees where such fees have been separately designated;

None

(3) In connection with cases identified in paragraph (1), above, the total number of employees in each fiscal year disciplined as defined in 5 C.F.R. § 724.102 and the specific nature, e.g., reprimand, etc., of the disciplinary actions taken, separated by the provision(s) of law involved;

None

(4) The final year-end data about discrimination complaints for each fiscal year that was posted in accordance with Equal Employment Opportunity Regulations at subpart G of title 29 of the Code of Federal Regulations (implementing section 301(c)(1)(b) of the No FEAR Act);

Attached is a copy of the No FEAR fiscal year-end data posted as of September 30, 2011, for fiscal year 2011.

(5) Whether or not in connection with cases in Federal court, the number of employees in each fiscal year disciplined as defined in 5 C.F.R. § 724.102 in accordance with any agency policy described in paragraph (6), below. The specific nature, e.g., reprimand, etc., of the disciplinary actions taken must be identified.

None

(6) A detailed description of the agency's policy for taking disciplinary action against Federal employees for conduct that is inconsistent with Federal Antidiscrimination Laws and Whistleblower Protection Laws or for conduct that constitutes another prohibited personnel practice revealed in connection with agency investigations of alleged violations of these laws;

The Board does not have a separate policy for disciplining Board employees found to have committed practices referenced above. However, the Board's disciplinary policies, the Disciplinary Actions Policy and the Adverse Action Policy, will be used to discipline such employees.

Under the Disciplinary Actions policy, the Board may take progressive discipline to correct unsatisfactory conduct or other work-related problems. Progressive discipline is the application of graduated actions in disciplinary cases. It can include, where appropriate, oral counseling, written warnings, and suspensions of 14 calendar days or less. Under the Adverse Action Policy, adverse action against an employee may be in the form of discharge, removal, or suspension without pay for a period of more than 14 calendar days, or a reduction in grade or pay.

(7) An analysis of the information provided in paragraphs (1) through (6), above, in conjunction with data provided to the Equal Employment Opportunity Commission in compliance with 29 C.F.R. § 1614. Such analysis must include: (i) An examination of trends; (ii) Causal analysis; (iii) Practical knowledge gained through experience; and (iv) Any actions planned or taken to improve complaint or civil rights programs of the agency with the goal of eliminating discrimination and retaliation in the workplace;

During the reporting period, the EEO staff collaborated and partnered with the Human Resources Employee Relations staff to identify issues, trends and workplace challenges relating to workplace harassment. Meetings were held with senior management to address harassment resolution. Customized managerial workplace harassment training was conducted for departments with related issues.

Although the Board has provided workplace harassment training, harassment complaints continue to enter the EEO complaint process. Behavioral transition from

receiving training to changing workplace behavior has been a challenge for the Board. Currently the Board is developing a Workplace Harassment Policy which will establish fundamental processes and procedures in an effort to address occurrences. A workplace harassment module for managerial and non-managerial employees has been included in the No FEAR required training. Training completion will be tracked in a Learning Management System. Customized workplace harassment classroom training was conducted in FY 2011 and will also be conducted in FY 2012 along with web-based training.

During FY 2011 the Board's EEO staff counseled 58 pre-complaints, of which 10 entered the formal complaint process. In FY 2010, 86 pre-complaint counseling sessions were held and 7 entered the formal complaint process. The increase in the number of formal complaints filed is attributable to an increase of alleged work place harassment issues. The EEO staff continues to focus on effective counseling in the informal stage in the attempt to reach resolutions through mediation and facilitated discussions between parties involved.

(8) For each fiscal year, any adjustment needed or made to the budget of the agency to comply with its Judgment Fund reimbursement obligation(s) incurred under 5 C.F.R. § 724.103.

None

(9) The agency's written plan developed under 5 C.F.R. § 724.203(a) to train its employees.

See attached agency No FEAR Act Training Plan.

Attachments as stated:

FY 2011 No FEAR Act data posting
No FEAR Act Training Plan

No FEAR Act

No FEAR Act Notice

The Notification and Federal Employee Anti-discrimination and Retaliation Act (No FEAR Act) of 2002 increases federal agency accountability for acts of discrimination or reprisal against employees.

The No FEAR Act requires agencies to post on their public web sites statistical data relating to equal employment opportunity complaints filed against the respective agencies.

The Federal Reserve Board's public web site contains statistical data in accordance with the No FEAR Act.

Information updated as of December 31, 2011

Complaint activity	Comparative data Previous fiscal year data					Fiscal Year 2012
	2007	2008	2009	2010	2011	10/2011 - 12/2011
Number of complaints filed	1	2	1	7	8	5
Number of complainants	4	3	3	9	15	16
Repeat filers	0	0	0	0	0	0

Complaints by basis	Comparative data Previous fiscal year data					Fiscal Year 2012
Note: Complaints can be filed alleging multiple bases. The sum of the bases may not equal total complaints filed	2007	2008	2009	2010	2011	10/2011 - 12/2011
Race	2	2	1	6	10	12
Color	0	1	0	1	2	2
Religion	0	1	0	0	0	0
Reprisal	3	1	1	2	5	7
Sex	2	2	1	5	8	9
National origin	1	1	1	2	3	2
Equal Pay Act	0	0	0	0	0	0
Age	2	3	3	6	8	11
Disability	0	1	0	3	2	3
Non EEO	0	0	0	0	0	0

Complaints by issue	Comparative data Previous fiscal year data					Fiscal Year 2012
Note: Complaints can be filed alleging multiple issues. The sum of the issues may not equal total complaints filed	2007	2008	2009	2010	2011	10/2011 - 12/2011
Appointment/hire	0	2	0	0	0	0
Assignment of duties	0	0	0	2	3	1
Awards	0	0	0	0	0	0
Conversion to full-time	0	0	0	0	0	0
Disciplinary action						
Demotion	0	0	0	0	0	0
Reprimand	0	0	0	0	0	1
Removal	0	0	0	2	2	2
Suspension	0	0	0	0	0	0
Other	0	0	0	0	0	0
Duty hours	0	0	0	1	0	0
Evaluation appraisal	1	1	1	1	2	2
Examination/test	0	0	0	0	0	0
Harassment						
Nonsexual	2	2	0	4	8	10
Sexual	0	0	0	1	2	1
Medical examination	0	0	0	0	0	0

Pay (including overtime)	0	0	0	1	1	0
Promotion/nonselection	3	1	2	5	6	6
Reassignment						
Denied	0	0	0	0	0	0
Directed	0	0	0	0	0	0
Reasonable accommodation	0	0	0	1	1	1
Reinstatement	0	0	0	0	0	0
Retirement	0	0	0	0	0	0
Termination	0	0	0	0	3	1
Terms/conditions of employment	0	0	0	2	2	4
Time and attendance	0	0	0	0	0	0
Training	0	0	0	0	0	0
Other	0	0	0	3	4	0

Processing time	Comparative data Previous fiscal year data					Fiscal Year 2012
	2007	2008	2009	2010	2011	10/2011 - 12/2011
Complaints pending during fiscal year						
Average number of days in investigation stage	136	169	209	68	163	129
Average number of days in final action stage	44	0	28	28	36	0
Complaints pending during fiscal year where hearing was requested						
Average number of days in investigation stage	136	137	209	93	163	148
Average number of days in final action stage	44	0	28	28	36	0
Complaints pending during fiscal year where hearing was not requested						
Average number of days in investigation stage	0	0	0	87	0	0
Average number of days in final action stage	0	0	0	62	0	0

Complaints dismissed by agency	Comparative data Previous fiscal year data					Fiscal Year 2012
	2007	2008	2009	2010	2011	10/2011 - 12/2011
Total complaints dismissed by agency	0	0	0	0	1	0
Average days pending prior to dismissal	0	0	0	0	531	0
Complaints withdrawn by complainants						
Total complaints withdrawn by complainants	0	1	0	0	0	1

Total final actions finding discrimination	Comparative data Previous fiscal year data										Fiscal Year 2012	
	2007		2008		2009		2010		2011		10/2011 - 12/2011	
	#	%	#	%	#	%	#	%	#	%	#	%
Total number findings	0		0		0		0		0		0	
Without hearing	0	0	0	0	0	0	0	0	0	0	0	0
With hearing	0	0	0	0	0	0	0	0	0	0	0	0

Findings of discrimination rendered by basis	Comparative data Previous fiscal year data										Fiscal Year 2012	
Note: Complaints can be filed alleging multiple bases. The sum of the bases may not equal total complaints and findings	2007		2008		2009		2010		2011		10/2010 - 9/2011	
	#	%	#	%	#	%	#	%	#	%	#	%
Total number findings	0		0		0		0		0		0	
Race	0	0	0	0	0	0	0	0	0	0	0	0
Color	0	0	0	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0	0	0	0
Reprisal	0	0	0	0	0	0	0	0	0	0	0	0
Sex	0	0	0	0	0	0	0	0	0	0	0	0
National origin	0	0	0	0	0	0	0	0	0	0	0	0
Equal Pay Act	0	0	0	0	0	0	0	0	0	0	0	0
Age	0	0	0	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0	0	0	0
Non EEO	0	0	0	0	0	0	0	0	0	0	0	0
Findings after hearing	0	0	0	0	0	0	0	0	0	0	0	0
Race	0	0	0	0	0	0	0	0	0	0	0	0
Color	0	0	0	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0	0	0	0
Reprisal	0	0	0	0	0	0	0	0	0	0	0	0
Sex	0	0	0	0	0	0	0	0	0	0	0	0
National origin	0	0	0	0	0	0	0	0	0	0	0	0
Equal Pay Act	0	0	0	0	0	0	0	0	0	0	0	0
Age	0	0	0	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0	0	0	0
Non EEO	0	0	0	0	0	0	0	0	0	0	0	0

Findings without hearing	0	0	0	0	0	0	0	0	0	0	0	0
Race	0	0	0	0	0	0	0	0	0	0	0	0
Color	0	0	0	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0	0	0	0
Reprisal	0	0	0	0	0	0	0	0	0	0	0	0
Sex	0	0	0	0	0	0	0	0	0	0	0	0
National origin	0	0	0	0	0	0	0	0	0	0	0	0
Equal Pay Act	0	0	0	0	0	0	0	0	0	0	0	0
Age	0	0	0	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0	0	0	0
Non EEO	0	0	0	0	0	0	0	0	0	0	0	0

Findings of discrimination rendered by issue	**Comparative data Previous fiscal year data**										**Fiscal Year 2012**	
	2007		**2008**		**2009**		**2010**		**2011**		**10/2011 - 12/2011**	
	#	**%**	**#**	**%**	**#**	**%**	**#**	**%**	**#**	**%**		**%**
Total number findings	0		0		0		0		0		0	
Appointment/hire	0	0	0	0	0	0	0	0	0	0	0	0
Assignment of duties	0	0	0	0	0	0	0	0	0	0	0	0
Awards	0	0	0	0	0	0	0	0	0	0	0	0
Conversion to full-time	0	0	0	0	0	0	0	0	0	0	0	0
Disciplinary action	0	0	0	0	0	0	0	0	0	0	0	0
Demotion	0	0	0	0	0	0	0	0	0	0	0	0
Reprimand	0	0	0	0	0	0	0	0	0	0	0	0
Suspension	0	0	0	0	0	0	0	0	0	0	0	0
Removal	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0
Duty hours	0	0	0	0	0	0	0	0	0	0	0	0
Evaluation appraisal	0	0	0	0	0	0	0	0	0	0	0	0
Examination/test	0	0	0	0	0	0	0	0	0	0	0	0
Harassment	0	0	0	0	0	0	0	0	0	0	0	0
Nonsexual	0	0	0	0	0	0	0	0	0	0	0	0
Sexual	0	0	0	0	0	0	0	0	0	0	0	0
Medical examination	0	0	0	0	0	0	0	0	0	0	0	0
Pay (including overtime)	0	0	0	0	0	0	0	0	0	0	0	0
Promotion/nonselection	0	0	0	0	0	0	0	0	0	0	0	0
Reassignment	0	0	0	0	0	0	0	0	0	0	0	0
Denied	0	0	0	0	0	0	0	0	0	0	0	0
Directed	0	0	0	0	0	0	0	0	0	0	0	0
Reasonable accommodation	0	0	0	0	0	0	0	0	0	0	0	0
Reinstatement	0	0	0	0	0	0	0	0	0	0	0	0
Retirement	0	0	0	0	0	0	0	0	0	0	0	0
Termination	0	0	0	0	0	0	0	0	0	0	0	0
Terms/conditions of employment	0	0	0	0	0	0	0	0	0	0	0	0
Time and attendance	0	0	0	0	0	0	0	0	0	0	0	0
Training	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0
Findings after hearing												
Appointment/hire	0	0	0	0	0	0	0	0	0	0	0	0
Assignment of duties	0	0	0	0	0	0	0	0	0	0	0	0
Awards	0	0	0	0	0	0	0	0	0	0	0	0
Conversion to full-time	0	0	0	0	0	0	0	0	0	0	0	0
Disciplinary action	0	0	0	0	0	0	0	0	0	0	0	0
Demotion	0	0	0	0	0	0	0	0	0	0	0	0
Reprimand	0	0	0	0	0	0	0	0	0	0	0	0
Suspension	0	0	0	0	0	0	0	0	0	0	0	0
Removal	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0
Duty hours	0	0	0	0	0	0	0	0	0	0	0	0
Evaluation appraisal	0	0	0	0	0	0	0	0	0	0	0	0
Examination/test	0	0	0	0	0	0	0	0	0	0	0	0
Harassment	0	0	0	0	0	0	0	0	0	0	0	0
Nonsexual	0	0	0	0	0	0	0	0	0	0	0	0
Sexual	0	0	0	0	0	0	0	0	0	0	0	0
Medical examination	0	0	0	0	0	0	0	0	0	0	0	0
Pay (including overtime)	0	0	0	0	0	0	0	0	0	0	0	0
Promotion/nonselection	0	0	0	0	0	0	0	0	0	0	0	0
Reassignment	0	0	0	0	0	0	0	0	0	0	0	0
Denied	0	0	0	0	0	0	0	0	0	0	0	0
Directed	0	0	0	0	0	0	0	0	0	0	0	0
Reasonable accommodation	0	0	0	0	0	0	0	0	0	0	0	0

Reinstatement	0	0	0	0	0	0	0	0	0	0	0	0
Retirement	0	0	0	0	0	0	0	0	0	0	0	0
Termination	0	0	0	0	0	0	0	0	0	0	0	0
Terms/conditions of employment	0	0	0	0	0	0	0	0	0	0	0	0
Time and attendance	0	0	0	0	0	0	0	0	0	0	0	0
Training	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0
Findings without hearing	0	0	0	0	0	0	0	0	0	0	0	0
Appointment/hire	0	0	0	0	0	0	0	0	0	0	0	0
Assignment of duties	0	0	0	0	0	0	0	0	0	0	0	0
Awards	0	0	0	0	0	0	0	0	0	0	0	0
Conversion to full-time	0	0	0	0	0	0	0	0	0	0	0	0
Disciplinary action	0	0	0	0	0	0	0	0	0	0	0	0
Demotion	0	0	0	0	0	0	0	0	0	0	0	0
Reprimand	0	0	0	0	0	0	0	0	0	0	0	0
Suspension	0	0	0	0	0	0	0	0	0	0	0	0
Removal	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0
Duty hours	0	0	0	0	0	0	0	0	0	0	0	0
Evaluation appraisal	0	0	0	0	0	0	0	0	0	0	0	0
Examination/test	0	0	0	0	0	0	0	0	0	0	0	0
Harassment	0	0	0	0	0	0	0	0	0	0	0	0
Nonsexual	0	0	0	0	0	0	0	0	0	0	0	0
Sexual	0	0	0	0	0	0	0	0	0	0	0	0
Medical examination	0	0	0	0	0	0	0	0	0	0	0	0
Pay (including overtime)	0	0	0	0	0	0	0	0	0	0	0	0
Promotion/nonselection	0	0	0	0	0	0	0	0	0	0	0	0
Reassignment	0	0	0	0	0	0	0	0	0	0	0	0
Denied	0	0	0	0	0	0	0	0	0	0	0	0
Directed	0	0	0	0	0	0	0	0	0	0	0	0
Reasonable accommodation	0	0	0	0	0	0	0	0	0	0	0	0
Reinstatement	0	0	0	0	0	0	0	0	0	0	0	0
Retirement	0	0	0	0	0	0	0	0	0	0	0	0
Termination	0	0	0	0	0	0	0	0	0	0	0	0
Terms/conditions of employment	0	0	0	0	0	0	0	0	0	0	0	0
Time and attendance	0	0	0	0	0	0	0	0	0	0	0	0
Training	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0

Pending complaints filed in previous fiscal years by status	Comparative data Previous fiscal year data					Fiscal Year 2012
	2007	2008	2009	2010	2011	10/2011 - 12/2011
Total complaints from previous fiscal years	4	1	2	2	7	8
Number complaints pending						
Investigation	0	0	0	0	0	1
Hearing	3	0	1	1	6	7
Final action	0	1	0	0	0	0
Appeal with EEOC Office of Federal Operations	1	0	1	1	1	0

Complaint investigations	Comparative data Previous fiscal year data					Fiscal Year 2012
	2007	2008	2009	2010	2011	10/2011 - 12/2011
Pending complaints where investigations exceed required time frames	0	2	3	0	2	1

For further information, please contact the Diversity and Inclusion Programs Director.

Office Diveristy and Inclusion Director, Stop 156
Board of Governors of the Federal Reserve System
20th and Constitution Avenue, NW
Washington, DC 20551

BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

ADDRESS OFFICIAL CORRESPONDENCE
TO THE BOARD

No FEAR Act Written Training Plan

Submitted by
Board of Governors of the Federal Reserve System

On July 20, 2006, the Office of Personnel Management (OPM) published its final rule implementing the training requirements of the Notification and Federal Employee Antidiscrimination and Retaliation Act (No FEAR Act).

The final rule required each agency to develop a written plan for training all of its employees, including supervisors and managers. The plan must describe:

- The instructional materials and method of the training
- The training schedule, and
- The means of documenting completion of training

On December 28, 2006, the Office of Personnel Management issued the final rule regarding "Implementations of Title II of the No FEAR Act of 2002 – Reporting and Best Practices." Among other things, this final rule requires each agency to provide annual reports on the number of items relating to the agency's implementation of the No FEAR Act, including the agency's written plan.

This document constitutes the Board of Governors of the Federal Reserve System's (Board) No FEAR Act written training Plan.

I. The instructional materials and method of the training

The final rules require federal agencies to train all employees on their rights and remedies under the federal antidiscrimination and whistleblower protection laws. Agencies must have trained all current employees by December 17, 2006, and all new employees within 90 days of hire. Agencies also must provide training to all employees every two years.

With these requirements in mind, the Board contracted with Global Compliance to provide instruction to employees through Global Compliance's interactive online No FEAR Act training course.

As required by the No FEAR Act and the OPM final rule, the Board's online course teaches our employees about their rights and remedies available under the antidiscrimination, retaliation, and whistleblower protection laws. With regard to rights under whistleblowing statutes, the No FEAR Act provides for notification and training only with regard to a federal statute that is inapplicable to employees of the Board. The Federal Deposit Insurance Act and the Inspector

General Act, however prohibit retaliation against Board employees if they make a protected disclosure of any possible violation of any law or regulation, gross mismanagement, a gross waste of funds, and abuse of authority, or a substantial and specific danger to public health or safety. Employees who believe they have experienced retaliation for such whistleblowing activities have been informed via the required Employee Notification of Rights No FEAR Act provision whom to contact.

The No FEAR Act course:

- Provides instruction on all topics required by the No FEAR Act and the OPM final rule
- Provides supervisors and managers additional instruction on their responsibilities
- Allows users to interact with a series of audio-visual scenarios so that they are continually engaged in the learning process

II. The training schedule

The Board has conducted mandatory EEO Training since 1979. We have maintained completion records through our training course data base. The Board has provided two days of EEO training for supervisory and non-supervisor employees. The training consisted of anti-discrimination laws, legal compliance topics, EEO complaint process and retaliation.

Beginning April 2007, access to the online course was provided. Employees completed their initial No FEAR Act training by April 30, 2007. The Board ensures that subsequently hired employees complete training within 90 days from their starting dates.

As required under the No FEAR Act, employees will be provided a refresher courses via blended training, i.e.: Web, classroom, and seminars focusing on the major principles of the previous training and addressing new and developing areas related to No FEAR compliance.

III. The means of documenting completion of training

The Board tracks employees' completion of the online training courses through Global Compliance's learning management system. Global Compliance automatically creates a record of each employee's course completion and enables training coordinator to monitor training activities such as start and incomplete.

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
Ninth Annual No FEAR Act Report
Fiscal Year 2012

The Board of Governors of the Federal Reserve System (Board) hereby submits this Ninth Annual Report pursuant to the requirements of Section 203 of the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (No FEAR Act), Public Law 107-174. In accordance with Section 203(a) of the No FEAR Act and its regulations there-under (5 C.F.R. § 724.302), this Ninth Annual Report is being forwarded to the Speaker of the House of Representatives, the President pro tempore of the Senate, the Committee on Governmental Affairs of the Senate, the Committee on Government Reform of the House of Representatives, each committee of Congress with jurisdiction relating to the Board, the Equal Employment Opportunity Commission, and the Attorney General of the United States, and the Director of the Office of Personnel Management.

The Board responds to the items listed in Section 203(a) (1) through (8) of the No FEAR Act and 5 C.F.R. § 724.302 as follows:

(1) The number of cases in Federal court pending or resolved in each fiscal year and arising under each of the respective provisions of the Federal Antidiscrimination Laws and Whistleblower Protection Laws applicable to the agency as defined in 5 C.F.R. § 724.102 in which an employee, former Federal employee, or applicant alleged a violation(s) of these laws, separating data by the provision(s) of law involved;

Fiscal Year 2012	
Basis of Actions	***Total Cases Pending or Resolved***
29 U.S.C. § 633a (Age)	1
42 U.S.C. § 2000e-16 (Race, Color, Religion, Sex, or National Origin)	2
29 U.S.C. § 206 (Equal Pay Act)	1
29 U.S.C . § 791 (Disability)	1

(2) In the aggregate, for the cases identified in paragraph (1), above, and separated by provision(s) of law involved:

(i) The status or disposition (including resolved);

Fiscal Year 2012	
Status or Disposition:	***Pending***
Basis of Actions	
29 U.S.C. § 633a (Age)	0
42 U.S.C. § 2000e-16 (Race, Color, Religion, Sex, or National Origin)	1
29 U.S.C. § 206 (Equal Pay)	1
29 U.S.C. § 791 (Disabiltiy)	0
	Resolved
Basis of Actions	
29 U.S.C. § 633a (Age)	1
42 U.S.C. § 2000e-16 (Race, Color, Religion, Sex, or National Origin)	1
29 U.S.C. § 791 (Disabiltiy)	1

(ii) The amount of money required to be reimbursed to the Judgment Fund by the agency for payments as defined in 5 C.F.R. § 724.102;

None

(iii) The amount of reimbursement to the Fund for attorney's fees where such fees have been separately designated;

None

(3) In connection with cases identified in paragraph (1), above, the total number of employees in each fiscal year disciplined as defined in 5 C.F.R. § 724.102 and the specific nature, e.g., reprimand, etc., of the disciplinary actions taken, separated by the provision(s) of law involved;

None

(4) The final year-end data about discrimination complaints for each fiscal year that was posted in accordance with Equal Employment Opportunity Regulations at subpart G of title 29 of the Code of Federal Regulations (implementing section 301(c)(1)(b) of the No FEAR Act);

Attached is a copy of the No FEAR Act FY 2012 data posted on the Board's public website.

(5) Whether or not in connection with cases in Federal court, the number of employees in each fiscal year disciplined as defined in 5 C.F.R. § 724.102 in accordance with any agency policy described in paragraph (6), below. The specific nature, e.g., reprimand, etc., of the disciplinary actions taken must be identified.

None

(6) A detailed description of the agency's policy for taking disciplinary action against Federal employees for conduct that is inconsistent with Federal Antidiscrimination Laws and Whistleblower Protection Laws or for conduct that constitutes another prohibited personnel practice revealed in connection with agency investigations of alleged violations of these laws;

The Board does not have a separate policy for disciplining Board employees found to have committed practices referenced above. However, the Board's disciplinary policies, the Disciplinary Actions Policy and the Adverse Action Policy, will be used to discipline such employees.

Under the Disciplinary Actions policy, the Board may take progressive discipline to correct unsatisfactory conduct or other work-related problems. Progressive discipline is the application of graduated actions in disciplinary cases. It can include, where appropriate, oral counseling, written warnings, and suspensions of 14 calendar days or less. Under the Adverse Action Policy, adverse action against an employee may be in the form of discharge, removal, or suspension without pay for a period of more than 14 calendar days, or a reduction in grade or pay.

(7) An analysis of the information provided in paragraphs (1) through (6), above, in conjunction with data provided to the Equal Employment Opportunity Commission in compliance with 29 C.F.R. § 1614. Such analysis must include: (i) An examination of trends; (ii) Causal analysis; (iii) Practical knowledge gained through experience; and (iv) Any actions planned or taken to improve complaint or civil rights programs of the agency with the goal of eliminating discrimination and retaliation in the workplace;

During FY 2012 the Board's EEO staff counseled 54 pre-complaints, of which 12 entered the formal complaint process compared to 58 pre-complaint counseling sessions in FY 2011 with 10 formal complaints filed.

An analysis of complaints filed identified an increase in the following bases: age, race, reprisal and non-sexual harassment. The EEO staff and the Employee Relations staff continue to focus on effective counseling in an attempt to reach resolutions through mediation and facilitated discussions between parties involved.

Also the counselors worked with management and employees to address effective ways to address complaints that did not enter the formal process.

In FY 2012, the Board conducted management training which focused on building respect in a diverse workplace, harassment awareness and prevention, and strategic diversity management competencies. Additional training was also provided on workplace related policies, effective coaching for development and effective communications with a focus on feedback techniques, team building and conflict resolution.

In accordance with the No FEAR Act training requirements, the Board will continue to provide training via web-base and classroom instruction. The Board issued a request for proposal (RFP) for web-based training which will continue the initial training modules and add additional EEO subjects, such as disability accommodations, GINA, and any updates to Federal employment regulations. The responses to the RFP are under review and an award is expected in May 2013.

In accordance with Board procedures, the Board is reviewing and revising employment policies where applicable. Among the policies being updated are Adverse Action, Leave, Reasonable Accommodation, EEO, and Sexual Harassment (to be renamed) Discriminatory Workplace Harassment. The updated policies are scheduled to be released in FY 2013. Updated and revised policies will strengthen the processes and procedures in addressing issues pertaining to EEO and other related workplace disputes, with the objective of decreasing and/or resolving complaints.

Also, included in the Board's on-boarding process, employees will continue to certify receipt and review of the Discriminatory Workplace Harassment which includes sexual harassment. The certifications are maintained by the Diversity and Inclusion office.

(8) For each fiscal year, any adjustment needed or made to the budget of the agency to comply with its Judgment Fund reimbursement obligation(s) incurred under 5 C.F.R. § 724.103.

None

(9) The agency's written plan developed under 5 C.F.R. § 724.203(a) to train its employees.

See attached agency No FEAR Act Training Plan.

Attachments as stated:

FY 2012 No FEAR Act data posting
No FEAR Act Training Plan

No FEAR Act

No FEAR Act Notice

The Notification and Federal Employee Anti-discrimination and Retaliation Act (No FEAR Act) of 2002 increases federal agency accountability for acts of discrimination or reprisal against employees.

The No FEAR Act requires agencies to post on their public web sites statistical data relating to equal employment opportunity complaints filed against the respective agencies.

The Federal Reserve Board's public web site contains statistical data in accordance with the No FEAR Act.

Information updated as of September 30, 2012

Complaint activity	Comparative data Previous fiscal year data					Fiscal Year 2012
	2007	2008	2009	2010	2011	10/2011 - 9/2012
Number of complaints filed	1	2	1	7	10	12
Number of complainants	4	3	3	9	17	23
Repeat filers	0	0	0	0	0	0

Complaints by basis	Comparative data Previous fiscal year data					Fiscal Year 2012
Note: Complaints can be filed alleging multiple bases. The sum of the bases may not equal total complaints filed	2007	2008	2009	2010	2011	10/2011 - 9/2012
Race	2	2	1	6	10	16
Color	0	1	0	1	2	3
Religion	0	1	0	0	0	2
Reprisal	3	1	1	2	5	11
Sex	2	2	1	5	8	11
National origin	1	1	1	2	3	3
Equal Pay Act	0	0	0	0	0	1
Age	2	3	3	6	8	15
Disability	0	1	0	3	2	5
Non EEO	0	0	0	0	0	0

Complaints by issue	Comparative data Previous fiscal year data					Fiscal Year 2012
Note: Complaints can be filed alleging multiple issues. The sum of the issues may not equal total complaints filed	2007	2008	2009	2010	2011	10/2011 - 9/2012
Appointment/hire	0	2	0	0	0	0
Assignment of duties	0	0	0	2	3	4
Awards	0	0	0	0	0	0
Conversion to full-time	0	0	0	0	0	0
Disciplinary action						
Demotion	0	0	0	0	0	0
Reprimand	0	0	0	0	0	1
Removal	0	0	0	2	2	2
Suspension	0	0	0	0	0	0
Other	0	0	0	0	0	1
Duty hours	0	0	0	1	0	0
Evaluation appraisal	1	1	1	1	2	4
Examination/test	0	0	0	0	0	0
Harassment						
Nonsexual	2	2	0	4	8	11
Sexual	0	0	0	1	2	1
Medical examination	0	0	0	0	0	0

Pay (including overtime)	0	0	0	1	1	1
Promotion/nonselection	3	1	2	5	6	10
Reassignment						
Denied	0	0	0	0	0	0
Directed	0	0	0	0	0	0
Reasonable accommodation	0	0	0	1	1	3
Reinstatement	0	0	0	0	0	0
Retirement	0	0	0	0	0	0
Termination	0	0	0	0	2	2
Terms/conditions of employment	0	0	0	2	2	9
Time and attendance	0	0	0	0	0	0
Training	0	0	0	0	0	0
Other	0	0	0	3	4	1

Processing time	Comparative data Previous fiscal year data					Fiscal Year 2012
	2007	2008	2009	2010	2011	10/2011 - 9/2012
Complaints pending during fiscal year						
Average number of days in investigation stage	136	169	209	68	151	133
Average number of days in final action stage	44	0	28	28	36	53
Complaints pending during fiscal year where hearing was requested						
Average number of days in investigation stage	136	137	209	93	183	148
Average number of days in final action stage	44	0	28	28	36	47
Complaints pending during fiscal year where hearing was not requested						
Average number of days in investigation stage	0	0	0	87	0	93
Average number of days in final action stage	0	0	0	62	0	92

Complaints dismissed by agency	Comparative data Previous fiscal year data					Fiscal Year 2012
	2007	2008	2009	2010	2011	10/2011 - 9/2012
Total complaints dismissed by agency	0	0	0	0	1	0
Average days pending prior to dismissal	0	0	0	0	531	0
Complaints withdrawn by complainants						
Total complaints withdrawn by complainants	0	1	0	0	0	1

Total final actions finding discrimination	Comparative data Previous fiscal year data										Fiscal Year 2012	
	2007		2008		2009		2010		2011		10/2011 - 9/2012	
	#	%	#	%	#	%	#	%	#	%	#	%
Total number findings	0		0		0		0		0		0	
Without hearing	0	0	0	0	0	0	0	0	0	0	0	0
With hearing	0	0	0	0	0	0	0	0	0	0	0	0

Findings of discrimination rendered by basis	Comparative data Previous fiscal year data										Fiscal Year 2012	
Note: Complaints can be filed alleging multiple bases. The sum of the bases may not equal total complaints and findings	2007		2008		2009		2010		2011		10/2011 - 9/2012	
	#	%	#	%	#	%	#	%	#	%	#	%
Total number findings	0		0		0		0		0		0	
Race	0	0	0	0	0	0	0	0	0	0	0	0
Color	0	0	0	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0	0	0	0
Reprisal	0	0	0	0	0	0	0	0	0	0	0	0
Sex	0	0	0	0	0	0	0	0	0	0	0	0
National origin	0	0	0	0	0	0	0	0	0	0	0	0
Equal Pay Act	0	0	0	0	0	0	0	0	0	0	0	0
Age	0	0	0	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0	0	0	0
Non EEO	0	0	0	0	0	0	0	0	0	0	0	0
Findings after hearing	0	0	0	0	0	0	0	0	0	0	0	0
Race	0	0	0	0	0	0	0	0	0	0	0	0
Color	0	0	0	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0	0	0	0
Reprisal	0	0	0	0	0	0	0	0	0	0	0	0
Sex	0	0	0	0	0	0	0	0	0	0	0	0
National origin	0	0	0	0	0	0	0	0	0	0	0	0
Equal Pay Act	0	0	0	0	0	0	0	0	0	0	0	0
Age	0	0	0	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0	0	0	0
Non EEO	0	0	0	0	0	0	0	0	0	0	0	0

Findings without hearing	0	0	0	0	0	0	0	0	0	0	0	0
Race	0	0	0	0	0	0	0	0	0	0	0	0
Color	0	0	0	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0	0	0	0
Reprisal	0	0	0	0	0	0	0	0	0	0	0	0
Sex	0	0	0	0	0	0	0	0	0	0	0	0
National origin	0	0	0	0	0	0	0	0	0	0	0	0
Equal Pay Act	0	0	0	0	0	0	0	0	0	0	0	0
Age	0	0	0	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0	0	0	0
Non EEO	0	0	0	0	0	0	0	0	0	0	0	0

Findings of discrimination rendered by issue	**Comparative data Previous fiscal year data**										**Fiscal Year 2012**	
	2007		**2008**		**2009**		**2010**		**2011**		**10/2011 - 9/2012**	
	#	**%**	**#**	**%**	**#**	**%**	**#**	**%**	**#**	**%**		**%**
Total number findings	0		0		0		0		0		0	
Appointment/hire	0	0	0	0	0	0	0	0	0	0	0	0
Assignment of duties	0	0	0	0	0	0	0	0	0	0	0	0
Awards	0	0	0	0	0	0	0	0	0	0	0	0
Conversion to full-time	0	0	0	0	0	0	0	0	0	0	0	0
Disciplinary action	0	0	0	0	0	0	0	0	0	0	0	0
Demotion	0	0	0	0	0	0	0	0	0	0	0	0
Reprimand	0	0	0	0	0	0	0	0	0	0	0	0
Suspension	0	0	0	0	0	0	0	0	0	0	0	0
Removal	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0
Duty hours	0	0	0	0	0	0	0	0	0	0	0	0
Evaluation appraisal	0	0	0	0	0	0	0	0	0	0	0	0
Examination/test	0	0	0	0	0	0	0	0	0	0	0	0
Harassment	0	0	0	0	0	0	0	0	0	0	0	0
Nonsexual	0	0	0	0	0	0	0	0	0	0	0	0
Sexual	0	0	0	0	0	0	0	0	0	0	0	0
Medical examination	0	0	0	0	0	0	0	0	0	0	0	0
Pay (including overtime)	0	0	0	0	0	0	0	0	0	0	0	0
Promotion/nonselection	0	0	0	0	0	0	0	0	0	0	0	0
Reassignment	0	0	0	0	0	0	0	0	0	0	0	0
Denied	0	0	0	0	0	0	0	0	0	0	0	0
Directed	0	0	0	0	0	0	0	0	0	0	0	0
Reasonable accommodation	0	0	0	0	0	0	0	0	0	0	0	0
Reinstatement	0	0	0	0	0	0	0	0	0	0	0	0
Retirement	0	0	0	0	0	0	0	0	0	0	0	0
Termination	0	0	0	0	0	0	0	0	0	0	0	0
Terms/conditions of employment	0	0	0	0	0	0	0	0	0	0	0	0
Time and attendance	0	0	0	0	0	0	0	0	0	0	0	0
Training	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0
Findings after hearing												
Appointment/hire	0	0	0	0	0	0	0	0	0	0	0	0
Assignment of duties	0	0	0	0	0	0	0	0	0	0	0	0
Awards	0	0	0	0	0	0	0	0	0	0	0	0
Conversion to full-time	0	0	0	0	0	0	0	0	0	0	0	0
Disciplinary action	0	0	0	0	0	0	0	0	0	0	0	0
Demotion	0	0	0	0	0	0	0	0	0	0	0	0
Reprimand	0	0	0	0	0	0	0	0	0	0	0	0
Suspension	0	0	0	0	0	0	0	0	0	0	0	0
Removal	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0
Duty hours	0	0	0	0	0	0	0	0	0	0	0	0
Evaluation appraisal	0	0	0	0	0	0	0	0	0	0	0	0
Examination/test	0	0	0	0	0	0	0	0	0	0	0	0
Harassment	0	0	0	0	0	0	0	0	0	0	0	0
Nonsexual	0	0	0	0	0	0	0	0	0	0	0	0
Sexual	0	0	0	0	0	0	0	0	0	0	0	0
Medical examination	0	0	0	0	0	0	0	0	0	0	0	0
Pay (including overtime)	0	0	0	0	0	0	0	0	0	0	0	0
Promotion/nonselection	0	0	0	0	0	0	0	0	0	0	0	0
Reassignment	0	0	0	0	0	0	0	0	0	0	0	0
Denied	0	0	0	0	0	0	0	0	0	0	0	0
Directed	0	0	0	0	0	0	0	0	0	0	0	0
Reasonable accommodation	0	0	0	0	0	0	0	0	0	0	0	0

Reinstatement	0	0	0	0	0	0	0	0	0	0	0	0
Retirement	0	0	0	0	0	0	0	0	0	0	0	0
Termination	0	0	0	0	0	0	0	0	0	0	0	0
Terms/conditions of employment	0	0	0	0	0	0	0	0	0	0	0	0
Time and attendance	0	0	0	0	0	0	0	0	0	0	0	0
Training	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0
Findings without hearing	0	0	0	0	0	0	0	0	0	0	0	0
Appointment/hire	0	0	0	0	0	0	0	0	0	0	0	0
Assignment of duties	0	0	0	0	0	0	0	0	0	0	0	0
Awards	0	0	0	0	0	0	0	0	0	0	0	0
Conversion to full-time	0	0	0	0	0	0	0	0	0	0	0	0
Disciplinary action	0	0	0	0	0	0	0	0	0	0	0	0
Demotion	0	0	0	0	0	0	0	0	0	0	0	0
Reprimand	0	0	0	0	0	0	0	0	0	0	0	0
Suspension	0	0	0	0	0	0	0	0	0	0	0	0
Removal	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0
Duty hours	0	0	0	0	0	0	0	0	0	0	0	0
Evaluation appraisal	0	0	0	0	0	0	0	0	0	0	0	0
Examination/test	0	0	0	0	0	0	0	0	0	0	0	0
Harassment	0	0	0	0	0	0	0	0	0	0	0	0
Nonsexual	0	0	0	0	0	0	0	0	0	0	0	0
Sexual	0	0	0	0	0	0	0	0	0	0	0	0
Medical examination	0	0	0	0	0	0	0	0	0	0	0	0
Pay (including overtime)	0	0	0	0	0	0	0	0	0	0	0	0
Promotion/nonselection	0	0	0	0	0	0	0	0	0	0	0	0
Reassignment	0	0	0	0	0	0	0	0	0	0	0	0
Denied	0	0	0	0	0	0	0	0	0	0	0	0
Directed	0	0	0	0	0	0	0	0	0	0	0	0
Reasonable accommodation	0	0	0	0	0	0	0	0	0	0	0	0
Reinstatement	0	0	0	0	0	0	0	0	0	0	0	0
Retirement	0	0	0	0	0	0	0	0	0	0	0	0
Termination	0	0	0	0	0	0	0	0	0	0	0	0
Terms/conditions of employment	0	0	0	0	0	0	0	0	0	0	0	0
Time and attendance	0	0	0	0	0	0	0	0	0	0	0	0
Training	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0

Pending complaints filed in previous fiscal years by status	Comparative data Previous fiscal year data					Fiscal Year 2012
	2007	2008	2009	2010	2011	10/2011 - 9/2012
Total complaints from previous fiscal years	4	1	2	2	10	13
Number complaints pending						
Investigation	0	0	0	0	0	0
Hearing	3	0	1	1	6	4
Final action	0	1	0	0	0	1
Appeal with EEOC Office of Federal Operations	1	0	1	1	1	2
Class Certification with EEOC Office of Federal Operations	0	0	0	0	1	4
District Court	0	0	0	0	2	2

Complaint investigations	Comparative data Previous fiscal year data					Fiscal Year 2012
	2007	2008	2009	2010	2011	10/2011 - 9/2012
Pending complaints where investigations exceed required time frames	0	2	3	0	2	3

For further information, please contact the Diversity and Inclusion Programs Director.

Office Diveristy and Inclusion Director, Stop 156
Board of Governors of the Federal Reserve System
20th and Constitution Avenue, NW
Washington, DC 20551

BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

ADDRESS OFFICIAL CORRESPONDENCE
TO THE BOARD

No FEAR Act Written Training Plan

Submitted by
Board of Governors of the Federal Reserve System

On July 20, 2006, the Office of Personnel Management (OPM) published its final rule implementing the training requirements of the Notification and Federal Employee Antidiscrimination and Retaliation Act (No FEAR Act).

The final rule required each agency to develop a written plan for training all of its employees, including supervisors and managers. The plan must describe:

- The instructional materials and method of the training
- The training schedule, and
- The means of documenting completion of training

On December 28, 2006, the Office of Personnel Management issued the final rule regarding "Implementations of Title II of the No FEAR Act of 2002 – Reporting and Best Practices." Among other things, this final rule requires each agency to provide annual reports on the number of items relating to the agency's implementation of the No FEAR Act, including the agency's written plan.

This document constitutes the Board of Governors of the Federal Reserve System's (Board) No FEAR Act written training Plan.

I. The instructional materials and method of the training

The final rules require federal agencies to train all employees on their rights and remedies under the federal antidiscrimination and whistleblower protection laws. Agencies must have trained all current employees by December 17, 2006, and all new employees within 90 days of hire. Agencies also must provide training to all employees every two years. With these requirements in mind, the Board will provide instruction to employees through interactive online No FEAR Act training courses.

As required by the No FEAR Act and the OPM final rule, the Board's online course teaches our employees about their rights and remedies available under the antidiscrimination, retaliation, and whistleblower protection laws. With regard to rights under whistleblowing statutes, the No FEAR Act provides for notification and training only with regard to a federal statute that is inapplicable to employees of the Board. The Federal Deposit Insurance Act and the Inspector

General Act, however, prohibit retaliation against Board employees if they make a protected disclosure of any possible violation of any law or regulation, gross mismanagement, a gross waste of funds, and abuse of authority, or a substantial and specific danger to public health or safety. Employees who believe they have experienced retaliation for such whistleblowing activities have been informed via the required Employee Notification of Rights No FEAR Act provision whom to contact.

The No FEAR Act course:

- Provides instruction on all topics required by the No FEAR Act and the OPM final rule
- Provides supervisors and managers additional instruction on their responsibilities
- Allows users to interact with a series of audio-visual scenarios so that they are continually engaged in the learning process
- Provides a quiz based on training content
- Portal for employees to submit questions to the EEO office based on training content

II. The training schedule

The Board has conducted required EEO Training for all employees since 1979. We have maintained completion records through our training course data base. The Board also provides specific EEO training for supervisory employees. The training modules cover anti-discrimination laws, legal compliance, workplace harassment (including sexual harassment), the EEO complaint process and retaliation.

Beginning April 2007, access to the online course was provided. Employees completed their initial No FEAR Act training by April 30, 2007 and subsequent training thereafter. The Board ensures that employees complete training within 90 days from their starting dates.

As required under the No FEAR Act, employees will be provided refresher courses via blended training, i.e.: Web, classroom, and seminars focusing on the major principles of the previous training and addressing new and developing areas related to No FEAR Act compliance.

III. The means of documenting completion of training

The Board tracks employees' completion of the online training courses through a learning management system which automatically creates a record of each employee's course completion and enables the training coordinator to monitor training scheduling and completion.

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
Tenth Annual No FEAR Act Report
Fiscal Year 2013

The Board of Governors of the Federal Reserve System (Board) hereby submits this Tenth Annual Report pursuant to the requirements of Section 203 of the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (No FEAR Act), Public Law 107-174. In accordance with Section 203(a) of the No FEAR Act and its regulations there-under (5 C.F.R. § 724.302), this Tenth Annual Report is being forwarded to the Speaker of the House of Representatives, the President pro tempore of the Senate, the Committee on Governmental Affairs of the Senate, the Committee on Government Reform of the House of Representatives, each committee of Congress with jurisdiction relating to the Board, the Equal Employment Opportunity Commission, and the Attorney General of the United States, and the Director of the Office of Personnel Management.

The Board responds to the items listed in Section 203(a) (1) through (8) of the No FEAR Act and 5 C.F.R. § 724.302 as follows:

(1) The number of cases in Federal court pending or resolved in each fiscal year and arising under each of the respective provisions of the Federal Antidiscrimination Laws and Whistleblower Protection Laws applicable to the agency as defined in 5 C.F.R. § 724.102 in which an employee, former Federal employee, or applicant alleged a violation(s) of these laws, separating data by the provision(s) of law involved;

Fiscal Year 2013	
Basis of Actions	***Total Cases Pending or Resolved***
29 U.S.C. § 633a (Age)	0
42 U.S.C. § 2000e-16 (Race, Color, Religion, Sex, or National Origin)	1
29 U.S.C. § 206 (Equal Pay Act)	1
29 U.S.C . § 791 (Disability)	0

(2) In the aggregate, for the cases identified in paragraph (1), above, and separated by provision(s) of law involved:

(i) The status or disposition (including resolved);

Basis of Actions	
29 U.S.C. § 633a (Age)	0
42 U.S.C. § 2000e-16 (Race, Color, Religion, Sex, or National Origin)	1
29 U.S.C. § 206 (Equal Pay)	1
29 U.S.C. § 791 (Disabiltiy)	0
	Resolved
Basis of Actions	
29 U.S.C. § 633a (Age)	0
42 U.S.C. § 2000e-16 (Race, Color, Religion, Sex, or National Origin)	0
29 U.S.C. § 791 (Disability)	0

(ii) The amount of money required to be reimbursed to the Judgment Fund by the agency for payments as defined in 5 C.F.R. § 724.102;

None

(iii) The amount of reimbursement to the Fund for attorney's fees where such fees have been separately designated;

None

(3) In connection with cases identified in paragraph (1), above, the total number of employees in each fiscal year disciplined as defined in 5 C.F.R. § 724.102 and the specific nature, e.g., reprimand, etc., of the disciplinary actions taken, separated by the provision(s) of law involved;

None

(4) The final year-end data about discrimination complaints for each fiscal year that was posted in accordance with Equal Employment Opportunity Regulations at subpart G of title 29 of the Code of Federal Regulations (implementing section 301(c)(1)(b) of the No FEAR Act);

Attached is a copy of the No FEAR Act FY 2013 data posted on the Board's public website.

(5) Whether or not in connection with cases in Federal court, the number of employees in each fiscal year disciplined as defined in 5 C.F.R. § 724.102 in accordance with any agency policy described in paragraph (6), below. The

specific nature, e.g., reprimand, etc., of the disciplinary actions taken must be identified.

None

(6) A detailed description of the agency's policy for taking disciplinary action against Federal employees for conduct that is inconsistent with Federal Antidiscrimination Laws and Whistleblower Protection Laws or for conduct that constitutes another prohibited personnel practice revealed in connection with agency investigations of alleged violations of these laws;

The Board does not have a separate policy for disciplining Board employees found to have committed practices referenced above. However, the Board's disciplinary policies; the Disciplinary Actions Policy and the Adverse Action Policy are used to discipline such employees.

Under the Disciplinary Actions policy, the Board may take progressive discipline to correct unsatisfactory conduct or other work-related matters. Progressive discipline is a process for dealing with job-related behavior that does not meet the Board's expected and communicated performance standards. The primary purpose for progressive discipline is to provide the employee aware of an opportunity to improve conduct or performance issues. It involves increasingly formal efforts to provide feedback to the employee so he or she can correct the problem. It can include, where appropriate, oral counseling, written warnings, and suspensions of 14 calendar days or less. Under the Adverse Action Policy, adverse action against an employee may be in the form of discharge, removal, or suspension without pay for a period of more than 14 calendar days or a reduction in grade or pay.

In accordance with Board procedures, the Board reviews and revises employment policies where applicable. The Equal Employment Opportunity, Discriminatory Workplace Harassment and Reasonable Accommodation policies are among the policies implemented or updated in fiscal year 2013. The updated policies strengthen and clarify the processes and procedures in addressing matters that pertain to EEO and other related workplace issues in order to avoid, decrease and/or resolve complaints. The Board informed employees of policy updates through the internal website and new employees certify receipt of the Workplace Harassment policy during the on-boarding process. Certifications are maintained by the Diversity and Inclusion office.

(7) An analysis of the information provided in paragraphs (1) through (6), above, in conjunction with data provided to the Equal Employment Opportunity Commission in compliance with 29 C.F.R. § 1614. Such analysis must include: (i) An examination of trends; (ii) Causal analysis; (iii) Practical knowledge gained through experience; and (iv) Any actions planned or taken to improve

complaint or civil rights programs of the agency with the goal of eliminating discrimination and retaliation in the workplace;

EEO Complaint Activity

In accordance with 29 C.F.R § 1614.105(d), pre-complaint counseling cases were completed timely within 30 calendar days, unless an extension was granted. During FY 2013, the Board's EEO counselors counseled 146 pre-complaints, of which 6 entered the formal complaint process. In FY 2012, 54 pre-complaint counseling sessions were held and 12 formal complaints were filed. Thus, while the number of pre-complaint counseling sessions increased, the number of formal EEO complaints filed in fiscal year 2013 decreased by 50 percent compared to fiscal year 2012.

The EEO and Employee Relations staff continue to collaborate to reach resolutions through mediation and facilitated discussions between parties involved. Also, counselors closely interacted with employees and management to effectively promote resolutions for complaints that did not enter the formal process.

EEO Investigations

In fiscal year 2013, the average number of days EEO formal complaints were in the investigative stage increased to 228 days, compared to 133 in FY 2012. Much of the increase in processing time was due to amendments of pending complaints, which required additional investigation. To address this issue, the Board has established the following procedure to improve the investigation processing time:

- Investigators are required to submit a status report of investigation within 45 days of the assignment.

- When a complaint is amended, the Office of Diversity and Inclusion will adjust the timeframe for completing the investigation based on the number of amended claims accepted by the Board for investigation.

Training

In fiscal year 2013, the Board continued to provide Workplace Harassment Prevention training and counseling services to divisions addressing EEO and/or diversity issues and trends. Other diversity-related training included Conflict Resolution, Management Awareness, Fierce Conversations, and Micro Inequities Workshop.

In compliance with the training requirements of the No FEAR Act, the Board has contracted with Navex Global to provide No FEAR web-based training in 2014. This training is required for all employees. The segments will cover EEO compliance, disability and accommodations and discriminatory workplace harassment.

(8) For each fiscal year, any adjustment needed or made to the budget of the agency to comply with its Judgment Fund reimbursement obligation(s) incurred under 5 C.F.R. § 724.103.

None

(9) The agency's written plan developed under 5 C.F.R. § 724.203(a) to train its employees.

See attached agency No FEAR Act Training Plan.

Attachments as stated:

FY 2013 No FEAR Act data posting
No FEAR Act Training Plan

No FEAR Act

No FEAR Act Notice

The Notification and Federal Employee Anti-discrimination and Retaliation Act (No FEAR Act) of 2002 increases federal agency accountability for acts of discrimination or reprisal against employees.

The No FEAR Act requires agencies to post on their public web sites statistical data relating to equal employment opportunity complaints filed against the respective agencies.

The Federal Reserve Board's public web site contains statistical data in accordance with the No FEAR Act.

Information updated as of September 30, 2013

Complaint activity	Comparative data Previous fiscal year data					Fiscal Year 2013
	2008	2009	2010	2011	2012	10/2012 - 9/2013
Number of complaints filed	2	1	7	10	12	6
Number of complainants	3	3	9	17	23	18
Repeat filers	0	0	0	0	0	0

Complaints by basis	Comparative data Previous fiscal year data					Fiscal Year 2013
Note: Complaints can be filed alleging multiple bases. The sum of the bases may not equal total complaints filed	2008	2009	2010	2011	2012	10/2012 - 9/2013
Race	2	1	6	10	16	15
Color	1	0	1	2	3	4
Religion	1	0	0	0	2	2
Reprisal	1	1	2	5	11	8
Sex	2	1	5	8	11	11
National origin	1	1	2	3	3	1
Equal Pay Act	0	0	0	0	1	3
Age	3	3	6	8	15	9
Disability	1	0	3	2	5	2
Non EEO	0	0	0	0	0	0

Complaints by issue	Comparative data Previous fiscal year data					Fiscal Year 2013
Note: Complaints can be filed alleging multiple issues. The sum of the issues may not equal total complaints filed	2008	2009	2010	2011	2012	10/2012 - 9/2013
Appointment/hire	2	0	0	0	0	0
Assignment of duties	0	0	2	3	4	4
Awards	0	0	0	0	0	0
Conversion to full-time	0	0	0	0	0	0
Disciplinary action						
Demotion	0	0	0	0	0	0
Reprimand	0	0	0	0	1	2
Removal	0	0	2	2	2	1
Suspension	0	0	0	0	0	0
Other	0	0	0	0	1	1
Duty hours	0	0	1	0	0	0
Evaluation appraisal	1	1	1	2	4	3
Examination/test	0	0	0	0	0	0
Harassment						
Nonsexual	2	0	4	8	11	10
Sexual	0	0	1	2	1	1
Medical examination	0	0	0	0	0	0

Pay (including overtime)	0	0	1	1	1	3
Promotion/nonselection	1	2	5	6	10	10
Reassignment						
Denied	0	0	0	0	0	0
Directed	0	0	0	0	0	0
Reasonable accommodation	0	0	1	1	3	2
Reinstatement	0	0	0	0	0	0
Retirement	0	0	0	0	0	0
Termination	0	0	0	2	2	0
Terms/conditions of employment	0	0	2	2	9	5
Time and attendance	0	0	0	0	0	0
Training	0	0	0	0	0	1
Other	0	0	3	4	1	2

Processing time	Comparative data Previous fiscal year data					Fiscal Year 2013
	2008	2009	2010	2011	2012	10/2012 - 9/2013
Complaints pending during fiscal year						
Average number of days in investigation stage	169	209	68	151	133	228
Average number of days in final action stage	0	28	28	36	53	26
Complaints pending during fiscal year where hearing was requested						
Average number of days in investigation stage	137	209	93	183	148	151
Average number of days in final action stage	0	28	28	36	47	27
Complaints pending during fiscal year where hearing was not requested						
Average number of days in investigation stage	0	0	87	0	93	220
Average number of days in final action stage	0	0	62	0	92	24

Complaints dismissed by agency	Comparative data Previous fiscal year data					Fiscal Year 2013
	2008	2009	2010	2011	2012	10/2012 - 9/2013
Total complaints dismissed by agency	0	0	0	1	0	1
Average days pending prior to dismissal	0	0	0	531	0	27
Complaints withdrawn by complainants						
Total complaints withdrawn by complainants	0	1	0	0	1	1

Total final actions finding discrimination	Comparative data Previous fiscal year data										Fiscal Year 2013	
	2008		20009		2010		2011		2012		10/2012 - 9/2013	
	#	%	#	%	#	%	#	%	#	%	#	%
Total number findings	0		0		0		0		0		0	
Without hearing	0	0	0	0	0	0	0	0	0	0	0	0
With hearing	0	0	0	0	0	0	0	0	0	0	0	0

Findings of discrimination rendered by basis	Comparative data Previous fiscal year data										Fiscal Year 2013	
Note: Complaints can be filed alleging multiple bases. The sum of the bases may not equal total complaints and findings	2008		2009		2010		2011		2012		10/2012 - 9/2013	
	#	%	#	%	#	%	#	%	#	%	#	%
Total number findings	0		0		0		0		0		0	
Race	0	0	0	0	0	0	0	0	0	0	0	0
Color	0	0	0	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0	0	0	0
Reprisal	0	0	0	0	0	0	0	0	0	0	0	0
Sex	0	0	0	0	0	0	0	0	0	0	0	0
National origin	0	0	0	0	0	0	0	0	0	0	0	0
Equal Pay Act	0	0	0	0	0	0	0	0	0	0	0	0
Age	0	0	0	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0	0	0	0
Non EEO	0	0	0	0	0	0	0	0	0	0	0	0
Findings after hearing	0	0	0	0	0	0	0	0	0	0	0	0
Race	0	0	0	0	0	0	0	0	0	0	0	0
Color	0	0	0	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0	0	0	0
Reprisal	0	0	0	0	0	0	0	0	0	0	0	0
Sex	0	0	0	0	0	0	0	0	0	0	0	0
National origin	0	0	0	0	0	0	0	0	0	0	0	0
Equal Pay Act	0	0	0	0	0	0	0	0	0	0	0	0
Age	0	0	0	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0	0	0	0
Non EEO	0	0	0	0	0	0	0	0	0	0	0	0

Findings without hearing	0	0	0	0	0	0	0	0	0	0	0	0
Race	0	0	0	0	0	0	0	0	0	0	0	0
Color	0	0	0	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0	0	0	0
Reprisal	0	0	0	0	0	0	0	0	0	0	0	0
Sex	0	0	0	0	0	0	0	0	0	0	0	0
National origin	0	0	0	0	0	0	0	0	0	0	0	0
Equal Pay Act	0	0	0	0	0	0	0	0	0	0	0	0
Age	0	0	0	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0	0	0	0
Non EEO	0	0	0	0	0	0	0	0	0	0	0	0

Findings of discrimination rendered by issue	**Comparative data Previous fiscal year data**										**Fiscal Year 2013**	
	2008		**2009**		**2010**		**2011**		**2012**		**10/2012 - 9/2013**	
	#	**%**	**#**	**%**	**#**	**%**	**#**	**%**	**#**	**%**		**%**
Total number findings	0		0		0		0		0		0	
Appointment/hire	0	0	0	0	0	0	0	0	0	0	0	0
Assignment of duties	0	0	0	0	0	0	0	0	0	0	0	0
Awards	0	0	0	0	0	0	0	0	0	0	0	0
Conversion to full-time	0	0	0	0	0	0	0	0	0	0	0	0
Disciplinary action	0	0	0	0	0	0	0	0	0	0	0	0
Demotion	0	0	0	0	0	0	0	0	0	0	0	0
Reprimand	0	0	0	0	0	0	0	0	0	0	0	0
Suspension	0	0	0	0	0	0	0	0	0	0	0	0
Removal	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0
Duty hours	0	0	0	0	0	0	0	0	0	0	0	0
Evaluation appraisal	0	0	0	0	0	0	0	0	0	0	0	0
Examination/test	0	0	0	0	0	0	0	0	0	0	0	0
Harassment	0	0	0	0	0	0	0	0	0	0	0	0
Nonsexual	0	0	0	0	0	0	0	0	0	0	0	0
Sexual	0	0	0	0	0	0	0	0	0	0	0	0
Medical examination	0	0	0	0	0	0	0	0	0	0	0	0
Pay (including overtime)	0	0	0	0	0	0	0	0	0	0	0	0
Promotion/nonselection	0	0	0	0	0	0	0	0	0	0	0	0
Reassignment	0	0	0	0	0	0	0	0	0	0	0	0
Denied	0	0	0	0	0	0	0	0	0	0	0	0
Directed	0	0	0	0	0	0	0	0	0	0	0	0
Reasonable accommodation	0	0	0	0	0	0	0	0	0	0	0	0
Reinstatement	0	0	0	0	0	0	0	0	0	0	0	0
Retirement	0	0	0	0	0	0	0	0	0	0	0	0
Termination	0	0	0	0	0	0	0	0	0	0	0	0
Terms/conditions of employment	0	0	0	0	0	0	0	0	0	0	0	0
Time and attendance	0	0	0	0	0	0	0	0	0	0	0	0
Training	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0
Findings after hearing												
Appointment/hire	0	0	0	0	0	0	0	0	0	0	0	0
Assignment of duties	0	0	0	0	0	0	0	0	0	0	0	0
Awards	0	0	0	0	0	0	0	0	0	0	0	0
Conversion to full-time	0	0	0	0	0	0	0	0	0	0	0	0
Disciplinary action	0	0	0	0	0	0	0	0	0	0	0	0
Demotion	0	0	0	0	0	0	0	0	0	0	0	0
Reprimand	0	0	0	0	0	0	0	0	0	0	0	0
Suspension	0	0	0	0	0	0	0	0	0	0	0	0
Removal	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0
Duty hours	0	0	0	0	0	0	0	0	0	0	0	0
Evaluation appraisal	0	0	0	0	0	0	0	0	0	0	0	0
Examination/test	0	0	0	0	0	0	0	0	0	0	0	0
Harassment	0	0	0	0	0	0	0	0	0	0	0	0
Nonsexual	0	0	0	0	0	0	0	0	0	0	0	0
Sexual	0	0	0	0	0	0	0	0	0	0	0	0
Medical examination	0	0	0	0	0	0	0	0	0	0	0	0
Pay (including overtime)	0	0	0	0	0	0	0	0	0	0	0	0
Promotion/nonselection	0	0	0	0	0	0	0	0	0	0	0	0
Reassignment	0	0	0	0	0	0	0	0	0	0	0	0
Denied	0	0	0	0	0	0	0	0	0	0	0	0
Directed	0	0	0	0	0	0	0	0	0	0	0	0
Reasonable accommodation	0	0	0	0	0	0	0	0	0	0	0	0

Reinstatement	0	0	0	0	0	0	0	0	0	0	0	0
Retirement	0	0	0	0	0	0	0	0	0	0	0	0
Termination	0	0	0	0	0	0	0	0	0	0	0	0
Terms/conditions of employment	0	0	0	0	0	0	0	0	0	0	0	0
Time and attendance	0	0	0	0	0	0	0	0	0	0	0	0
Training	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0
Findings without hearing	0	0	0	0	0	0	0	0	0	0	0	0
Appointment/hire	0	0	0	0	0	0	0	0	0	0	0	0
Assignment of duties	0	0	0	0	0	0	0	0	0	0	0	0
Awards	0	0	0	0	0	0	0	0	0	0	0	0
Conversion to full-time	0	0	0	0	0	0	0	0	0	0	0	0
Disciplinary action	0	0	0	0	0	0	0	0	0	0	0	0
Demotion	0	0	0	0	0	0	0	0	0	0	0	0
Reprimand	0	0	0	0	0	0	0	0	0	0	0	0
Suspension	0	0	0	0	0	0	0	0	0	0	0	0
Removal	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0
Duty hours	0	0	0	0	0	0	0	0	0	0	0	0
Evaluation appraisal	0	0	0	0	0	0	0	0	0	0	0	0
Examination/test	0	0	0	0	0	0	0	0	0	0	0	0
Harassment	0	0	0	0	0	0	0	0	0	0	0	0
Nonsexual	0	0	0	0	0	0	0	0	0	0	0	0
Sexual	0	0	0	0	0	0	0	0	0	0	0	0
Medical examination	0	0	0	0	0	0	0	0	0	0	0	0
Pay (including overtime)	0	0	0	0	0	0	0	0	0	0	0	0
Promotion/nonselection	0	0	0	0	0	0	0	0	0	0	0	0
Reassignment	0	0	0	0	0	0	0	0	0	0	0	0
Denied	0	0	0	0	0	0	0	0	0	0	0	0
Directed	0	0	0	0	0	0	0	0	0	0	0	0
Reasonable accommodation	0	0	0	0	0	0	0	0	0	0	0	0
Reinstatement	0	0	0	0	0	0	0	0	0	0	0	0
Retirement	0	0	0	0	0	0	0	0	0	0	0	0
Termination	0	0	0	0	0	0	0	0	0	0	0	0
Terms/conditions of employment	0	0	0	0	0	0	0	0	0	0	0	0
Time and attendance	0	0	0	0	0	0	0	0	0	0	0	0
Training	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0

Pending complaints filed in previous fiscal years by status	Comparative data Previous fiscal year data					Fiscal Year 2013
	2008	2009	2010	2011	2012	10/2012 - 9/2013
Total complaints from previous fiscal years	1	2	2	10	13	14
Number complaints pending						
Investigation	0	0	0	0	0	4
Hearing	0	1	1	6	4	7
Final action	1	0	0	0	1	0
Appeal with EEOC Office of Federal Operations	0	1	1	1	2	2
Class Certification with EEOC Office of Federal Operations	0	0	0	1	4	0
District Court	0	0	0	2	2	1

Complaint investigations	Comparative data Previous fiscal year data					Fiscal Year 2013
	2008	2009	2010	2011	2012	10/2012 - 9/2013
Pending complaints where investigations exceed required time frames	2	3	0	2	3	8

For further information, please contact the Diversity and Inclusion Programs Director.

Office Diveristy and Inclusion Director, Stop 156
Board of Governors of the Federal Reserve System
20th and Constitution Avenue, NW
Washington, DC 20551

BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

ADDRESS OFFICIAL CORRESPONDENCE
TO THE BOARD

No FEAR Act Written Training Plan

Submitted by
Board of Governors of the Federal Reserve System

On July 20, 2006, the Office of Personnel Management (OPM) published its final rule implementing the training requirements of the Notification and Federal Employee Antidiscrimination and Retaliation Act ("No FEAR Act").

The final rule required each agency to develop a written plan for training all of its employees, including supervisors and managers. The plan must describe:

- The instructional materials and method of the training
- The training schedule, and
- The means of documenting completion of training

On December 28, 2006, the Office of Personnel Management issued the final rule regarding "Implementations of Title II of the No FEAR Act of 2002 – Reporting and Best Practices." Among other things, this final rule requires each agency to provide annual reports on the number of items relating to the agency's implementation of the No FEAR Act, including the agency's written plan.

This document constitutes the Board of Governors of the Federal Reserve System's (Board) No FEAR Act written training Plan.

I. The instructional materials and method of the training

The final rules require federal agencies to train all employees on their rights and remedies under the federal antidiscrimination and whistleblower protection laws. Agencies must have trained all current employees by December 17, 2006, and all new employees within 90 days of hire. Agencies also must provide training to all employees every two years.

With these requirements in mind, the Board contracted with Brightline Compliance, LLC to provide instruction to employees through Brightline's interactive online No FEAR Act training course.

As required by the No FEAR Act and the OPM final rule, the Board's online course teaches our employees about their rights and remedies available under the antidiscrimination, retaliation, and whistleblower protection laws. With regard to rights under whistleblowing statutes, the No FEAR Act provides for notification and training only with regard to a federal statute that is inapplicable to employees of the Board. The Federal Deposit Insurance Act and the Inspector

General Act, however prohibit retaliation against Board employees if they make a protected disclosure of any possible violation of any law or regulation, gross mismanagement, a gross waste of funds, and abuse of authority, or a substantial and specific danger to public health or safety. Employees who believe they have experienced retaliation for such whistleblowing activities have been informed via the required "Employee Notification of Rights" No FEAR Act provision whom to contact.

The No FEAR Act course:

- Provides instruction on all topics required by the No FEAR Act and the OPM final rule
- Provides supervisors and managers additional instruction on their responsibilities
- Allows users to interact with a series of audio-visual scenarios so that they are continually engaged in the learning process

II. The training schedule

The Board has conducted mandatory EEO Training since 1979. We have maintained completion records through our training course data base. The Board has provided two days of EEO training for supervisory and non-supervisor employees. The training consisted of anti-discrimination laws, legal compliance topics, EEO complaint process and retaliation.

Beginning April 2007, access to the online course was provided. Employees completed their initial No FEAR Act training by April 30, 2007. The Board ensures that subsequently hired employees complete training within 90 days from their starting dates.

As required under the No FEAR Act, employees will be provided a refresher courses via blended training, i.e.: Web, classroom, and seminars focusing on the major principles of the previous training and addressing new and developing areas related to No FEAR compliance.

III. The means of documenting completion of training

The Board tracks employees' completion of the online training courses through a learning management system which automatically creates a record of each employee's course completion and enables training coordinator to monitor training activities such as start and incomplete.

PSSC: See E.3.PRG wp Non-EEO Complaints - Data Analyses.

Source: Allison Dichoso, Employee Relations Supervisor, 202-452-6402

GLOSSARY

1. *Adverse Actions* – a discharge, removal, suspension without pay for a period of more than 14 calendar days, or a reduction in grade or base pay against an employee. All other actions do not constitute adverse actions. In addition, adverse actions do not include:

    - actions the employee voluntarily agrees to or takes on his or her own behalf;
    - actions that reduce an employee's variable pay, bonuses, cash awards, or any other type of pay that does not constitute base pay;
    - any action taken under the Board's Workforce Reduction policy (including separation or reduction in grade or pay); or
    - actions taken to carry out a transfer of function(s) required by law or other actions required by applicable law

2. *AWA* – an alternative work arrangement (AWA) is a work arrangement that varies from the traditional five-day workweek schedule. Options include, but are not limited to, compressed work schedules, flextime, job sharing, voluntary part-time employment, and telecommuting.

3. *Benefits* – Any ER issue involving equity or fairness in administration of benefits. Benefits include both financial and convenience benefits:

    - **Financial Benefits**: The Board provides its employees with subsidized health (i.e., medical, dental, vision) benefits, a savings plan (Thrift Plan) with matching contributions, a defined benefit retirement plan, paid leave, tuition assistance, a transportation subsidy, and other benefits as appropriate to the market.
    - **Convenience Benefits:** The Board also provides its employees non-financial benefits that contribute to employee health, well-being, and efficiency. They include medical services, a subsidized cafeteria, a fitness center, a credit union with an automated teller machine, and a convenience store.

4. *BOA (ER)* – A Basic Ordering Agreement for ER is a contract with an external vendor for Job Coaching or Mediation services that sets forth the price schedule for specified services:

    - **Job Coaching:** Management may hire a job coach to help an employee (supervisory or non-supervisory) develop and improve skills. Job coaches may be requested when management notes performance deficiencies or when an employee simply wants to improve his/her own skills with assistance from an external source.
    - **Mediation:** Staff or management may request a neutral, third party mediator to assist in resolving workplace concerns and issues. The mediator's role is to promote an open dialogue between participants, assist them in defining the problem, and help them find a mutually beneficial solution.

5. *Compensation* - Any ER issue involving pay equity or pay fairness arising out of the Board's cash compensation programs (including (1) base salaries and the guidelines used to set and adjust salaries, and (2) additional pay programs, such as cash awards, variable pay plans, sign-on and retention bonuses, project incentives or pay as described in the Overtime and Other Forms of Premium Pay Policy.)

6. *Disability* –Any ER matter or complaint initiated because of an employee's stated medical disability and that is not primarily involved with the processing of an informal accommodation or formal reasonable accommodation under the Board's Reasonable Accommodation Policy. With respect to an individual, a disability is a physical or mental impairment that substantially limits one or more of such individual's "major life activities," such as walking, seeing, hearing, speaking, performing manual tasks, eating, sleeping, working, operating major bodily functions, etc. An impairment that is episodic or in remission may constitute a disability if it would substantially limit a major life activity when active.

7. *Disciplinary Actions* – a documented oral counseling, a written warning or suspension of 14 calendar days or less. Disciplinary Actions only address conduct-related problems and provide for less-severe disciplinary measures than the Adverse Action Policy and Procedures.

8. *EAP* – The Employee Assistance Program (EAP) is a voluntary, confidential resource for support when you are experiencing any personal difficulty. Objective advice, practical problem-solving, and information are offered to help you resolve problems. Serious problems may consume an employee's attention, causing job efficiency to suffer. The EAP can help employees resolve such problems early, before they affect job performance. ER may collaborate with an employee and the EAP to assist in the resolution of personal difficulties.

9. *EEO* – The Board's policy is to provide *Equal Employment Opportunity* in employment for all persons, including discrimination involving race, color, religion, sex, national origin, age, disability, genetic information, employment applications, memberships, service in the uniformed services, and sexual orientation. ER may receive initial complaints of prohibited discrimination under the EEO policy. ER may assist the Office of Diversity & Inclusion to investigate claims of discrimination or harassment.

10. *Fit for Duty* – The Board's Mandatory Fitness Program is applicable to employees in positions that affect the public safety and to applicants seeking such positions. The Mandatory Fitness Program is designed to ensure that employees and applicants subject to this policy meet the physical, physiological, and mental fitness standards applicable to their jobs. The following employees are subject to periodic medical examinations:

    - an employee who is authorized under the Board's law enforcement authority to carry a firearm; or
    - an employee in any other position that affects the public safety

11. *FMLA* – The Family and Medical Leave Act of 1993 (FMLA) is a United States federal law requiring covered employers to provide employees job-protected and unpaid leave for qualified medical and family reasons. Qualified medical and family reasons include: personal or family illness, family military leave, pregnancy, adoption, or the foster care placement of a child.

12. *Harassment* – Discriminatory harassment is verbal or physical conduct that demeans or shows hostility or aversion toward an individual because of his or her race, color, religion, sex, gender, national origin, age (40 or older), disability, genetic information, or because of retaliation for engaging in protected activity. Discriminatory harassment is against the law when it has the purpose or effect of unreasonably interfering with an individual's work performance or of creating an intimidating, hostile, or offensive working environment. ER may assist the Office of Diversity & Inclusion to investigate claims of discrimination or harassment.

13. *Leave (Violations)* – All employees must ensure that they work a full work day or receive approval to be absent and accurately report and account for leave taken to cover such absences. Common Leave Violations include an employee's failure to follow procedures for requesting leave and for getting leave approved, like tardiness and call-offs, that may result in a period of unauthorized leave without pay, as well as making false statements in connection with a leave request.

14. *Leave (Processing)* – All leave matters not involving violations of the Leave Policy, including leave administration matters like FMLA requests (now administered by the Employee Life function of HR), that involve the granting of leave under the Board's Leave Policy.

15. *PEP* – The Board's provisional employment period for newly hired employees is two years, except as noted below. This time period permits supervisors and the division to determine the employee's overall suitability for continued employment. A provisional employee may be separated from employment at the will of the Board for any reason that is not unlawful. A provisional employee has no right to continued employment.

16. *Performance/PMP* – Includes ER matters related to an employee's performance problems under the Board's 3Cs Program and the Board's PMP Policy.

17. *Rehab Act* – Any matter involving an informal accommodation or a Reasonable Accommodation under the Rehabilitation Act of 1973. A reasonable accommodation includes any change in the work environment or in the way things are customarily done that would not create an undue hardship for the Board and would enable (1) a qualified individual with a disability to perform the essential functions of his or her job, (2) an employee with a disability to enjoy the equal benefits and privileges of employment, and/or (3) an individual with a disability to apply for a job at the Board.

    - an **informal accommodation** is an accommodation the Board may make in the ordinary course of its business, such as an ergonomic equipment adjustment, whether or not the employee is disabled under the Rehabilitation Act.
    - a **formal reasonable accommodation** is an accommodation the Board would make as a result of its legal obligation to provide reasonable accommodations to qualified individuals with disabilities under the Rehabilitation Act.

18. *Selection* – Any employee complaint involving the Board's internal hiring practices as governed by the Board's Vacant-Position Posting Policy.

19. *Suitability* – Generally, suitability means fitness or eligibility to perform services for the Board, as evidenced by an individual's past and present conduct. An individual is not suitable to perform services for the Board if the Board has reason to believe that he or she will not protect and promote the integrity, efficiency, and security of its operations. Suitability determinations often occur at the beginning of an individual's employment, when the Board receives the results of its initial background investigation. However, they may also occur at any time, including well after completion of an initial background investigation, if the Board becomes aware of information that presents a concern about an individual's suitability to perform Board work. Employees who fail to meet the Board's suitability requirements may be disciplined, transferred, suspended, terminated, limited in their ability to access sensitive or classified information, or subject to other actions that the Board deems appropriate to remedy its suitability concern.

20. *Work Related* – The Work Related case type includes work related problems like employee complaints or questions regarding unfair treatment on the basis of conduct or reasons that do not adversely affect the employee's performance and that are not covered under existing laws regarding discrimination. The Board's Adjusting Work Related Problems Policy covers these work related problems. In addition, the Work Related case type may include workplace conflict involving two or more staff persons, as well as conflict between staff and management. ER incorporates dispute resolution strategies to address workplace conflicts. Unlike the ER BOA case type, which is used whenever an external consultant is used to perform job coaching or mediation services, the Work Related case type may not involve the use of an external consultant.

21. *Worker Compensation* – Any matter involving an employee who suffers from a work-related illness or injury and is therefore unable to perform the full range of duties of his or her position and who is receiving workers' compensation. The Board's Return-to-Work Policy covers the administration of worker's compensation cases.

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

DIVISION OF RESEARCH AND STATISTICS

PROPOSED JULY, 2009

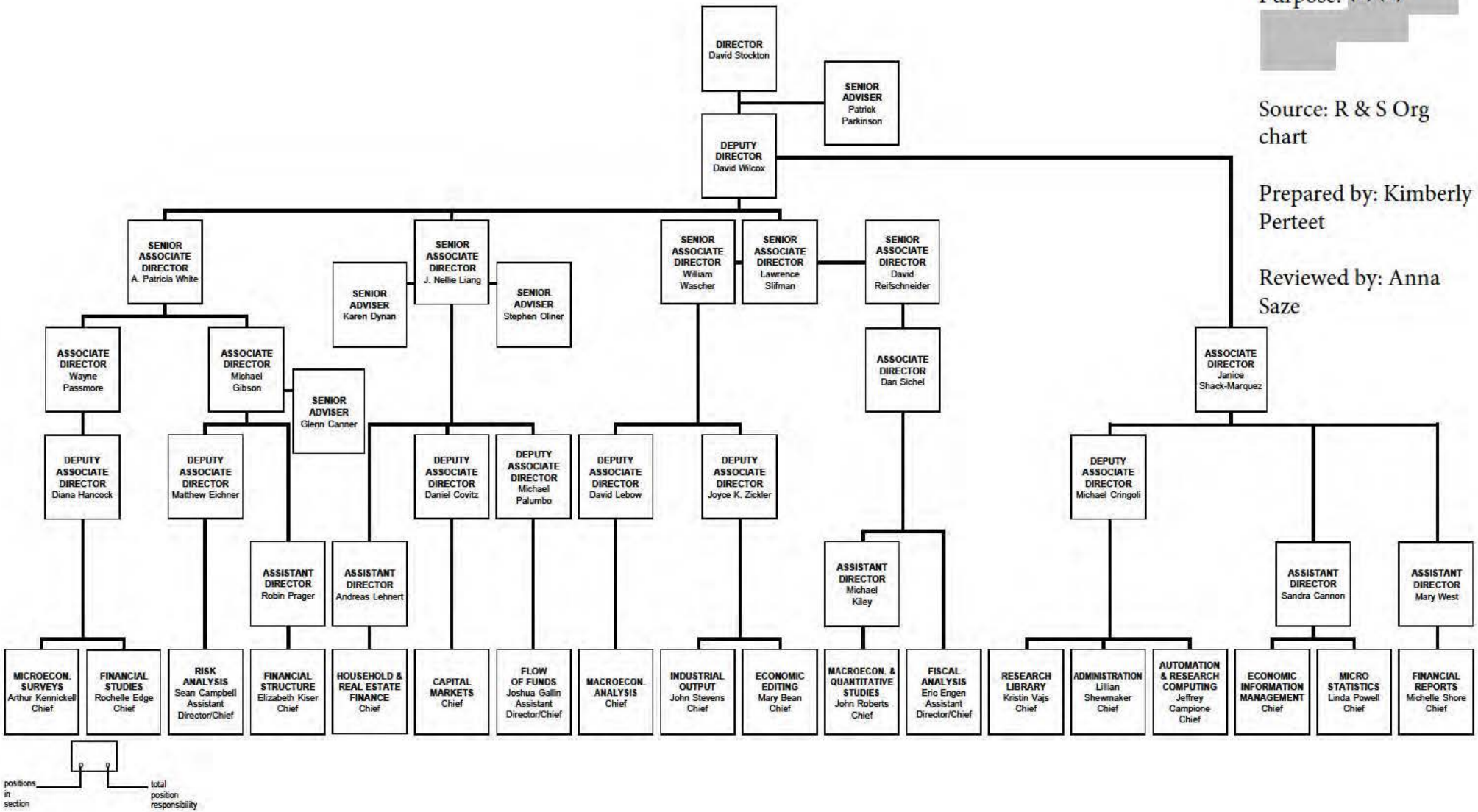
PSSC: E.2 PRG

Purpose: (b) (5)

Source: R & S Org chart

Prepared by: Kimberly Perteet

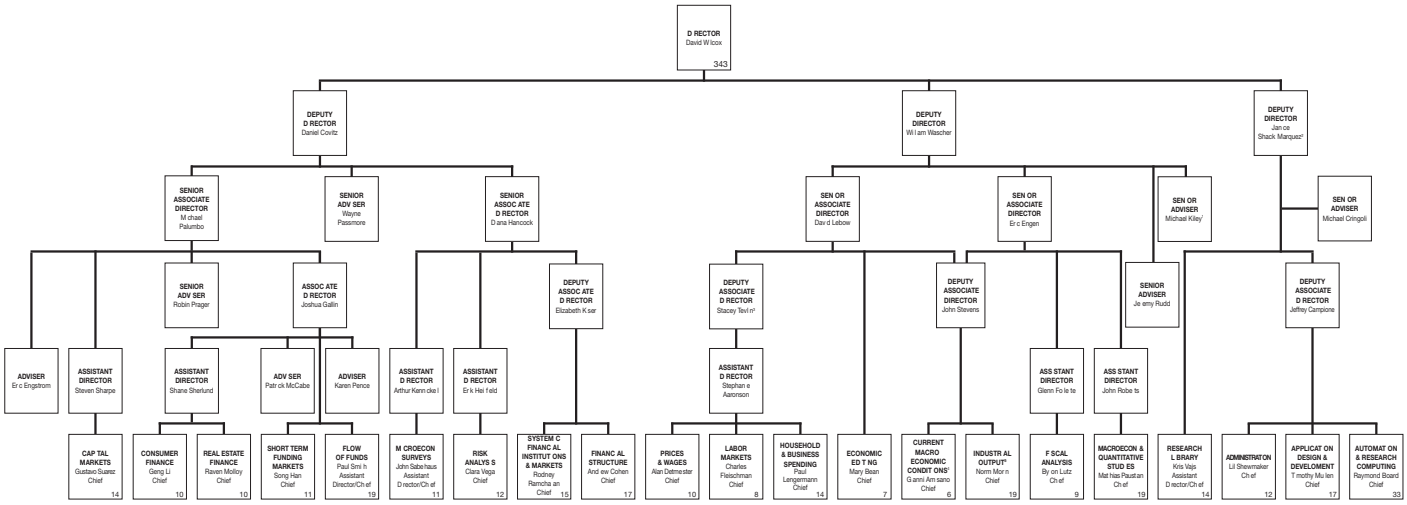
Reviewed by: Anna Saze



BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

DIVISION OF RESEARCH AND STATISTICS

January 9 , 2015



1 Mr K ley also has Senior Associate Director respons b l ty in OFS

2 Ms Shack Marquez also has Deputy D rector respons bi ity n MA

3 Ms Tev in is on detail to the Of ice of Board Members working with the Vice Cha r

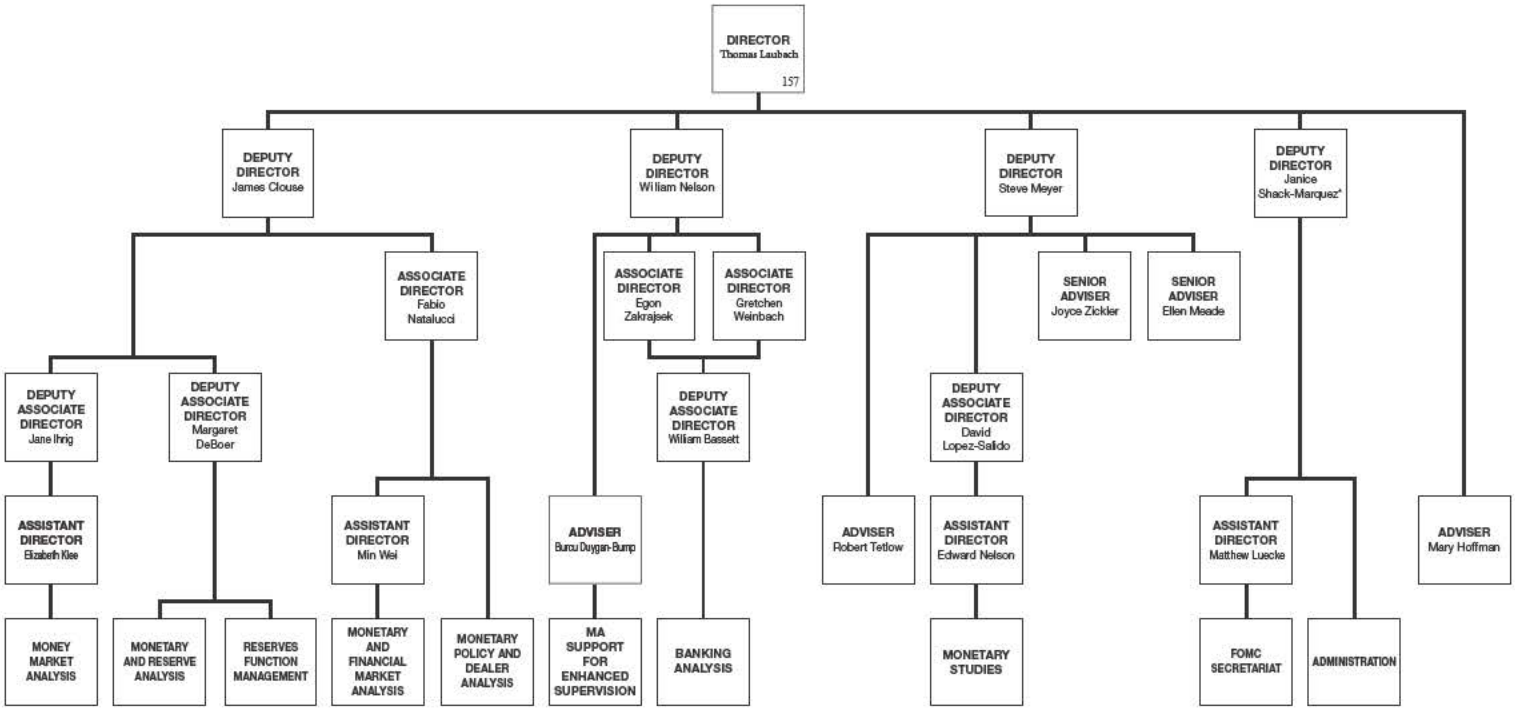
4 CMC w ll repo t through Mr Stevens to Mr Lebow and Mr Engen

5 IO w l eport hrough Mr Stevens to Mr Engen

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

DIVISION OF MONETARY AFFAIRS

JANUARY, 2015

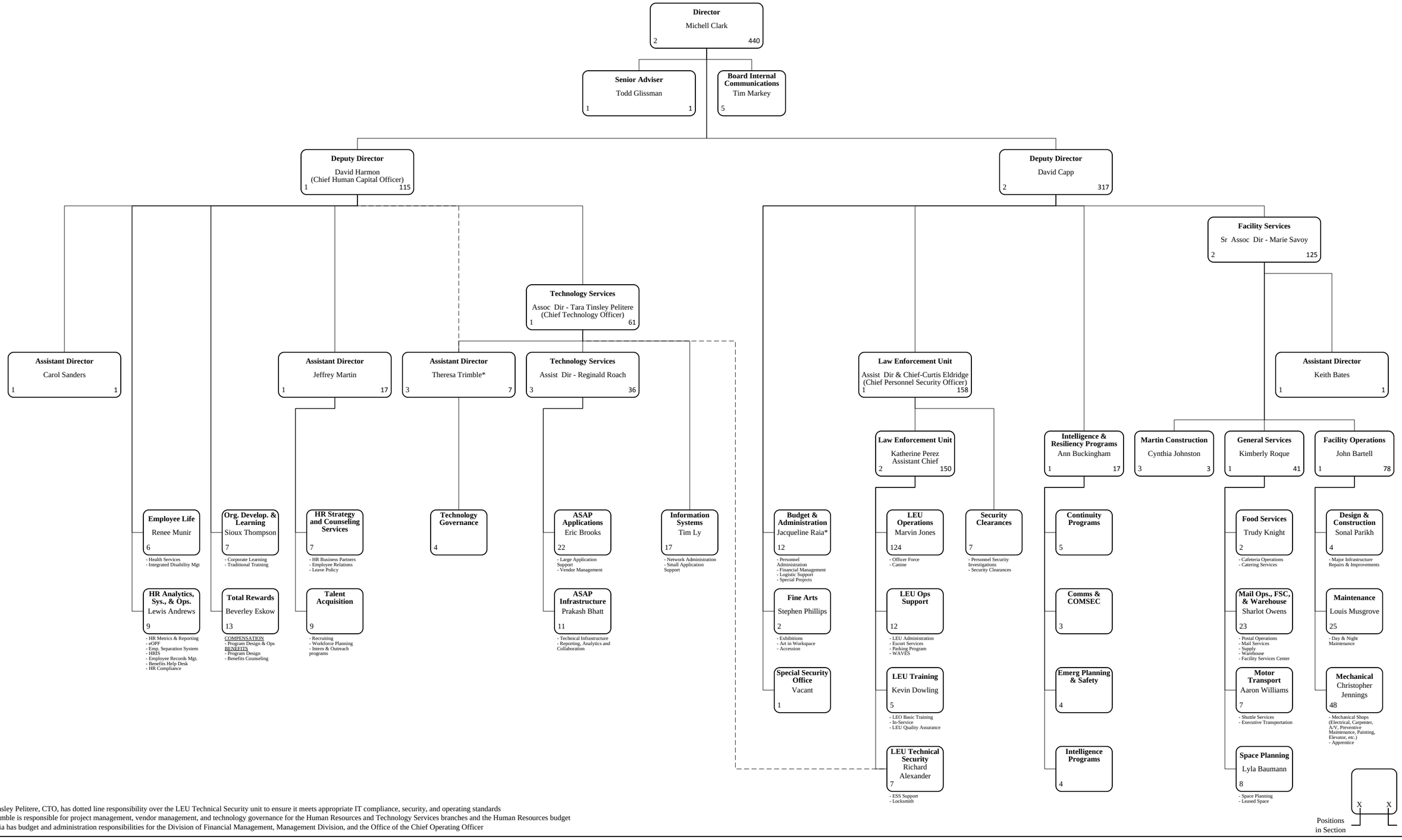


* Ms Shack Marquez also has Deputy Director responsibility in RS

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

MANAGEMENT DIVISION

September 15, 2014

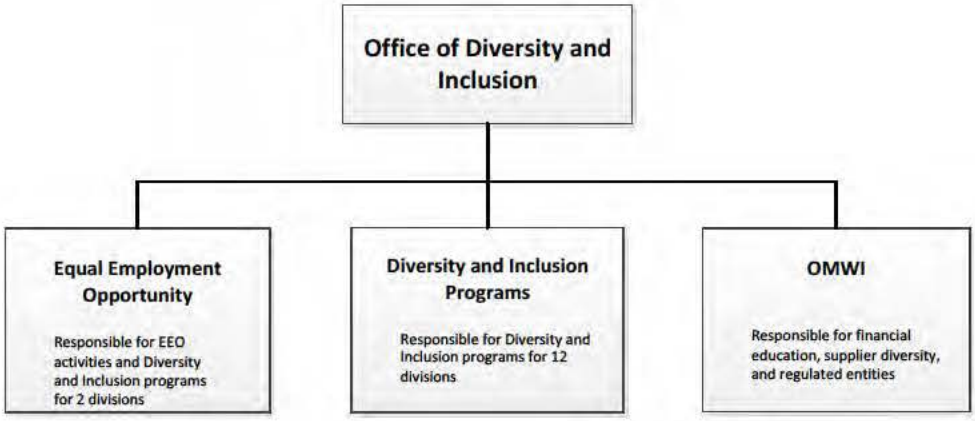


Notes:

* Ms Tinsley Pelitere, CTO, has dotted line responsibility over the LEU Technical Security unit to ensure it meets appropriate IT compliance, security, and operating standards
* Ms Trimble is responsible for project management, vendor management, and technology governance for the Human Resources and Technology Services branches and the Human Resources budget
* Ms Raia has budget and administration responsibilities for the Division of Financial Management, Management Division, and the Office of the Chief Operating Officer

PSSC:
OWMI - Gain an Understanding of the Office

Source: Created by Sopeany Keo, OIG Auditor based on interviews with OD&I official.



December 27, 2010

Establishment of the Office of Diversity and Inclusion and appointment of the program director

From Governor Kevin M. Warsh and Stephen R. Malphrus, Staff Director

Section 342 of the Dodd-Frank Act requires the Board and each Reserve Bank, as well as other financial regulatory agencies, to establish a diversity and inclusion office by January 21, 2011.

To comply with this provision, the Board approved, effective January 2, 2011, the establishment of a new Office of Diversity and Inclusion that will incorporate the EEO Programs Office as well as other areas of focus under section 342, including fostering diversity in the Board's procurements and assisting in developing standards to assess the diversity practices of the entities the Board regulates. The Office will work with other areas of the Board, including Procurement, Staffing, Bank Supervision and Regulation, and Consumer and Community Affairs to carry out its statutory responsibilities.

Sheila Clark has been appointed program director for the office. Sheila joined the Board in February 1995 as the EEO programs director and has administered the Board's equal employment opportunity and affirmative action programs over the last 15 years. She works with business units and divisions to promote equal opportunity and diversity in their employment practices. She has been responsible for providing training to Board employees regarding their rights and responsibilities under the federal EEO laws and providing an effective counseling program to address complaints of discrimination.

In addition, Sheila works with and evaluates the Reserve Bank EEO programs. Prior to joining the Board, Sheila was manager of Workplace Diversity Programs at Dow Jones Company, where she gained extensive experience in equal employment opportunity and affirmative action in the private sector. During her employment with Dow Jones, she was responsible for the company's EEO/affirmative action initiatives, work-family initiatives, college recruitment, and diversity training. Sheila has a BA in management.

FRONT PAGE

(b) (5)

BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

April 10, 2007

The Honorable Nancy Pelosi
Speaker of the House of Representatives
Washington, D.C. 20515

Dear Madam Speaker:

On behalf of the Board of Governors of the Federal Reserve System, I am submitting the third annual report pursuant to the requirements of Section 203(a) of the Notification and Federal Employee Anti-discrimination and Retaliation Act of 2002 ("No FEAR Act"), Public Law 107-174. In accordance with Section 203(b) of the No FEAR Act, this report includes data for fiscal year 2006. Also enclosed are Supplemental Reports to the First and Second Annual No FEAR reports previously submitted which include data for fiscal years 1999 through 2005.

Sincerely,

(signed) Sheila Clark

Sheila Clark
EEO Programs Director

Enclosures
Identical letters sent to the attached list. (07-2779)
bcc: S. Clark, J. Bruce, R. McKinney (w/copy of report), S. Seldin (w/copy of report)

Distribution List for No FEAR Act report to Congress
April 2007

The Honorable Robert C. Byrd
President Pro Tempore of the Senate
Washington, D.C. 20510
Dear Senator

The Honorable Nancy Pelosi
Speaker of the House of Representatives
Washington, D.C. 20515
Dear Madam Speaker

The Honorable Joe Lieberman
Chairman
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, D.C. 20510
Dear Mr. Chairman:

The Honorable Susan M. Collins
Ranking Member
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, D.C. 20510
Dear Senator:

The Honorable Henry A. Waxman
Chairman
Committee on Oversight and
Government Reform
House of Representatives
Washington, D.C. 20515
Dear Mr. Chairman:

The Honorable Tom Davis
Ranking Member
Committee on Oversight and
Government Reform
House of Representatives
Washington, D.C. 20515
Dear Congressman:

The Honorable Christopher J. Dodd
Chairman
Committee on Banking, Housing,
and Urban Affairs
United States Senate
Washington, D.C. 20510
Dear Mr. Chairman:

The Honorable Richard C. Shelby
Ranking Member
Committee on Banking, Housing,
and Urban Affairs
United States Senate
Washington, D.C. 20510
Dear Senator:

The Honorable Barney Frank
Chairman
Committee on Financial Services
House of Representatives
Washington, D.C. 20515
Dear Mr. Chairman:

The Honorable Spencer Bachus
Ranking Member
Committee on Financial Services
House of Representatives
Washington, D.C. 20515
Dear Congressman

The Honorable Naomi C. Earp
Chair
Equal Employment Opportunity Commission
1801 L Street, N.W.
Washington, D.C. 20507
Dear Madam Chair:

The Honorable Alberto R. Gonzales
Attorney General
Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530
Dear Mr. Attorney General:

(b) (5)

BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

ADDRESS OFFICIAL CORRESPONDENCE
TO THE BOARD

No FEAR Act Written Training Plan

Submitted by
Board of Governors of the Federal Reserve System

On July 20, 2006, the Office of Personnel Management (OPM) published its final rule implementing the training requirements of the Notification and Federal Employee Antidiscrimination and Retaliation Act ("No FEAR Act").

The final rule required each agency to develop a written plan for training all of its employees, including supervisors and managers. The plan must describe:

- The instructional materials and method of the training
- The training schedule, and
- The means of documenting completion of training

On December 28, 2006, the Office of Personnel Management issued the final rule regarding "Implementations of Title II of the No FEAR Act of 2002 – Reporting and Best Practices." Among other things, this final rule requires each agency to provide annual reports on the number of items relating to the agency's implementation of the No FEAR Act, including the agency's written plan.

This document constitutes the Board of Governors of the Federal Reserve System's (Board) No FEAR Act written training Plan.

I. The instructional materials and method of the training

The final rules require federal agencies to train all employees on their rights and remedies under the federal antidiscrimination and whistleblower protection laws. Agencies must have trained all current employees by December 17, 2007, and all new employees within 90 days of hire. Agencies also must provide training to all employees every two years.

With these requirements in mind, the Board contracted with Brightline Compliance, LLC to provide instruction to employees through Brightline's interactive online No FEAR Act training course.

As required by the No FEAR Act and the OPM final rule, the Board's online course teaches our employees about their rights and remedies available under the antidiscrimination, retaliation, and whistleblower protection laws. With regard to rights under whistleblowing statutes, the No FEAR Act provides for notification and training only with regard to a federal statute that is inapplicable to employees of the Board. The Federal Deposit Insurance Act and the Inspector

General Act, however prohibit retaliation against Board employees if they make a protected disclosure of any possible violation of any law or regulation, gross mismanagement, a gross waste of funds, and abuse of authority, or a substantial and specific danger to public health or safety. Employees who believe they have experienced retaliation for such whistleblowing activities have been informed via the required "Employee Notification of Rights" No FEAR Act provision whom to contact.

The No FEAR Act course:

- Provides instruction on all topics required by the No FEAR Act and the OPM final rule
- Provides supervisors and managers additional instruction on their responsibilities
- Allows users to interact with a series of audio-visual scenarios so that they are continually engaged in the learning process

II. The training schedule

The Board has conducted mandatory EEO Training since 1979. We have maintained completion records through our training course data base. The Board has provided two days of EEO training for supervisory and non-supervisor employees. The training consisted of anti-discrimination laws, legal compliance topics, EEO complaint process and retaliation.

Beginning April 2007, access to the online course was provided. Employees completed their initial No FEAR Act training by April 30, 2007. The Board ensures that subsequently hired employees complete training within 90 days from their starting dates.

As required under the No FEAR Act, employees will be provided a refresher courses via blended training, i.e.: Web, classroom, and seminars focusing on the major principles of the previous training and addressing new and developing areas related to No FEAR compliance.

III. The means of documenting completion of training

The Board tracks employees' completion of the online training courses through Brightline's learning management system, BrightlineLMS. BrightlineLMS automatically creates a record of each employee's course completion and enables training coordinator to monitor training activities such as start and incomplete.

(b) (5)

April 22, 2011

The Honorable Daniel Inouye
President Pro Tempore of the Senate
S-128 Capitol Bldg.
Washington, DC 20510

Dear Senator:

On behalf of the Board of Governors of the Federal Reserve System, I am submitting the seventh annual report pursuant to the requirements of Section 203(a) of the Notification and Federal Employee Anti-discrimination and Retaliation Act of 2002 (No FEAR Act), Public Law 107-174. In accordance with Section 203(b) of the No FEAR Act, this report includes data for fiscal year 2010.

Sincerely,

Sheila Clark
Diversity and Inclusion Programs Director

Enclosure:

CY 2010 No FEAR Act Congressional Report
CY 2010 Report
Federal Reserve Board Training Plan

Prefix	Name	Title	Committee	House-Senate	Adress	Address	State	zip	salutation
The Honorable	Daniel Inouye	President Pro Tempore of the Senate			S-128 Capitol Bldg.	Washington	DC	20510	Senator
The Honorable	John Boehner	Speaker of the House of Representatives			H-232 Capitol Bldg.	Washington	DC	20515	Mr. Speaker
The Honorable	Joseph I. Lieberman	Chairman	Committee on Homeland Security and Governmental Affairs	United States Senate	SD-340 Dirksen Bldg.	Washington	DC	20510	Mr. Chairman
The Honorable	Susan M. Collins	Ranking Member	Committee on Homeland Security and Governmental Affairs	United States Senate	SD-340 Dirksen Bldg.	Washington	DC	20510	Senator
The Honorable	Darrell Issa	Chairman	Committee on Oversight and Government Reform	House of Representatives	2157 Rayburn Bldg.	Washington	DC	20515	Mr. Chairman
The Honorable	Stephen Lynch	Ranking Member	Committee on Oversight and Government Reform	House of Representatives	B-350A Rayburn Bldg.	Washington	DC	20515	Congressman
The Honorable	Tim Johnson	Chairman	Committee on Banking, Housing, and Urban Affairs	United States Senate	SD-534 Dirksen Bldg.	Washington	DC	20510	Mr. Chairman
The Honorable	Richard C. Shelby	Ranking Member	Committee on Banking, Housing, and Urban Affairs	United States Senate	SD-534 Dirksen Bldg.	Washington	DC	20510	Senator
The Honorable	Spencer Bachus	Chairman	Committee on Financial Services	House of Representatives	2129 Rayburn Bldg.	Washington	DC	20515	Mr. Chairman
The Honorable	Barney Frank	Ranking Member	Committee on Financial Services	House of Representatives	B-371A Rayburn Bldg.	Washington	DC	20515	Congressman
The Honorable	Jacqueline A Barrien	Chair	Equal Employment Opportunity Commission		131 M Street, NE	Washington	DC	20507	Ms. Madam Chair
The Honorable	Eric H. Holder	Attorney General	Department of Justice		950 Pennsylvania Avenue, N.W.	Washington	DC	20530	Mr. Attorney General
Mr.	Gary D. Wahlert	Office of Personnel Management	Center for Workforce Relations		1900 E Street, N.W., Suite 7H28	Washington	DC	20415	Mr. Wahlert

(b) (5)

(b) (5)

March 27, 2012

Dear :

On behalf of the Board of Governors of the Federal Reserve System, I am submitting the eighth annual report pursuant to the requirements of Section 203(a) of the Notification and Federal Employee Anti-discrimination and Retaliation Act of 2002 (No FEAR Act), Public Law 107-174. In accordance with Section 203(b) of the No FEAR Act, this report includes data for fiscal year 2011.

Sincerely,

Sheila Clark
Diversity and Inclusion Programs Director

Enclosure:

FY 2011 No FEAR Act Congressional Report
FY 2011 No FEAR Act Report
Federal Reserve Board Training Plan

Prefix	Name	Title	Committee	House-Senate	Adress	Address	State	zip	salutation
The Honorable	Daniel Inouye	President Pro Tempore of the Senate			S-128 Capitol Bldg.	Washington	DC	20510	Senator
The Honorable	John Boehner	Speaker of the House of Representatives			H-232 Capitol Bldg.	Washington	DC	20515	Mr. Speaker
The Honorable	Joseph I. Lieberman	Chairman	Committee on Homeland Security and Governmental Affairs	United States Senate	SD-340 Dirksen Bldg.	Washington	DC	20510	Mr. Chairman
The Honorable	Susan M. Collins	Ranking Member	Committee on Homeland Security and Governmental Affairs	United States Senate	SD-340 Dirksen Bldg.	Washington	DC	20510	Senator
The Honorable	Darrell Issa	Chairman	Committee on Oversight and Government Reform	House of Representatives	2157 Rayburn Bldg.	Washington	DC	20515	Mr. Chairman
The Honorable	Elijah Cummings	Ranking Member	Committee on Oversight and Government Reform	House of Representatives	B-350A Rayburn Bldg.	Washington	DC	20515	Congressman
The Honorable	Tim Johnson	Chairman	Committee on Banking, Housing and Urban Affairs	United States Senate	SD-534 Dirksen Bldg.	Washington	DC	20510	Mr. Chairman
The Honorable	Richard C. Shelby	Ranking Member	Committee on Banking, Housing, and Urban Affairs	United States Senate	SD-534 Dirksen Bldg.	Washington	DC	20510	Senator
The Honorable	Spencer Bachus	Chairman	Committee on Financial Services	House of Representatives	2129 Rayburn Bldg.	Washington	DC	20515	Mr. Chairman
The Honorable	Barney Frank	Ranking Member	Committee on Financial Services	House of Representatives	B-371A Rayburn Bldg.	Washington	DC	20515	Congressman
The Honorable	Jacqueline A Barrien	Chair	Equal Employment Opportunity Commission		131 M Street, NE	Washington	DC	20507	Ms. Madam Chair
The Honorable	Eric H. Holder	Attorney General	Department of Justice		950 Pennsylvania Avenue, N.W.	Washington	DC	20530	Mr. Attorney General
Mr.	Gary D. Wahlert	Office of Personnel Management	Center for Workforce Relations		1900 E Street, N.W., Suite 7H28	Washington	DC	20415	Mr. Wahlert

(b) (5)

Attachment #3(e)

April 18, 2013

On behalf of the Board of Governors of the Federal Reserve System, I am submitting the ninth annual report pursuant to the requirements of Section 203(a) of the Notification and Federal Employee Anti-discrimination and Retaliation Act of 2002 (No FEAR Act), Public Law 107-174. In accordance with Section 203(b) of the No FEAR Act, this report includes data for fiscal year 2012.

Sincerely,

Sheila Clark
Diversity and Inclusion Programs Director

Enclosures:

FY 2012 No FEAR Act Congressional Report
FY 2012 No FEAR Act Report
Federal Reserve Board Training Plan

Prefix	Name	Title	Committee	House-Senate	Adress	Address	State	zip	salutation
The Honorable	Patrick Leahy	President Pro Tempore of the Senate			S-128 Capitol Bldg.	Washington	DC	20510	Senator
The Honorable	John Boehner	Speaker of the House of Representatives			H-232 Capitol Bldg.	Washington	DC	20515	Mr. Speaker
The Honorable	Thomas R. Carper	Chairman	Committee on Homeland Security and Governmental Affairs	United States Senate	SD-340 Dirksen Bldg.	Washington	DC	20510	Mr. Chairman
The Honorable	Tom Coburn	Ranking Member	Committee on Homeland Security and Governmental Affairs	United States Senate	SD-340 Dirksen Bldg.	Washington	DC	20510	Senator
The Honorable	Darrell Issa	Chairman	Committee on Oversight and Government Reform	House of Representatives	2157 Rayburn Bldg.	Washington	DC	20515	Mr. Chairman
The Honorable	Elijah Cummings	Ranking Member	Committee on Oversight and Government Reform	House of Representatives	B-350A Rayburn Bldg.	Washington	DC	20515	Congressman
The Honorable	Tim Johnson	Chairman	Committee on Banking, Housing and Urban Affairs	United States Senate	SD-534 Dirksen Bldg.	Washington	DC	20510	Mr. Chairman
The Honorable	Mike Crapo	Ranking Member	Committee on Banking, Housing, and Urban Affairs	United States Senate	SD-534 Dirksen Bldg.	Washington	DC	20510	Senator
The Honorable	Jeb Hensarling	Chairman	Committee on Financial Services	House of Representatives	2129 Rayburn Bldg.	Washington	DC	20515	Mr. Chairman
The Honorable	Maxine Waters	Ranking Member	Committee on Financial Services	House of Representatives	B-371A Rayburn Bldg.	Washington	DC	20515	Congressman
The Honorable	Jacqueline A. Berrien	Chair	Equal Employment Opportunity Commission		131 M Street, NE	Washington	DC	20507	Ms. Madam Chair
The Honorable	Eric H. Holder	Attorney General	Department of Justice		950 Pennsylvania Avenue, N.W.	Washington	DC	20530	Mr. Attorney General
Mr.	Tim Curry	Office of Personnel Management	Partnership and Labor Relations		1900 E Street, N.W., Suite 7H28	Washington	DC	20415	Mr. Wahlert

(b) (5)

April 18, 2014

On behalf of the Board of Governors of the Federal Reserve System, I am submitting the tenth annual report pursuant to the requirements of Section 203(a) of the Notification and Federal Employee Anti-discrimination and Retaliation Act of 2002 (No FEAR Act), Public Law 107-174. In accordance with Section 203(b) of the No FEAR Act, this report includes data for fiscal year 2013.

Sincerely,

Sheila Clark
Diversity and Inclusion Programs Director

Enclosures:

FY 2013 No FEAR Act Congressional Report
FY 2013 No FEAR Act Report
Federal Reserve Board Training Plan

Prefix	Name	Title	Committee	House-Senate	Adress	Address	State	zip	salutation
The Honorable	Patrick Leahy	President Pro Tempore of the Senate			S-128 Capitol Bldg.	Washington	DC	20510	Senator
The Honorable	John Boehner	Speaker of the House of Representatives			H-232 Capitol Bldg.	Washington	DC	20515	Mr. Speaker
The Honorable	Thomas R. Carper	Chairman	Committee on Homeland Security and Governmental Affairs	United States Senate	SD-340 Dirksen Bldg.	Washington	DC	20510	Mr. Chairman
The Honorable	Tom Coburn	Ranking Member	Committee on Homeland Security and Governmental Affairs	United States Senate	SD-340 Dirksen Bldg.	Washington	DC	20510	Senator
The Honorable	Darrell Issa	Chairman	Committee on Oversight and Government Reform	House of Representatives	2157 Rayburn Bldg.	Washington	DC	20515	Mr. Chairman
The Honorable	Elijah Cummings	Ranking Member	Committee on Oversight and Government Reform	House of Representatives	B-350A Rayburn Bldg.	Washington	DC	20515	Congressman
The Honorable	Tim Johnson	Chairman	Committee on Banking, Housing and Urban Affairs	United States Senate	SD-534 Dirksen Bldg.	Washington	DC	20510	Mr. Chairman
The Honorable	Mike Crapo	Ranking Member	Committee on Banking, Housing, and Urban Affairs	United States Senate	SD-534 Dirksen Bldg.	Washington	DC	20510	Senator
The Honorable	Jeb Hensarling	Chairman	Committee on Financial Services	House of Representatives	2129 Rayburn Bldg.	Washington	DC	20515	Mr. Chairman
The Honorable	Maxine Waters	Ranking Member	Committee on Financial Services	House of Representatives	B-371A Rayburn Bldg.	Washington	DC	20515	Congressman
The Honorable	Jacqueline A. Berrien	Chair	Equal Employment Opportunity Commission		131 M Street, NE	Washington	DC	20507	Ms. Madam Chair
The Honorable	Eric H. Holder	Attorney General	Department of Justice		950 Pennsylvania Avenue, N.W.	Washington	DC	20530	Mr. Attorney General
Mr.	Tim Curry	Office of Personnel Management	Partnership and Labor Relations		1900 E Street, N.W., Suite 7H28	Washington	DC	20415	Mr. Wahlert

Help

WRP
Workforce Recruitment Program

About Us | Employers | Schools | Students | Resources

Welcome to the 2015 Workforce Recruitment Program (WRP)

If you are an Employer in the federal government and wish to take advantage of WRP,

Register Now!

If you are a private sector employer and wish to take advantage of WRP, go to www.askEARN.org.

If you're a school or student interested in WRP and wish to learn more, read our About Us section for more details.

Do you need highly qualified candidates for jobs at your office? The Workforce Recruitment Program can help! The WRP is a recruitment and referral program that connects federal and private sector employers nationwide with highly motivated college students and recent graduates with disabilities who are eager to prove their abilities in the workplace through summer or permanent jobs.

The U.S. Department of Labor's Office of Disability Employment Policy (ODEP) and the U.S. Department of Defense's Office of Diversity Management & Equal Opportunity (ODMEO) manage the program, which continues to be successful with the participation of many other federal agencies and sub-agencies. Since the program's expansion in 1995, over 6,000 students and recent graduates have received temporary and permanent employment opportunities through the WRP.

In 2011, the Office of Personnel Management (OPM) highlighted the WRP as a model strategy in its guidance to federal agencies regarding the recruitment and hiring of people with disabilities in response to Executive Order 13548, Increasing Federal Employment of Individuals with Disabilities.

Annually, trained WRP recruiters from federal agencies conduct personal interviews with interested candidates on college and university campuses across the country. Candidates represent all majors, and range from college freshmen to graduate students and law students. Information from these candidate interviews is compiled in a searchable database that is available through this website to federal Human Resources Specialists, Equal Employment Opportunity Specialists, and other hiring officials in federal agencies. You can request a password here. If you are an employer in the private sector, or a student interested in private sector employment, you can take advantage of the WRP through the National Employer Technical Assistance Center at www.askEARN.org.

sign in

email

password

Sign In

Forgot your password?

Disclaimer: This is a U.S. Government computer system. U.S. Government computer systems are provided for the processing of Official U.S. Government information only. All information contained on this system is owned by the Department of Labor and the Department of Defense and may be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel.

ODEP
Office of Disability Employment Policy

Cosponsored by the Department of Labor's Office of Disability Employment Policy and the U.S. Department of Defense.

The information contained herein is for United States Government use only and should be treated as privileged information. Safeguard the confidential nature of this data.

Office of Inspector General Statement of Independence for Individual Projects

Employees of the Office of Inspector General (OIG) or its contractors who are engaged in audit, attestation, inspection, evaluation, or investigative work are to conduct themselves in a manner consistent with the Federal Reserve Board's and OIG's core values, the "Ethics Handbook for Board Employees," the *Government Auditing Standards*, the *Quality Standards for Inspection and Evaluation*, and the standards applicable to their project. Employees of the OIG and its contractors must take precautions to ensure that their conduct is perceived as being independent, professional, and appropriate and are not to become involved in conflict-of-interest situations or situations that give the appearance that a conflict exists.

The OIG and its staff and contractors must be free from personal, external, and organizational impairments to independence and must avoid appearance of such impairments of independence, so their work will be viewed as impartial by objective third parties. Employees of the OI and its contractors should refer to the Quality Standards for Inspection and Evaluation and chapter 3 of the *Government Auditing Standards* a comprehensive discussion of personal, external, and organizational impairments to independence. Impairments to independence include, are not limited to:

--financial interest that is direct, or is significant/material though indirect, in the audited entity or program.
--seeking employment with the entity to be reviewed or under review.
--preconceived ideas toward individuals, groups, organizations, or objectives of a particular program that could bias the project.
--official, professional, personal, or financial relationships that might cause an employee of the OIG or its contractors to limit the extent of his/her inquiry, to limit disclosure, or to weaken or slant findings in any way.
--external interference or influence that improperly or imprudently limits or modifies the scope of project work.

Employees of the OIG and its contractors should be aware that independence impairments can occur because of the potential to develop close personal relationships with Board staff who work in program areas being audited or otherwise reviewed. Also, employees of the OIG and its contractors may wish to apply for job postings in other Board divisions at a time when they are assigned to or about to be assigned to review a program in that division. When these or other apparent or potential conflicts of interest occur, the individual should fully disclose the situation to the cognizant OIG manager. In consultation with the Inspector General, appropriate action by management might include reassigning the individual, limiting the individual's role, or providing additional reviews of the individual's work. Failure to comply with the OIG's policies and procedures regarding personal impairments may result in disciplinary action against the individual, consistent with the Board's Disciplinary Actions policy.

Instructions:

This form, which documents compliance with applicable independence standards, is to be completed at the start of each project by OIG or contractor project team members. The completed and signed form should be scanned into the project database. Individuals who are either not able to sign this statement or experience a situation in the future where they believe their independence and/or objectivity is or may be impaired should notify the cognizant OIG manager to discuss their situation. The Assistant Inspector General for Legal Services and the Board's Ethics Officer are also available for consultation.

I have read the above and attest that I have neither personal nor external impairments to my independence that will keep me from objectively planning and conducting my work on this project and reaching independent conclusions based on the evidence. I will reevaluate my independence whenever my assignment is changed and whenever my circumstances change. If changes affecting either my independence or my objectivity occur subsequent to the completion of this form, I will promptly notify the cognizant OIG manager.

Project Name 2014 Congressional Request on the Board's Personnel Practices

Individual's Name: Anna Saez

Date Individual Started Work on Project: 4/8/2014

Individual's Signature: _____ **Date:** 4-9-2014

Office of Inspector General Statement of Independence for Individual Projects

Employees of the Office of Inspector General (OIG) or its contractors who are engaged in audit, attestation, inspection, evaluation, or investigative work are to conduct themselves in a manner consistent with the Federal Reserve Board's and OIG's core values, the "Ethics Handbook for Board Employees," the *Government Auditing Standards*, the *Quality Standards for Inspection and Evaluation*, and the standards applicable to their project. Employees of the OIG and its contractors must take precautions to ensure that their conduct is perceived as being independent, professional, and appropriate and are not to become involved in conflict-of-interest situations or situations that give the appearance that a conflict exists.

The OIG and its staff and contractors must be free from personal, external, and organizational impairments to independence and must avoid appearance of such impairments of independence, so their work will be viewed as impartial by objective third parties. Employees of the OI and its contractors should refer to the Quality Standards for Inspection and Evaluation and chapter 3 of the *Government Auditing Standards* a comprehensive discussion of personal, external, and organizational impairments to independence. Impairments to independence include, are not limited to:

--financial interest that is direct, or is significant/material though indirect, in the audited entity or program.
--seeking employment with the entity to be reviewed or under review.
--preconceived ideas toward individuals, groups, organizations, or objectives of a particular program that could bias the project.
--official, professional, personal, or financial relationships that might cause an employee of the OIG or its contractors to limit the extent of his/her inquiry, to limit disclosure, or to weaken or slant findings in any way.
--external interference or influence that improperly or imprudently limits or modifies the scope of project work.

Employees of the OIG and its contractors should be aware that independence impairments can occur because of the potential to develop close personal relationships with Board staff who work in program areas being audited or otherwise reviewed. Also, employees of the OIG and its contractors may wish to apply for job postings in other Board divisions at a time when they are assigned to or about to be assigned to review a program in that division. When these or other apparent or potential conflicts of interest occur, the individual should fully disclose the situation to the cognizant OIG manager. In consultation with the Inspector General, appropriate action by management might include reassigning the individual, limiting the individual's role, or providing additional reviews of the individual's work. Failure to comply with the OIG's policies and procedures regarding personal impairments may result in disciplinary action against the individual, consistent with the Board's Disciplinary Actions policy.

Instructions:

This form, which documents compliance with applicable independence standards, is to be completed at the start of each project by OIG or contractor project team members. The completed and signed form should be scanned into the project database. Individuals who are either not able to sign this statement or experience a situation in the future where they believe their independence and/or objectivity is or may be impaired should notify the cognizant OIG manager to discuss their situation. The Assistant Inspector General for Legal Services and the Board's Ethics Officer are also available for consultation.

I have read the above and attest that I have neither personal nor external impairments to my independence that will keep me from objectively planning and conducting my work on this project and reaching independent conclusions based on the evidence. I will reevaluate my independence whenever my assignment is changed and whenever my circumstances change. If changes affecting either my independence or my objectivity occur subsequent to the completion of this form, I will promptly notify the cognizant OIG manager.

Project Name 2014 Congressional Request on the Board's Personnel Practices

Individual's Name: Anna Saez

Date Individual Started Work on Project: 4/8/2014

Individual's Signature:  **Date:** 4-9-2014

Office of Inspector General
Officer Statement of Independence for Individual Projects

Office of Inspector General (OIG) officers engaged in audit, attestation, inspection, evaluation, or investigative work are to conduct themselves in a manner consistent with the Federal Reserve Board's and OIG's core values, the "Ethics Handbook for Board Employees," the *Government Auditing Standards*, the *Quality Standards for Inspection and Evaluation*, and any other standards applicable to the specific project.

OIG staff must be free from personal, external, and organizational impairments to independence and must avoid the appearance of such impairments of independence, so their work will be viewed as impartial by objective third parties. Officers should refer to the *Quality Standards for Inspection and Evaluation* and chapter 3 of the *Government Auditing Standards* for a comprehensive discussion of personal, external, and organizational impairments to independence. Impairments to independence include, but are not limited to:

--financial interest that is direct, or is significant/material though indirect, in the audited entity or program;
--preconceived ideas toward individuals, groups, organizations, or objectives of a particular program that could bias the project;
--official, professional, personal, or financial relationships that might cause one to limit the extent of his/her inquiry, to limit disclosure, or to weaken or slant findings in any way;
--seeking employment with the entity to be reviewed or under review; or
--external interference or influence that improperly or imprudently limits or modifies the scope of project work.

When an actual, potential, or perceived conflict of interest occurs, the individual should fully disclose the situation to the Inspector General or, in the case of the Inspector General, the OIG's Assistant Inspector General for Legal Services. The Board's Ethics Officer also is available for consultation. Appropriate action to address the matter might include recusal from a specific project, reassigning the individual, limiting the individual's role, or providing additional reviews of the individual's work.

This form, which documents compliance with applicable independence standards, is to be completed by an officer when he/she becomes involved in a project. The signed form should be scanned into the project database or provided to the project manager for inclusion. An officer who subsequently experiences a situation where his/her independence and/or objectivity is or may be impaired should fully disclose the situation as provided in the previous paragraph. Failure to comply with the OIG's policies and procedures regarding personal impairments may result in disciplinary action against the employee, consistent with the Board's Disciplinary Actions policy.

I have read the above and attest that I do not have any personal, external, or organizational impairment to my independence with respect to this project. I am able to objectively oversee this project and reach independent conclusions or decisions based on the evidence. I will reevaluate my independence whenever my circumstances change and will notify the appropriate official as necessary.

Project Name 2014 Congressional Request on the Board's Personnel Practices

Individual's Name: Melissa Heist

Date Individual Started Work on Project: 4/8/2014

Individual's Signature: Melissa Heist **Date:** 4/10/14

Kimberly Perteet

From: Tim Rogers
Sent: Friday, April 25, 2014 12:14 PM
To: Donald Hammond
Cc: Michell Clark; Sheila Clark; David Harmon; Bill Mitchell; WilliamsO@gao.gov; Mark Bialek; Tony Ogden; Melissa M. Heist; Andrew Patchan; Anna Saez; Kimberly Perteet
Subject: OIG Audit of the Board's Diversity and Inclusion Processes -ZFRSSE-
Attachments: Board Announcement CR Diversity April 2014.pdf

Good afternoon,

The Office of Inspector General received a letter from the House Committee on Financial Services requesting that our office review activities related to workplace diversity and inclusion at the Board. As described in the attached memorandum, we are initiating an audit of the Board's personnel operations and other efforts to provide equal employment opportunities, and will be contacting your offices shortly to arrange an entrance conference. If you have any questions concerning this audit, please contact me at (202) 973-5042 or Anna Saez, OIG Manager at (202) 973-5027.

Regards,
Tim Rogers

Timothy Rogers | Sr. OIG Manager for Management and Operations
Audits and Evaluations
Office of Inspector General
Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-5042 | c: 202-450-7792 | timothy.p.rogers@frb.gov

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

April 25, 2014

MEMORANDUM

TO: Donald Hammond
Chief Operating Officer

FROM: Timothy Rogers
Senior OIG Manager for Management and Operations
Office of Audits and Evaluations

SUBJECT: Congressional Request Regarding the Board's Diversity and Inclusion Processes

In response to a recent letter from the House Committee on Financial Services (attachment A), the Office of Inspector General is initiating an audit of the Board of Governors of the Federal Reserve System's (Board) activities related to diversity and inclusion processes. The objective of this audit is to assess the Board's personnel operations and other efforts to provide for equal employment opportunities, including equal opportunity for minorities and women to obtain senior management positions, and for racial, ethnic, and gender diversity in the workforce.

To answer our objective, we plan to

- analyze information related to trend statistics, such as performance management results and promotions for minority and women employees, informal and formal equal employment opportunity complaint statistics, and employee satisfaction survey results

- review relevant Board personnel operations, policies, and procedures, such as those related to performance management, to determine whether adequate controls are established to prevent and detect bias or discrimination

- assess the Board's efforts to respond to complaints, employee satisfaction survey results, or other potential indications of bias and to increase diversity in management

- evaluate the Office of Minority and Women Inclusion's role and involvement in monitoring the impact of the Board's personnel policies on minorities and women, as well as monitoring the agency's efforts to increase diversity in senior management positions

- identify any factors that may impact the Board's ability to increase diversity in senior management positions

Our scope will include personnel activities that took place from January 2011 through December 2013, as well as changes to policies and procedures since December 2013.

We will contact your office shortly to schedule an entrance conference to further discuss our planned work in more detail. Attachment B contains our initial list of documents that we are requesting to assist us in addressing our objective. Please provide the documents at your earliest convenience. If you have any questions concerning this audit, please contact Anna Saez, OIG Manager, at 202-973-5027 or me at 202-973-5042.

Attachments
cc: Michell Clark, Director, Management Division
David Harmon, Chief Human Capital Officer
Sheila Clark, Program Director, Office of Minority and Women Inclusion
William Mitchell, Chief Financial Officer and Director, Division of Financial Management
Orice Williams Brown, U.S. Government Accountability Office
Mark Bialek, Inspector General
J. Anthony Ogden, Deputy Inspector General
Melissa Heist, Associate Inspector General for Audits and Evaluations
Andrew Patchan Jr., Associate Inspector General for Information Technology

Attachment A

JEB HENSARLING, TX, CHAIRMAN

MAXINE WATERS, CA, RANKING MEMBER

United States House of Representatives
Committee on Financial Services
Washington, D.C. 20515

March 24, 2014

Inspector General Mark Bialek
Board of Governors of the Federal Reserve System
Office of Inspector General
20th and C Streets N.W.
Mail Stop 300
Washington, DC 20551

Dear Inspector General Bialek:

We write to request that the Office of the Inspector General (OIG) for the Board of Governors of the Federal Reserve System (FRS) review the agency's internal operations to determine whether any personnel practices have created a discriminatory workplace or otherwise systematically disadvantaged minorities from obtaining senior management positions.

Section 342 of the Dodd-Frank Wall Street Reform and Consumer Protection Act established an Office of Minority and Women Inclusion (OMWI) at most of the federal financial regulatory agencies, responsible for matters relating to diversity in management, employment, and business activities. Despite this statutory mandate, the Government Accountability Office (GAO) concluded in a report released last year that management-level representation of minorities and women among federal financial agencies and Federal Reserve Banks has not changed substantially from 2007 through 2011. In fact, across all federal financial regulators, agency representation of minorities was as low as 6 percent and dropped as low as zero percent at one of the Reserve Banks. In light of these findings and the concerns raised by employee performance evaluations at the Consumer Financial Protection Bureau (CFPB), we believe the OIG should work in cooperation with Federal Reserve System's OMWI Director to assess current personnel practices and make recommendations necessary to ensure full compliance with the law.

The 2013 GAO report, entitled "Trends and Practices in the Financial Industry and Agencies after the Recent Financial Crisis," documented the extremely poor representation of women and minorities in leadership positions within the financial services industry and among federal financial regulators. According to GAO, industry representation of minorities in 2011 was higher in lower-level management positions – approximately 20 percent – as compared to about 11 percent of senior-level manager positions.

While public attention is currently and justifiably focused on the CFPB, the most recent OMWI reports suggest the disparities impeding internal upward mobility for minorities may be endemic throughout all the agencies regulating the financial services industry. According to the Treasury Department's 2013 OMWI report, among its senior executive management, 86 percent are white men, compared to 7 percent Black men, 4 percent Hispanic men, and 3 percent Asian men. Among the agency's GS-15 employees, which serves as a pipeline to senior level management, white men are once again overrepresented at 86 percent, compared to 6 percent Black men, 2 percent Hispanic men, and 6 percent Asian men.

At the Federal Reserve, white men represent 50 percent of executive senior level managers, compared to just 28.7 percent represented by white women. Along ethnic categories, black and Hispanic men represent, respectively, roughly 5 percent and 1 percent of executive senior level managers. Black women represent roughly 6 percent and Hispanic women represent nearly 2 percent of senior managers.

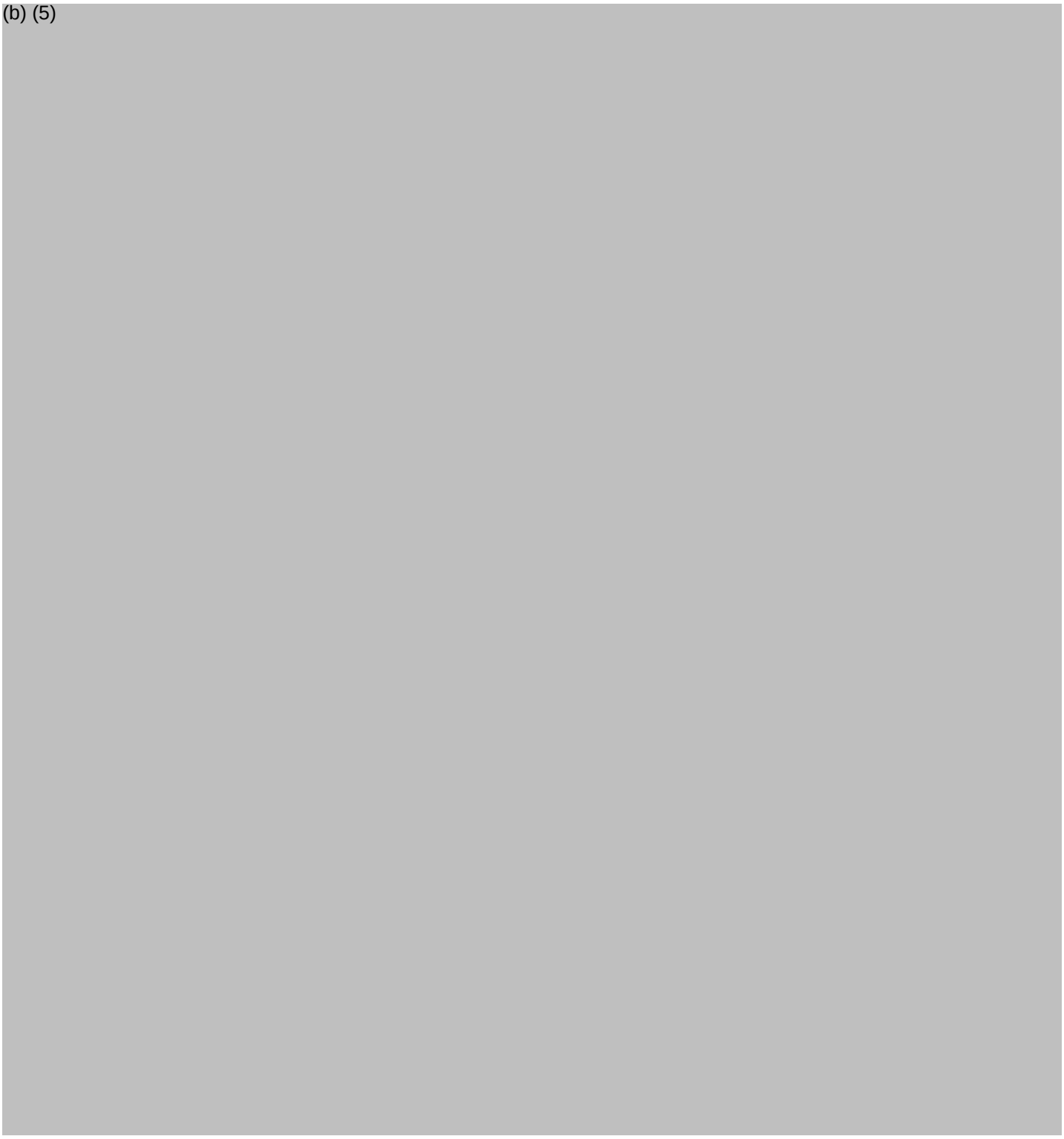
According to the most recent information from the GAO, at the National Credit Union Administration (NCUA), whites represent 88 percent of senior level management positions, compared to 4 percent represented by blacks and 4 percent by Hispanics. At the Office of the Comptroller of the Currency (OCC), whites represent 82 percent of senior level managers, compared to 9 percent black and 5 percent Hispanic. Whites represent 89 percent of senior level management positions at the Securities and Exchange Commission, compared to 2 percent black and 5 percent Hispanic. Minorities appear to fair best at the Federal Housing Finance Agency, where whites represent 76 percent of senior level management positions, compared to 16 percent black and 8 percent Hispanic. However, more comprehensive analysis is still needed from the agency to fully assess the racial and gender employment of minorities in senior positions beyond the GAO's limited information.

Accordingly, we request that the OIG examine any employee complaints, formal or informal, related to personnel practices, workplace policies and the findings from any employee satisfaction surveys, whether conducted by the Federal Reserve System or an outside entity. If the OIG identifies any individuals or groups of individuals who have exhibited discriminatory behaviors or patterns of unfair or unequal treatment, we ask that the OIG provide recommendations about appropriate actions, including remedial training or removal from employment with the agency. Furthermore, we request that the OIG assess the agency's OMWI operations, and ensure corrective actions are taken within the agency with regard to employee compensation, rating systems, retention, and promotion of women and minorities.

Sincerely,

Attachment B

(b) (5)



Office of Inspector General Statement of Independence for Individual Projects

Employees of the Office of Inspector General (OIG) or its contractors who are engaged in audit, attestation, inspection, evaluation, or investigative work are to conduct themselves in a manner consistent with the Federal Reserve Board's and OIG's core values, the "Ethics Handbook for Board Employees," the *Government Auditing Standards*, the *Quality Standards for Inspection and Evaluation*, and the standards applicable to their project. Employees of the OIG and its contractors must take precautions to ensure that their conduct is perceived as being independent, professional, and appropriate and are not to become involved in conflict-of-interest situations or situations that give the appearance that a conflict exists.

The OIG and its staff and contractors must be free from personal, external, and organizational impairments to independence and must avoid the appearance of such impairments of independence, so their work will be viewed as impartial by objective third parties. Employees of the OIG and its contractors should refer to the Quality Standards for Inspection and Evaluation and chapter 3 of the *Government Auditing Standards* for a comprehensive discussion of personal, external, and organizational impairments to independence. Impairments to independence include, but are not limited to:

- financial interest that is direct, or is significant/material though indirect, in the audited entity or program.
- seeking employment with the entity to be reviewed or under review.
- preconceived ideas toward individuals, groups, organizations, or objectives of a particular program that could bias the project.
- official, professional, personal, or financial relationships that might cause an employee of the OIG or its contractors to limit the extent of his/her inquiry, to limit disclosure, or to weaken or slant findings in any way.
- external interference or influence that improperly or imprudently limits or modifies the scope of project work.

Employees of the OIG and its contractors should be aware that independence impairments can occur because of the potential to develop close personal relationships with Board staff who work in program areas being audited or otherwise reviewed. Also, employees of the OIG and its contractors may wish to apply for job postings in other Board divisions at a time when they are assigned to or about to be assigned to review a program in that division. When these or other apparent or potential conflicts of interest occur, the individual should fully disclose the situation to the cognizant OIG manager. In consultation with the Inspector General, appropriate action by management might include reassigning the individual, limiting the individual's role, or providing additional reviews of the individual's work. Failure to comply with the OIG's policies and procedures regarding personal impairments may result in disciplinary action against the individual, consistent with the Board's Disciplinary Actions policy.

Instructions:

This form, which documents compliance with applicable independence standards, is to be completed at the start of each project by OIG or contractor project team members. The completed and signed form should be scanned into the project database. Individuals who are either not able to sign this statement or experience a situation in the future where they believe their independence and/or objectivity is or may be impaired should notify the cognizant OIG manager to discuss their situation. The Assistant Inspector General for Legal Services and the Board's Ethics Officer are also available for consultation.

- - - - - - - - - -

I have read the above and attest that I have neither personal nor external impairments to my independence that will keep me from objectively planning and conducting my work on this project and reaching independent conclusions based on the evidence. I will reevaluate my independence whenever my assignment is changed and whenever my circumstances change. If changes affecting either my independence or my objectivity occur subsequent to the completion of this form, I will promptly notify the cognizant OIG manager.

Project Name: Audit of the Board's Diversity and Inclusion Processes

Individual's Name: Jina Hwang

Date Individual Started Work on Project: 4/8/2014

Signature: _____ **Date:** 5/20/2014

Office of Inspector General Statement of Independence for Individual Projects

Employees of the Office of Inspector General (OIG) or its contractors who are engaged in audit, attestation, inspection, evaluation, or investigative work are to conduct themselves in a manner consistent with the Federal Reserve Board's and OIG's core values, the "Ethics Handbook for Board Employees," the *Government Auditing Standards*, the *Quality Standards for Inspection and Evaluation*, and the standards applicable to their project. Employees of the OIG and its contractors must take precautions to ensure that their conduct is perceived as being independent, professional, and appropriate and are not to become involved in conflict-of-interest situations or situations that give the appearance that a conflict exists.

The OIG and its staff and contractors must be free from personal, external, and organizational impairments to independence and must avoid the appearance of such impairments of independence, so their work will be viewed as impartial by objective third parties. Employees of the OIG and its contractors should refer to the Quality Standards for Inspection and Evaluation and chapter 3 of the *Government Auditing Standards* for a comprehensive discussion of personal, external, and organizational impairments to independence. Impairments to independence include, but are not limited to:

- financial interest that is direct, or is significant/material though indirect, in the audited entity or program.
- seeking employment with the entity to be reviewed or under review.
- preconceived ideas toward individuals, groups, organizations, or objectives of a particular program that could bias the project.
- official, professional, personal, or financial relationships that might cause an employee of the OIG or its contractors to limit the extent of his/her inquiry, to limit disclosure, or to weaken or slant findings in any way.
- external interference or influence that improperly or imprudently limits or modifies the scope of project work.

Employees of the OIG and its contractors should be aware that independence impairments can occur because of the potential to develop close personal relationships with Board staff who work in program areas being audited or otherwise reviewed. Also, employees of the OIG and its contractors may wish to apply for job postings in other Board divisions at a time when they are assigned to or about to be assigned to review a program in that division. When these or other apparent or potential conflicts of interest occur, the individual should fully disclose the situation to the cognizant OIG manager. In consultation with the Inspector General, appropriate action by management might include reassigning the individual, limiting the individual's role, or providing additional reviews of the individual's work. Failure to comply with the OIG's policies and procedures regarding personal impairments may result in disciplinary action against the individual, consistent with the Board's Disciplinary Actions policy.

Instructions:

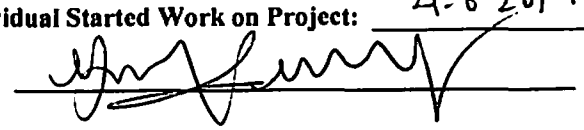
This form, which documents compliance with applicable independence standards, is to be completed at the start of each project by OIG or contractor project team members. The completed and signed form should be scanned into the project database. Individuals who are either not able to sign this statement or experience a situation in the future where they believe their independence and/or objectivity is or may be impaired should notify the cognizant OIG manager to discuss their situation. The Assistant Inspector General for Legal Services and the Board's Ethics Officer are also available for consultation.

I have read the above and attest that I have neither personal nor external impairments to my independence that will keep me from objectively planning and conducting my work on this project and reaching independent conclusions based on the evidence. I will reevaluate my independence whenever my assignment is changed and whenever my circumstances change. If changes affecting either my independence or my objectivity occur subsequent to the completion of this form, I will promptly notify the cognizant OIG manager.

Project Name: Audit of the Board's Diversity and Inclusion Processes

Individual's Name: Geeta Mullaney

Date Individual Started Work on Project: 4-8-2014

Signature:  **Date:** 5-22-2014

Entrance Conference for the Audit of the Board's Diversity and Inclusion Processes

Date: 5/12/2014

Participants:

- Donald Hammond, Chief Operating Officer, COO
- Michell Clark, Director, Management Division
- David Harmon, Deputy Director, Human Capital
- Shelia Clark, Program Director, Diversity and Inclusion
- Melissa Heist, Associate Inspector General, OIG
- Timothy Rogers, Senior Manager, OIG
- Kimberly Perteet, Senior Auditor, OIG
- Jina Hwang, Counsel, OIG
- Brian Murphy, Auditor, OIG
- Brandon Lee, Auditor, OIG

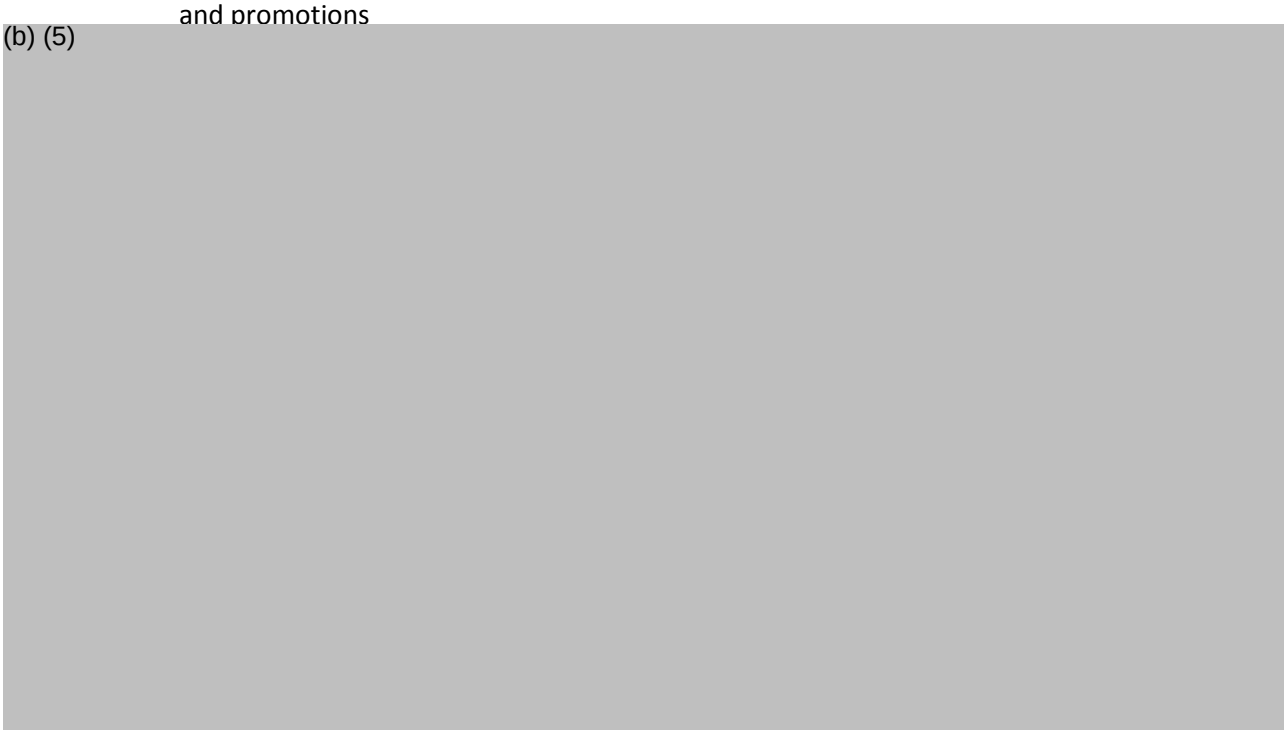
Meeting objective/Purpose:

The purpose of this meeting was to provide senior Management Division staff of objective, scope, methodology, and key dates related to the audit.

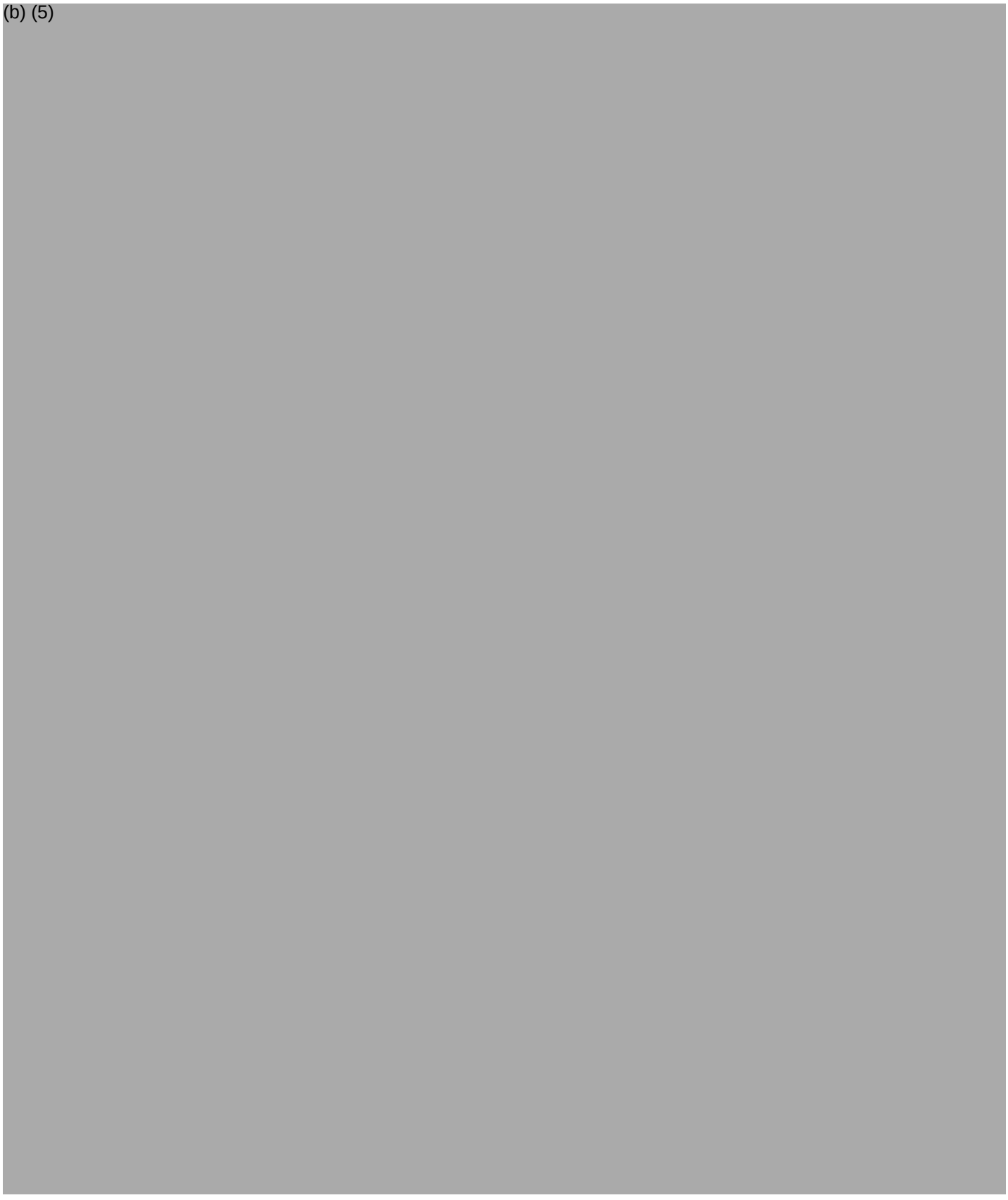
Minutes:

- The audit team presented an agenda and audit process documents.
- The team informed the auditees of the objective, scope and methodology.
    - The audit team mentioned policies, procedures, and internal controls will be examined during this audit.
    - Also, the audit team will analyze statistical trends related to EEO complaints, the PMP, and promotions

(b) (5)



(b) (5)



OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

May 12, 2014

SUBJECT: Entrance Conference for the Audit of the Board's Diversity and Inclusion Processes

Objective

Assess the Board's personnel operations and other efforts to provide equal employment opportunities, including equal opportunity for minorities and women to obtain senior management positions, and for racial, ethnic, and gender diversity in the workforce.

Scope

- Personnel activities from January 2011 through December 2013
- Changes to policies and procedures since December 2013

Methodology

- Interview various agency personnel
- Review personnel operations, policies and procedures, reports, existing statistics, and other relevant documentation
- Analyze data to identify statistical trends
- Conduct internal control testing to assess the adequacy of established controls

Key Dates

(b) (5)

OIG Contacts

- Primary contact:
  - Kimberly Perteet, Project Leader, (202) 973-7318, kimberly.l.perteet@frb.gov
  - Anna Saez, Project Manager, (202) 973-5027, annabelle.saez@frb.gov

- Additional contacts:
  - Brandon Lee, Auditor, (202) 973-7322, brandon.m.lee@frb.gov
  - Brian Murphy, Auditor, (202) 973-6179, brian.p.murphy@frb.gov
  - Tim Rogers, Senior OIG Manager for Management and Operations, (202) 973-5042, timothy.p.rogers@frb.gov
  - Melissa Heist, Associate Inspector General for Audits and Evaluations, (202) 973-5024, melissa.m.heist@frb.gov

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

Statement of Independence on Individual Projects

The Office of Inspector General (OIG) and its staff and contractors must be independent in all matters relating to audit, inspection, and evaluation work. OIG employees and contractors who are engaged in audits, inspections, or evaluations are to comply with the OIG policy AE-001, *Independence,* and conduct themselves in a manner consistent with the Board of Governors of the Federal Reserve System's (Board) and the OIG's core values; the Board's *Principles of Ethical Conduct*; the *Standards of Ethical Conduct for Employees of the Executive Branch,* issued by the U.S. Office of Government Ethics; the generally accepted government auditing standards (GAGAS), issued by the Comptroller General of the United States; *Quality Standards for Inspection and Evaluation*, issued by the Council of the Inspectors General on Integrity and Efficiency; and any other standards applicable to their project. OIG employees and contractors must take precautions to ensure that their conduct is perceived as being independent, professional, and appropriate and are not to become involved in situations that impair independence or give the appearance that impairment to independence exists.

Independence comprises independence of mind and independence in appearance. Independence of mind is the state of mind that permits the performance of an audit without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism. Independence in appearance is the absence of circumstances that would cause a reasonable and informed third party, having knowledge of the relevant information, to reasonably conclude that the integrity, objectivity, or professional skepticism of an audit organization or member of the audit team had been compromised (GAGAS 3.03).

GAGAS establishes the conceptual framework (see GAGAS 3.07–3.26 and appendix II) that OIG employees and contractors must use to identify and evaluate threats to independence given the circumstances of their work. Whether independence is impaired depends on the nature of the threat, whether the threat is of such significance that it would compromise an auditor's professional judgment or create the appearance that the auditor's professional judgment may be compromised, and the specific safeguards applied to eliminate the threat or reduce it to an acceptable level. GAGAS provides broad categories of threats (GAGAS 3.14) and examples of circumstances that create threats to independence (GAGAS A3.02–A3.09) and it describes safeguards that may be effective in certain circumstances (GAGAS 3.16–3.19).

Consistent with GAGAS 3.21, 3.64, and 3.65, auditors use professional judgment in applying the conceptual framework to determine independence in a given situation. When identifying and evaluating threats to independence, OIG employees and contractors must consider the broad

categories of threats to independence and the example safeguards provided in GAGAS, as well as the unique circumstances of the project. In addition to the GAGAS examples, specific situations that threaten independence and must be reported to the project manager or an appropriate official if the project manager is not available include the following:

- financial interest that is direct, or is significant or material though indirect, in the audited entity or program
- seeking employment with the division or program area to be reviewed or under review (including the time period leading up to the submission of a job application)
- preconceived ideas toward individuals, groups, organizations, or objectives of a particular program that could bias the project
- official, professional, personal, financial, or any kind of relationship that might cause an OIG employee or contractor to limit the extent of his or her inquiry, to limit disclosure, or to weaken or slant findings in any way
- external interference or influence that improperly or imprudently limits or modifies the scope of project work

When these or any other apparent or potential threats to independence are identified, the individual must immediately and fully disclose the situation to the project manager. The project manager, in consultation with the applicable Senior OIG Manager and Associate Inspector General, must determine whether identified threats to independence are significant and whether they can be reduced to an acceptable level with the imposition of safeguards. Any disclosed threats to independence and applied safeguards must be documented on this form (GAGAS 3.24). If the disclosed threats to independence are deemed insignificant, the basis for that determination must be documented on this form.

Failure to comply with the OIG's policies and procedures regarding independence may result in adverse or disciplinary action against the individual, up to and including termination, consistent with applicable Board policy.

Instructions

This form, which documents compliance with applicable independence standards, is to be completed at the start of each project by OIG or contractor project team members, as well as any OIG staff members who substantially contribute to the project in accordance with the OIG's *Independence* policy. Generally, the project's start date refers to the date the project is initiated in the audit system. A new form must be completed when circumstances change or when threats to independence arise that impact the individual's independence. In addition, this form must be completed by OIG referencers prior to their involvement in the project. The completed forms are maintained as electronic workpapers in the audit systems.

Certification

I certify that I have read and understand the above, as well as the OIG's *Independence* policy and GAGAS independence standards. With regard to the assigned project, I have evaluated threats to my independence, both independence of mind and in appearance, and attest that (select one):

☑ I have not identified any threats to my independence.

☐ I have identified threats to independence and applied safeguards, as described below.

Describe any threats to independence identified and safeguards applied (attach additional page if necessary).

☐ As a **referencer** for this project, I certify that I have not identified any threats to my independence that would prevent me from objectively performing the independent reference review.

I also agree to reevaluate my independence whenever my assignment is changed or whenever my circumstances change while working on this project. If changes affecting either my independence or my objectivity regarding this project occur subsequent to the completion of this form, I will immediately notify the project manager or an appropriate official if the project manager is not available.

Project name: 2014 Congressional Request on the Board's Personnel Practices

Individual's name: Sean Newman

Date individual started on project: 6/10/14

Signature: [signature] **Date:** 7/9/14

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

Statement of Independence on Individual Projects

The Office of Inspector General (OIG) and its staff and contractors must be independent in all matters relating to audit, inspection, and evaluation work. OIG employees and contractors who are engaged in audits, inspections, or evaluations are to comply with the OIG policy AE-001, *Independence,* and conduct themselves in a manner consistent with the Board of Governors of the Federal Reserve System's (Board) and the OIG's core values; the Board's *Principles of Ethical Conduct*; the *Standards of Ethical Conduct for Employees of the Executive Branch*, issued by the U.S. Office of Government Ethics; the generally accepted government auditing standards (GAGAS), issued by the Comptroller General of the United States; *Quality Standards for Inspection and Evaluation*, issued by the Council of the Inspectors General on Integrity and Efficiency; and any other standards applicable to their project. OIG employees and contractors must take precautions to ensure that their conduct is perceived as being independent, professional, and appropriate and are not to become involved in situations that impair independence or give the appearance that impairment to independence exists.

Independence comprises independence of mind and independence in appearance. Independence of mind is the state of mind that permits the performance of an audit without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism. Independence in appearance is the absence of circumstances that would cause a reasonable and informed third party, having knowledge of the relevant information, to reasonably conclude that the integrity, objectivity, or professional skepticism of an audit organization or member of the audit team had been compromised (GAGAS 3.03).

GAGAS establishes the conceptual framework (see GAGAS 3.07–3.26 and appendix II) that OIG employees and contractors must use to identify and evaluate threats to independence given the circumstances of their work. Whether independence is impaired depends on the nature of the threat, whether the threat is of such significance that it would compromise an auditor's professional judgment or create the appearance that the auditor's professional judgment may be compromised, and the specific safeguards applied to eliminate the threat or reduce it to an acceptable level. GAGAS provides broad categories of threats (GAGAS 3.14) and examples of circumstances that create threats to independence (GAGAS A3.02–A3.09) and it describes safeguards that may be effective in certain circumstances (GAGAS 3.16–3.19).

Consistent with GAGAS 3.21, 3.64, and 3.65, auditors use professional judgment in applying the conceptual framework to determine independence in a given situation. When identifying and evaluating threats to independence, OIG employees and contractors must consider the broad

categories of threats to independence and the example safeguards provided in GAGAS, as well as the unique circumstances of the project. In addition to the GAGAS examples, specific situations that threaten independence and must be reported to the project manager or an appropriate official if the project manager is not available include the following:

- financial interest that is direct, or is significant or material though indirect, in the audited entity or program
- seeking employment with the division or program area to be reviewed or under review (including the time period leading up to the submission of a job application)
- preconceived ideas toward individuals, groups, organizations, or objectives of a particular program that could bias the project
- official, professional, personal, financial, or any kind of relationship that might cause an OIG employee or contractor to limit the extent of his or her inquiry, to limit disclosure, or to weaken or slant findings in any way
- external interference or influence that improperly or imprudently limits or modifies the scope of project work

When these or any other apparent or potential threats to independence are identified, the individual must immediately and fully disclose the situation to the project manager. The project manager, in consultation with the applicable Senior OIG Manager and Associate Inspector General, must determine whether identified threats to independence are significant and whether they can be reduced to an acceptable level with the imposition of safeguards. Any disclosed threats to independence and applied safeguards must be documented on this form (GAGAS 3.24). If the disclosed threats to independence are deemed insignificant, the basis for that determination must be documented on this form.

Failure to comply with the OIG's policies and procedures regarding independence may result in adverse or disciplinary action against the individual, up to and including termination, consistent with applicable Board policy.

Instructions

This form, which documents compliance with applicable independence standards, is to be completed at the start of each project by OIG or contractor project team members, as well as any OIG staff members who substantially contribute to the project in accordance with the OIG's *Independence* policy. Generally, the project's start date refers to the date the project is initiated in the audit system. A new form must be completed when circumstances change or when threats to independence arise that impact the individual's independence. In addition, this form must be completed by OIG referencers prior to their involvement in the project. The completed forms are maintained as electronic workpapers in the audit systems.

Certification

I certify that I have read and understand the above, as well as the OIG's *Independence* policy and GAGAS independence standards. With regard to the assigned project, I have evaluated threats to my independence, both independence of mind and in appearance, and attest that (select one):

☒ I have not identified any threats to my independence.

☐ I have identified threats to independence and applied safeguards, as described below.

Describe any threats to independence identified and safeguards applied (attach additional page if necessary).

☐ As a **referencer** for this project, I certify that I have not identified any threats to my independence that would prevent me from objectively performing the independent reference review.

I also agree to reevaluate my independence whenever my assignment is changed or whenever my circumstances change while working on this project. If changes affecting either my independence or my objectivity regarding this project occur subsequent to the completion of this form, I will immediately notify the project manager or an appropriate official if the project manager is not available.

Project name: 2014 Congressional Request on the Board's Personnel Practices

Individual's name: Victor Calderon

Date individual started on project: 6/27/14

Signature: _____ **Date:** 7/22/14

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

Statement of Independence on Individual Projects

The Office of Inspector General (OIG) and its staff and contractors must be independent in all matters relating to audit, inspection, and evaluation work. OIG employees and contractors who are engaged in audits, inspections, or evaluations are to comply with the OIG policy AE-001, *Independence,* and conduct themselves in a manner consistent with the Board of Governors of the Federal Reserve System's (Board) and the OIG's core values; the Board's *Principles of Ethical Conduct*; the *Standards of Ethical Conduct for Employees of the Executive Branch*, issued by the U.S. Office of Government Ethics; the generally accepted government auditing standards (GAGAS), issued by the Comptroller General of the United States; *Quality Standards for Inspection and Evaluation*, issued by the Council of the Inspectors General on Integrity and Efficiency; and any other standards applicable to their project. OIG employees and contractors must take precautions to ensure that their conduct is perceived as being independent, professional, and appropriate and are not to become involved in situations that impair independence or give the appearance that impairment to independence exists.

Independence comprises independence of mind and independence in appearance. Independence of mind is the state of mind that permits the performance of an audit without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism. Independence in appearance is the absence of circumstances that would cause a reasonable and informed third party, having knowledge of the relevant information, to reasonably conclude that the integrity, objectivity, or professional skepticism of an audit organization or member of the audit team had been compromised (GAGAS 3.03).

GAGAS establishes the conceptual framework (see GAGAS 3.07–3.26 and appendix II) that OIG employees and contractors must use to identify and evaluate threats to independence given the circumstances of their work. Whether independence is impaired depends on the nature of the threat, whether the threat is of such significance that it would compromise an auditor's professional judgment or create the appearance that the auditor's professional judgment may be compromised, and the specific safeguards applied to eliminate the threat or reduce it to an acceptable level. GAGAS provides broad categories of threats (GAGAS 3.14) and examples of circumstances that create threats to independence (GAGAS A3.02–A3.09) and it describes safeguards that may be effective in certain circumstances (GAGAS 3.16–3.19).

Consistent with GAGAS 3.21, 3.64, and 3.65, auditors use professional judgment in applying the conceptual framework to determine independence in a given situation. When identifying and evaluating threats to independence, OIG employees and contractors must consider the broad

categories of threats to independence and the example safeguards provided in GAGAS, as well as the unique circumstances of the project. In addition to the GAGAS examples, specific situations that threaten independence and must be reported to the project manager or an appropriate official if the project manager is not available include the following:

- financial interest that is direct, or is significant or material though indirect, in the audited entity or program
- seeking employment with the division or program area to be reviewed or under review (including the time period leading up to the submission of a job application)
- preconceived ideas toward individuals, groups, organizations, or objectives of a particular program that could bias the project
- official, professional, personal, financial, or any kind of relationship that might cause an OIG employee or contractor to limit the extent of his or her inquiry, to limit disclosure, or to weaken or slant findings in any way
- external interference or influence that improperly or imprudently limits or modifies the scope of project work

When these or any other apparent or potential threats to independence are identified, the individual must immediately and fully disclose the situation to the project manager. The project manager, in consultation with the applicable Senior OIG Manager and Associate Inspector General, must determine whether identified threats to independence are significant and whether they can be reduced to an acceptable level with the imposition of safeguards. Any disclosed threats to independence and applied safeguards must be documented on this form (GAGAS 3.24). If the disclosed threats to independence are deemed insignificant, the basis for that determination must be documented on this form.

Failure to comply with the OIG's policies and procedures regarding independence may result in adverse or disciplinary action against the individual, up to and including termination, consistent with applicable Board policy.

Instructions

This form, which documents compliance with applicable independence standards, is to be completed at the start of each project by OIG or contractor project team members, as well as any OIG staff members who substantially contribute to the project in accordance with the OIG's *Independence* policy. Generally, the project's start date refers to the date the project is initiated in the audit system. A new form must be completed when circumstances change or when threats to independence arise that impact the individual's independence. In addition, this form must be completed by OIG referencers prior to their involvement in the project. The completed forms are maintained as electronic workpapers in the audit systems.

Certification

I certify that I have read and understand the above, as well as the OIG's *Independence* policy and GAGAS independence standards. With regard to the assigned project, I have evaluated threats to my independence, both independence of mind and in appearance, and attest that (select one):

☑ I have not identified any threats to my independence.

☐ I have identified threats to independence and applied safeguards, as described below.

Describe any threats to independence identified and safeguards applied (attach additional page if necessary).

☐ As a **referencer** for this project, I certify that I have not identified any threats to my independence that would prevent me from objectively performing the independent reference review.

I also agree to reevaluate my independence whenever my assignment is changed or whenever my circumstances change while working on this project. If changes affecting either my independence or my objectivity regarding this project occur subsequent to the completion of this form, I will immediately notify the project manager or an appropriate official if the project manager is not available.

Project name: 2014 Congressional Request on the Board's Personnel Practices

Individual's name: Jina Hwang

Date individual started on project: 4/8/2014

Signature: [signature] **Date:** 7/24/2014

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

Statement of Independence on Individual Projects

The Office of Inspector General (OIG) and its staff and contractors must be independent in all matters relating to audit, inspection, and evaluation work. OIG employees and contractors who are engaged in audits, inspections, or evaluations are to comply with the OIG policy AE-001, *Independence,* and conduct themselves in a manner consistent with the Board of Governors of the Federal Reserve System's (Board) and the OIG's core values; the Board's *Principles of Ethical Conduct*; the *Standards of Ethical Conduct for Employees of the Executive Branch*, issued by the U.S. Office of Government Ethics; the generally accepted government auditing standards (GAGAS), issued by the Comptroller General of the United States; *Quality Standards for Inspection and Evaluation*, issued by the Council of the Inspectors General on Integrity and Efficiency; and any other standards applicable to their project. OIG employees and contractors must take precautions to ensure that their conduct is perceived as being independent, professional, and appropriate and are not to become involved in situations that impair independence or give the appearance that impairment to independence exists.

Independence comprises independence of mind and independence in appearance. Independence of mind is the state of mind that permits the performance of an audit without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism. Independence in appearance is the absence of circumstances that would cause a reasonable and informed third party, having knowledge of the relevant information, to reasonably conclude that the integrity, objectivity, or professional skepticism of an audit organization or member of the audit team had been compromised (GAGAS 3.03).

GAGAS establishes the conceptual framework (see GAGAS 3.07–3.26 and appendix II) that OIG employees and contractors must use to identify and evaluate threats to independence given the circumstances of their work. Whether independence is impaired depends on the nature of the threat, whether the threat is of such significance that it would compromise an auditor's professional judgment or create the appearance that the auditor's professional judgment may be compromised, and the specific safeguards applied to eliminate the threat or reduce it to an acceptable level. GAGAS provides broad categories of threats (GAGAS 3.14) and examples of circumstances that create threats to independence (GAGAS A3.02–A3.09) and it describes safeguards that may be effective in certain circumstances (GAGAS 3.16–3.19).

Consistent with GAGAS 3.21, 3.64, and 3.65, auditors use professional judgment in applying the conceptual framework to determine independence in a given situation. When identifying and evaluating threats to independence, OIG employees and contractors must consider the broad

categories of threats to independence and the example safeguards provided in GAGAS, as well as the unique circumstances of the project. In addition to the GAGAS examples, specific situations that threaten independence and must be reported to the project manager or an appropriate official if the project manager is not available include the following:

- financial interest that is direct, or is significant or material though indirect, in the audited entity or program
- seeking employment with the division or program area to be reviewed or under review (including the time period leading up to the submission of a job application)
- preconceived ideas toward individuals, groups, organizations, or objectives of a particular program that could bias the project
- official, professional, personal, financial, or any kind of relationship that might cause an OIG employee or contractor to limit the extent of his or her inquiry, to limit disclosure, or to weaken or slant findings in any way
- external interference or influence that improperly or imprudently limits or modifies the scope of project work

When these or any other apparent or potential threats to independence are identified, the individual must immediately and fully disclose the situation to the project manager. The project manager, in consultation with the applicable Senior OIG Manager and Associate Inspector General, must determine whether identified threats to independence are significant and whether they can be reduced to an acceptable level with the imposition of safeguards. Any disclosed threats to independence and applied safeguards must be documented on this form (GAGAS 3.24). If the disclosed threats to independence are deemed insignificant, the basis for that determination must be documented on this form.

Failure to comply with the OIG's policies and procedures regarding independence may result in adverse or disciplinary action against the individual, up to and including termination, consistent with applicable Board policy.

Instructions

This form, which documents compliance with applicable independence standards, is to be completed at the start of each project by OIG or contractor project team members, as well as any OIG staff members who substantially contribute to the project in accordance with the OIG's *Independence* policy. Generally, the project's start date refers to the date the project is initiated in the audit system. A new form must be completed when circumstances change or when threats to independence arise that impact the individual's independence. In addition, this form must be completed by OIG referencers prior to their involvement in the project. The completed forms are maintained as electronic workpapers in the audit systems.

Certification

I certify that I have read and understand the above, as well as the OIG's *Independence* policy and GAGAS independence standards. With regard to the assigned project, I have evaluated threats to my independence, both independence of mind and in appearance, and attest that (select one):

☑ I have not identified any threats to my independence.

☐ I have identified threats to independence and applied safeguards, as described below.

Describe any threats to independence identified and safeguards applied (attach additional page if necessary).

☐ As a **referencer** for this project, I certify that I have not identified any threats to my independence that would prevent me from objectively performing the independent reference review.

I also agree to reevaluate my independence whenever my assignment is changed or whenever my circumstances change while working on this project. If changes affecting either my independence or my objectivity regarding this project occur subsequent to the completion of this form, I will immediately notify the project manager or an appropriate official if the project manager is not available.

Project name: 2014 Congressional Request on the Board's Personnel Practices

Individual's name: Geeta Mullaney

Date individual started on project: 6-24-2014

Signature: _____ **Date:** 7-25-2014

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

Statement of Independence on Individual Projects

The Office of Inspector General (OIG) and its staff and contractors must be independent in all matters relating to audit, inspection, and evaluation work. OIG employees and contractors who are engaged in audits, inspections, or evaluations are to comply with the OIG policy AE-001, *Independence,* and conduct themselves in a manner consistent with the Board of Governors of the Federal Reserve System's (Board) and the OIG's core values; the Board's *Principles of Ethical Conduct*; the *Standards of Ethical Conduct for Employees of the Executive Branch,* issued by the U.S. Office of Government Ethics; the generally accepted government auditing standards (GAGAS), issued by the Comptroller General of the United States; *Quality Standards for Inspection and Evaluation*, issued by the Council of the Inspectors General on Integrity and Efficiency; and any other standards applicable to their project. OIG employees and contractors must take precautions to ensure that their conduct is perceived as being independent, professional, and appropriate and are not to become involved in situations that impair independence or give the appearance that impairment to independence exists.

Independence comprises independence of mind and independence in appearance. Independence of mind is the state of mind that permits the performance of an audit without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism. Independence in appearance is the absence of circumstances that would cause a reasonable and informed third party, having knowledge of the relevant information, to reasonably conclude that the integrity, objectivity, or professional skepticism of an audit organization or member of the audit team had been compromised (GAGAS 3.03).

GAGAS establishes the conceptual framework (see GAGAS 3.07–3.26 and appendix II) that OIG employees and contractors must use to identify and evaluate threats to independence given the circumstances of their work. Whether independence is impaired depends on the nature of the threat, whether the threat is of such significance that it would compromise an auditor's professional judgment or create the appearance that the auditor's professional judgment may be compromised, and the specific safeguards applied to eliminate the threat or reduce it to an acceptable level. GAGAS provides broad categories of threats (GAGAS 3.14) and examples of circumstances that create threats to independence (GAGAS A3.02–A3.09) and it describes safeguards that may be effective in certain circumstances (GAGAS 3.16–3.19).

Consistent with GAGAS 3.21, 3.64, and 3.65, auditors use professional judgment in applying the conceptual framework to determine independence in a given situation. When identifying and evaluating threats to independence, OIG employees and contractors must consider the broad

categories of threats to independence and the example safeguards provided in GAGAS, as well as the unique circumstances of the project. In addition to the GAGAS examples, specific situations that threaten independence and must be reported to the project manager or an appropriate official if the project manager is not available include the following:

- financial interest that is direct, or is significant or material though indirect, in the audited entity or program
- seeking employment with the division or program area to be reviewed or under review (including the time period leading up to the submission of a job application)
- preconceived ideas toward individuals, groups, organizations, or objectives of a particular program that could bias the project
- official, professional, personal, financial, or any kind of relationship that might cause an OIG employee or contractor to limit the extent of his or her inquiry, to limit disclosure, or to weaken or slant findings in any way
- external interference or influence that improperly or imprudently limits or modifies the scope of project work

When these or any other apparent or potential threats to independence are identified, the individual must immediately and fully disclose the situation to the project manager. The project manager, in consultation with the applicable Senior OIG Manager and Associate Inspector General, must determine whether identified threats to independence are significant and whether they can be reduced to an acceptable level with the imposition of safeguards. Any disclosed threats to independence and applied safeguards must be documented on this form (GAGAS 3.24). If the disclosed threats to independence are deemed insignificant, the basis for that determination must be documented on this form.

Failure to comply with the OIG's policies and procedures regarding independence may result in adverse or disciplinary action against the individual, up to and including termination, consistent with applicable Board policy.

Instructions

This form, which documents compliance with applicable independence standards, is to be completed at the start of each project by OIG or contractor project team members, as well as any OIG staff members who substantially contribute to the project in accordance with the OIG's *Independence* policy. Generally, the project's start date refers to the date the project is initiated in the audit system. A new form must be completed when circumstances change or when threats to independence arise that impact the individual's independence. In addition, this form must be completed by OIG referencers prior to their involvement in the project. The completed forms are maintained as electronic workpapers in the audit systems.

Certification

I certify that I have read and understand the above, as well as the OIG's *Independence* policy and GAGAS independence standards. With regard to the assigned project, I have evaluated threats to my independence, both independence of mind and in appearance, and attest that (select one):

☑ I have not identified any threats to my independence.

☐ I have identified threats to independence and applied safeguards, as described below.

Describe any threats to independence identified and safeguards applied (attach additional page if necessary).

☐ As a **referencer** for this project, I certify that I have not identified any threats to my independence that would prevent me from objectively performing the independent reference review.

I also agree to reevaluate my independence whenever my assignment is changed or whenever my circumstances change while working on this project. If changes affecting either my independence or my objectivity regarding this project occur subsequent to the completion of this form, I will immediately notify the project manager or an appropriate official if the project manager is not available.

Project name: 2014 Congressional Request on the Board's Personnel Practices

Individual's name: Melissa Hasl

Date individual started on project: 4/8/14

Signature: Melissa Hasl **Date:** 9/23/14

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

Statement of Independence on Individual Projects

The Office of Inspector General (OIG) and its staff and contractors must be independent in all matters relating to audit, inspection, and evaluation work. OIG employees and contractors who are engaged in audits, inspections, or evaluations are to comply with the OIG policy AE-001, *Independence,* and conduct themselves in a manner consistent with the Board of Governors of the Federal Reserve System's (Board) and the OIG's core values; the Board's *Principles of Ethical Conduct*; the *Standards of Ethical Conduct for Employees of the Executive Branch,* issued by the U.S. Office of Government Ethics; the generally accepted government auditing standards (GAGAS), issued by the Comptroller General of the United States; *Quality Standards for Inspection and Evaluation,* issued by the Council of the Inspectors General on Integrity and Efficiency; and any other standards applicable to their project. OIG employees and contractors must take precautions to ensure that their conduct is perceived as being independent, professional, and appropriate and are not to become involved in situations that impair independence or give the appearance that impairment to independence exists.

Independence comprises independence of mind and independence in appearance. Independence of mind is the state of mind that permits the performance of an audit without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism. Independence in appearance is the absence of circumstances that would cause a reasonable and informed third party, having knowledge of the relevant information, to reasonably conclude that the integrity, objectivity, or professional skepticism of an audit organization or member of the audit team had been compromised (GAGAS 3.03).

GAGAS establishes the conceptual framework (see GAGAS 3.07–3.26 and appendix II) that OIG employees and contractors must use to identify and evaluate threats to independence given the circumstances of their work. Whether independence is impaired depends on the nature of the threat, whether the threat is of such significance that it would compromise an auditor's professional judgment or create the appearance that the auditor's professional judgment may be compromised, and the specific safeguards applied to eliminate the threat or reduce it to an acceptable level. GAGAS provides broad categories of threats (GAGAS 3.14) and examples of circumstances that create threats to independence (GAGAS A3.02–A3.09) and it describes safeguards that may be effective in certain circumstances (GAGAS 3.16–3.19).

Consistent with GAGAS 3.21, 3.64, and 3.65, auditors use professional judgment in applying the conceptual framework to determine independence in a given situation. When identifying and evaluating threats to independence, OIG employees and contractors must consider the broad

categories of threats to independence and the example safeguards provided in GAGAS, as well as the unique circumstances of the project. In addition to the GAGAS examples, specific situations that threaten independence and must be reported to the project manager or an appropriate official if the project manager is not available include the following:

- financial interest that is direct, or is significant or material though indirect, in the audited entity or program
- seeking employment with the division or program area to be reviewed or under review (including the time period leading up to the submission of a job application)
- preconceived ideas toward individuals, groups, organizations, or objectives of a particular program that could bias the project
- official, professional, personal, financial, or any kind of relationship that might cause an OIG employee or contractor to limit the extent of his or her inquiry, to limit disclosure, or to weaken or slant findings in any way
- external interference or influence that improperly or imprudently limits or modifies the scope of project work

When these or any other apparent or potential threats to independence are identified, the individual must immediately and fully disclose the situation to the project manager. The project manager, in consultation with the applicable Senior OIG Manager and Associate Inspector General, must determine whether identified threats to independence are significant and whether they can be reduced to an acceptable level with the imposition of safeguards. Any disclosed threats to independence and applied safeguards must be documented on this form (GAGAS 3.24). If the disclosed threats to independence are deemed insignificant, the basis for that determination must be documented on this form.

Failure to comply with the OIG's policies and procedures regarding independence may result in adverse or disciplinary action against the individual, up to and including termination, consistent with applicable Board policy.

Instructions

This form, which documents compliance with applicable independence standards, is to be completed at the start of each project by OIG or contractor project team members, as well as any OIG staff members who substantially contribute to the project in accordance with the OIG's *Independence* policy. Generally, the project's start date refers to the date the project is initiated in the audit system. A new form must be completed when circumstances change or when threats to independence arise that impact the individual's independence. In addition, this form must be completed by OIG referencers prior to their involvement in the project. The completed forms are maintained as electronic workpapers in the audit systems.

Certification

I certify that I have read and understand the above, as well as the OIG's *Independence* policy and GAGAS independence standards. With regard to the assigned project, I have evaluated threats to my independence, both independence of mind and in appearance, and attest that (select one):

☑ I have not identified any threats to my independence.

☐ I have identified threats to independence and applied safeguards, as described below.

Describe any threats to independence identified and safeguards applied (attach additional page if necessary).

☐ As a **referencer** for this project, I certify that I have not identified any threats to my independence that would prevent me from objectively performing the independent reference review.

I also agree to reevaluate my independence whenever my assignment is changed or whenever my circumstances change while working on this project. If changes affecting either my independence or my objectivity regarding this project occur subsequent to the completion of this form, I will immediately notify the project manager or an appropriate official if the project manager is not available.

Project name: Audit of the Board's Diversity and Inclusion Processes

Individual's name: Christopher Lyons

Date individual started on project: 10/23/14

Signature: _____ **Date:** 10/23/14

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

Statement of Independence on Individual Projects

The Office of Inspector General (OIG) and its staff and contractors must be independent in all matters relating to audit, inspection, and evaluation work. OIG employees and contractors who are engaged in audits, inspections, or evaluations are to comply with the OIG policy AE-001, *Independence,* and conduct themselves in a manner consistent with the Board of Governors of the Federal Reserve System's (Board) and the OIG's core values; the Board's *Principles of Ethical Conduct*; the *Standards of Ethical Conduct for Employees of the Executive Branch*, issued by the U.S. Office of Government Ethics; the generally accepted government auditing standards (GAGAS), issued by the Comptroller General of the United States; *Quality Standards for Inspection and Evaluation*, issued by the Council of the Inspectors General on Integrity and Efficiency; and any other standards applicable to their project. OIG employees and contractors must take precautions to ensure that their conduct is perceived as being independent, professional, and appropriate and are not to become involved in situations that impair independence or give the appearance that impairment to independence exists.

Independence comprises independence of mind and independence in appearance. Independence of mind is the state of mind that permits the performance of an audit without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism. Independence in appearance is the absence of circumstances that would cause a reasonable and informed third party, having knowledge of the relevant information, to reasonably conclude that the integrity, objectivity, or professional skepticism of an audit organization or member of the audit team had been compromised (GAGAS 3.03).

GAGAS establishes the conceptual framework (see GAGAS 3.07–3.26 and appendix II) that OIG employees and contractors must use to identify and evaluate threats to independence given the circumstances of their work. Whether independence is impaired depends on the nature of the threat, whether the threat is of such significance that it would compromise an auditor's professional judgment or create the appearance that the auditor's professional judgment may be compromised, and the specific safeguards applied to eliminate the threat or reduce it to an acceptable level. GAGAS provides broad categories of threats (GAGAS 3.14) and examples of circumstances that create threats to independence (GAGAS A3.02–A3.09) and it describes safeguards that may be effective in certain circumstances (GAGAS 3.16–3.19).

Consistent with GAGAS 3.21, 3.64, and 3.65, auditors use professional judgment in applying the conceptual framework to determine independence in a given situation. When identifying and evaluating threats to independence, OIG employees and contractors must consider the broad

categories of threats to independence and the example safeguards provided in GAGAS, as well as the unique circumstances of the project. In addition to the GAGAS examples, specific situations that threaten independence and must be reported to the project manager or an appropriate official if the project manager is not available include the following:

- financial interest that is direct, or is significant or material though indirect, in the audited entity or program
- seeking employment with the division or program area to be reviewed or under review (including the time period leading up to the submission of a job application)
- preconceived ideas toward individuals, groups, organizations, or objectives of a particular program that could bias the project
- official, professional, personal, financial, or any kind of relationship that might cause an OIG employee or contractor to limit the extent of his or her inquiry, to limit disclosure, or to weaken or slant findings in any way
- external interference or influence that improperly or imprudently limits or modifies the scope of project work

When these or any other apparent or potential threats to independence are identified, the individual must immediately and fully disclose the situation to the project manager. The project manager, in consultation with the applicable Senior OIG Manager and Associate Inspector General, must determine whether identified threats to independence are significant and whether they can be reduced to an acceptable level with the imposition of safeguards. Any disclosed threats to independence and applied safeguards must be documented on this form (GAGAS 3.24). If the disclosed threats to independence are deemed insignificant, the basis for that determination must be documented on this form.

Failure to comply with the OIG's policies and procedures regarding independence may result in adverse or disciplinary action against the individual, up to and including termination, consistent with applicable Board policy.

Instructions

This form, which documents compliance with applicable independence standards, is to be completed at the start of each project by OIG or contractor project team members, as well as any OIG staff members who substantially contribute to the project in accordance with the OIG's *Independence* policy. Generally, the project's start date refers to the date the project is initiated in the audit system. A new form must be completed when circumstances change or when threats to independence arise that impact the individual's independence. In addition, this form must be completed by OIG referencers prior to their involvement in the project. The completed forms are maintained as electronic workpapers in the audit systems.

Certification

I certify that I have read and understand the above, as well as the OIG's *Independence* policy and GAGAS independence standards. With regard to the assigned project, I have evaluated threats to my independence, both independence of mind and in appearance, and attest that (select one):

☐ I have not identified any threats to my independence.

☐ I have identified threats to independence and applied safeguards, as described below.

Describe any threats to independence identified and safeguards applied (attach additional page if necessary).

☒ As a **referencer** for this project, I certify that I have not identified any threats to my independence that would prevent me from objectively performing the independent reference review.

I also agree to reevaluate my independence whenever my assignment is changed or whenever my circumstances change while working on this project. If changes affecting either my independence or my objectivity regarding this project occur subsequent to the completion of this form, I will immediately notify the project manager or an appropriate official if the project manager is not available.

Project name: The Board Can Enhance Its Diversity & Inclusion Efforts

Individual's name: Brenda M Rohm

Date individual started on project: 1-16-2015

Signature: Brenda M Rohm **Date:** 1-16-2015

From:	Tim Rogers
To:	Donald Hammond; Steven Kamin; Thomas Laubach; Nellie Liang; David Wilcox
Cc:	Michell Clark; David Harmon; Sheila Clark; Lil Shewmaker; Tony Ogden; Melissa Heist; Mark Bialek; Anna Saez; Kimberly Perteet
Subject:	OIG Discussion Draft Report - Board Diversity and Inclusion [FRSONLY]
Date:	Wednesday, March 04, 2015 4:35:24 PM
Attachments:	OIG Board Discussion Draft Report Diversity and Inclusion 3_4_2015.pdf

RESTRICTED FR

Restricted-FR

Good afternoon,

We are providing the attached discussion draft report on our audit related to the Board's diversity and inclusion efforts, *The Board Can Enhance its Diversity and Inclusion Efforts,* for your review. Our report is in response to the congressional letter that we received in March 2014 requesting our review of areas within the Board related to diversity and inclusion, including performance management, employee complaint handling, and recruiting and hiring, among others. The report includes recommendations designed to enhance and promote diversity and inclusion, as well as to strengthen related controls. The discussion draft will be used to facilitate our exit conference, to be scheduled for next week. Should you have any questions, please contact Anna Saez, OIG Manager, at 202-973-5027, or me at 202-973-5042.

Because the draft report is still subject to revision, please appropriately safeguard the report to prevent premature disclosure. We appreciate the cooperation we have received from many staff throughout the Board, and look forward to meeting with you to discuss the diversity and inclusion draft report.

Regards,

Tim Rogers

Timothy Rogers | Sr. OIG Manager for Management and Operations
Audits and Evaluations
Office of Inspector General
Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-5042 | c: 202-450-7792 | timothy.p.rogers@frb.gov

From: Melissa Heist
To: Tim Rogers; Anna Saez; Kimberly Perteet; Brian Murphy; Sean Newman; Sopeany Keo
Cc: Matt Simber
Subject: FW: OIG Draft Report on Board Diversity and Inclusion Efforts [FRSONLY]
Date: Thursday, March 19, 2015 3:59:10 PM
Attachments: OIG Draft Report for Official Comment_Board Diversity_03-19-15.pdf

---

INTERNAL FR

Thank you so much! I hope you'll now be able to have the really great weekend you all deserve.

Melissa

Melissa M. Heist | Associate Inspector General for Audits and Evaluations
Office of Inspector General
Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-5024 | c: 202-689-9189 | f: 202-973-5044 | melissa.m.heist@frb.gov
OIG Hotline: 800-827-3340 | oighotline@frb.gov

www.federalreserve.gov/oig

From: Melissa Heist
Sent: Thursday, March 19, 2015 3:53 PM
To: Donald Hammond; Steven Kamin; Thomas Laubach; Nellie Liang; David Wilcox
Cc: David Harmon; Sheila Clark; Michell Clark; Lil Shewmaker; Scott Alvarez; Tony Ogden; Kit Wheatley
Subject: OIG Draft Report on Board Diversity and Inclusion Efforts [FRSONLY]

INTERNAL FR

Good Afternoon,

We are providing for your comment the attached draft report on our audit of the Board's diversity and inclusion efforts. We greatly appreciate the cooperation and support provided by you and your staff during this audit. The Congressional requestor for this audit has asked that we issue this report by March 31, so we are requesting you provide your written comments by Thursday, March 26, 2015. If you or your staff have any questions, please feel free to contact me or Tim Rogers, Senior OIG Manager, at 202-973-5042.

Thank you,
Melissa

Melissa M. Heist | Associate Inspector General for Audits and Evaluations
Office of Inspector General
Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-5024 | c: 202-689-9189 | f: 202-973-5044 | melissa.m.heist@frb.gov
OIG Hotline: 800-827-3340 | oighotline@frb.gov

www.federalreserve.gov/oig

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

To assess the Board's personnel operations and other efforts to provide for equal employment opportunities, including equal opportunity for minorities and women to obtain senior management positions, and increase racial, ethnic, and gender diversity in the workforce.

To answer our objective, we will:

- analyze information related to trend statistics for minority and women employees (e.g., performance management and recognition results, promotions, and representation at all levels of the agency); informal and formal EEO complaint statistics; and employee satisfaction survey results to determine whether this information suggests disparities in race/ethnicity, gender or age.
- review relevant agency personnel operations, policies, and procedures (e.g., performance management, recruitment and hiring practices, and promotion) to determine whether adequate controls are established to prevent and detect bias or discrimination
- assess the agency's efforts to respond to complaints, employee satisfaction survey results, or other potential indications of bias or discrimination and to increase diversity throughout the agency
- evaluate the Office of Minority and Women Inclusion's (OMWI) role and involvement in monitoring the impact of the Board's personnel policies on minorities and women, as well as monitoring the Board's efforts to increase diversity in senior management positions
- identify factors that may impact the Board's ability to increase diversity in senior management positions

Fieldwork Program: Personnel Operations, Policies, and Procedures

Procedure Title	Record of Work Done	Comments Where Applicable	Auditor-in-Charge

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

Hiring - Gain an Understanding of the Process	(b) (5)	Sean Newman
For Divisions that exclude Human Capital in Some Hiring Processes		Kim Perteet Sopeany Keo
Hiring - Test Compliance with Applicable Laws, Regulations, and Best Practices		Kim Perteet Sopeany Keo
Hiring - Test Internal Controls		Sean Newman Sopeany Keo

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

	(b) (5)	Kim Perteet (Please check to see if Sopeany has conducted any work on this to prevent duplicative work)
Hiring – Document Alleged or Proven Bias or Discrimination		Sean Newman Sopeany Keo Kim Perteet
Performance Management - Gain an Understanding of the Process		Brian Murphy

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

	(b) (5)	
Performance Management - Test Compliance with Applicable Laws, Regulations, and Best Practices		Sopeany Keo Kim Perteet
Performance Management - Test Internal Controls		Sopeany Keo Brian Murphy Kim Perteet
Performance Management - Document instances of Alleged or Proven Bias or Discrimination		Sopeany Keo Kim Perteet
Promotions - Gain an Understanding of the Process		Brian Murphy

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

	(b) (5)	
Promotions - Test Compliance with Applicable Laws, Regulations, and Best Practices		Sean Newman
Promotions - Test Internal Controls		Sean Newman
Promotions – Document Alleged or Proven Bias or Discrimination		Sean Newman
Employee Satisfaction Surveys		Sean Newman

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

	(b) (5)	
EEO Complaints - Gain an Understanding of the Process		Brian Murphy

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

EEO Complaints - Test Compliance with Applicable Laws, Regulations, and Best Practices	(b) (5)	Sean Newman
EEO Complaints - Test Internal Controls		Sopeany Keo
EEO Complaints - Identify Alleged or Proven Bias or Discrimination		Kim Perteet Brian Murphy
Non-EEO Complaints - Gain an Understanding of the Process	(b) (5)	Brian Murphy

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

	(b) (5)	
Non-EEO Complaints - Test Compliance with Applicable Laws, Regulations, and Best Practices		Sopeany Keo
Non-EEO Complaints - Test Internal Controls		Sopeany Keo
Non-EEO Complaints – Document Alleged or Proven Bias or Discrimination		Brian Murphy Kim Perteet
Employee Exit Interview		

Fieldwork Program: OMWI

Procedure Title	Error! Unknown document property name.	Comments Where Applicable	Auditor-in-Charge

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

OWMI - Gain an understanding of the Office	(b) (5)		Sean Newman
OMWI - Test Compliance with Laws, Regulations, and Best Practices			Sean Newman

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

	(b) (5)	
OMWI - Test Internal Controls		Sean Newman
Efforts to Increase Diversity - OMWI		Sean Newman

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

	(b) (5)	
Diversity Training - OMWI		Sean Newman
Communications and Awareness - OMWI		Sean Newman
Management's Response to GAO Recommendation(s) - OMWI		Sean Newman

Fieldwork Program: Data Analyses

Procedure Title	Error! Unknown document property name.	Comments Where Applicable	Auditor-in-Charge
Workforce Demographics - Data Collection	(b) (5)		Brian Murphy Victor Calderon
Workforce Demographics - Data Reliability			Brian Murphy Victor Calderon

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

	(b) (5)	
Workforce Demographics - Data Analyses		Brian Murphy Victor Calderon
Hiring - Data Collection		Brian Murphy Victor Calderon
Hiring - Data Reliability		Brian Murphy Victor Calderon
Hiring - Data Analyses		Brian Murphy Victor Calderon

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

	(b) (5)	
Performance Management - Data Collection		Brian Murphy Victor Calderon
Performance Management - Data Reliability		Brian Murphy Victor Calderon
Performance Management - Data Analyses		Brian Murphy Victor Calderon

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

	(b) (5)	
Promotions - Data Collection		Brian Murphy Victor Calderon
Promotions - Data Reliability		Brian Murphy Victor Calderon
Promotions - Data Analyses		Brian Murphy Victor Calderon

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

	(b) (5)	
EEO Complaints - Data Collection		Sopeany Keo Brian Murphy
EEO Complaints - Data Reliability		Sopeany Keo Brian Murphy
EEO Complaints - Data Analyses		Sopeany Keo Brian Murphy
Non-EEO Complaints - Data Collection		\Brian Murphy Victor Calderon
Non-EEO Complaints - Data Reliability		Brian Murphy Victor Calderon
Non-EEO Complaints - Data Analyses		Brian Murphy Victor Calderon

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

	(b) (5)	
EEO and Non-EEO complaints related to PMP		Sopeany Keo Brian Murphy
Separation - Data Collection		Brian Murphy Victor Calderon
Separation - Data Reliability		Brian Murphy Victor Calderon
Separation - Data Analyses		Brian Murphy Victor Calderon

Fieldwork Program: Management's Efforts

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

Procedure Title	Error! Unknown document property name.	Comments Where Applicable	Auditor-in-Charge
Efforts to Respond to EEO Complaints - EEO	(b) (5)		Sopeany Keo Brian Murphy
Efforts to Respond to Other Potential Indications of Bias or Discrimination - EEO			Sopeany Keo Brian Murphy
Efforts to Increase Diversity - EEO			Sopeany Keo Brian Murphy
Efforts to Respond to Non- EEO Complaints – OHC ER			Brian Murphy
Efforts to Respond to PMP Trends – OHC ER			Brian Murphy
Efforts to Respond to Other Potential Indications of Bias or Discrimination – OHC ER			Brian Murphy

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

Efforts to Increase Diversity – OHC (Dave Harmon)	(b) (5)	Sean Newman
Efforts to Respond to Complaints, PMP, Hiring, Promotions, and Diversity - Divisions		Kim Perteet Brian Murphy

FR Restricted
C.3 PRG Report Distribution List Prepared By: Kim Perteet
Reviewed By: Anna Saez

AN: For attachments, please click on the respective links.

From: John Manibusan
To: Kimberly Perteet
Subject: FW: Board-CFPB OIG Report on Board Diversity and Inclusion
Date: Tuesday, April 07, 2015 12:02:18 PM
Attachments: Beatty Transmittal Letter-Board.pdf
board-diversity-inclusion-mar2015.pdf

John Manibusan | Assistant Congressional and Media Liaison
Office of Inspector General
Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-5043 | f: 202-973-5044 | john.p.manibusan@frb.gov
OIG Hotline: 800-827-3340 | oighotline@frb.gov

http://oig.federalreserve.gov | http://oig.consumerfinance.gov

---

From: John Manibusan
Sent: Tuesday, March 31, 2015 5:03 PM
To: 'jennifer.storipan@mail.house.gov'
Subject: Board-CFPB OIG Report on Board Diversity and Inclusion

Hi Jennifer:

Please find attached our final report, "The Board Can Enhance Its Diversity and Inclusion Efforts," dated March 31, 2015. A hard copy will follow. This report responds to a March 24, 2014, letter requesting that we evaluate whether the Board's personnel practices and policies have created an unfair or discriminatory workplace for minorities and women at the Board and to assess the roles and operations of the Board's Office of Minority and Women Inclusion in dealing with personnel matters. This report will be posted on our website on Friday, April 3. We ask that you not release the report outside your office until it is available on our website.

Let me know if you have any questions.

Thanks,

John Manibusan | Assistant Congressional and Media Liaison
Office of Inspector General
Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-5043 | f: 202-973-5044 | john.p.manibusan@frb.gov
OIG Hotline: 800-827-3340 | oighotline@frb.gov

http://oig.federalreserve.gov | http://oig.consumerfinance.gov

FR Restricted
C.3 PRG Report Distribution List
Prepared By: Kim Perteet
Reviewed By: Anna Saez

AN: For attachments, please click on the respective links.

From: John Manibusan
To: Kimberly Perteet
Subject: FW: Board-CFPB OIG Report on Board Diversity and Inclusion
Date: Tuesday, April 07, 2015 12:01:12 PM
Attachments: Cleaver Transmittal Letter-Board.pdf
board-diversity-inclusion-mar2015.pdf

John Manibusan | Assistant Congressional and Media Liaison
Office of Inspector General
Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-5043 | f: 202-973-5044 | john.p.manibusan@frb.gov
OIG Hotline: 800-827-3340 | oighotline@frb.gov

http://oig.federalreserve.gov | http://oig.consumerfinance.gov

From: John Manibusan
Sent: Tuesday, March 31, 2015 5:02 PM
To: 'jennifer.shapiro@mail.house.gov'
Subject: Board-CFPB OIG Report on Board Diversity and Inclusion

Hi Jennifer:

Please find attached our final report, "The Board Can Enhance Its Diversity and Inclusion Efforts," dated March 31, 2015. A hard copy will follow. This report responds to a March 24, 2014, letter requesting that we evaluate whether the Board's personnel practices and policies have created an unfair or discriminatory workplace for minorities and women at the Board and to assess the roles and operations of the Board's Office of Minority and Women Inclusion in dealing with personnel matters. This report will be posted on our website on Friday, April 3. We ask that you not release the report outside your office until it is available on our website.

Let me know if you have any questions.

Thanks,

John Manibusan | Assistant Congressional and Media Liaison
Office of Inspector General
Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-5043 | f: 202-973-5044 | john.p.manibusan@frb.gov
OIG Hotline: 800-827-3340 | oighotline@frb.gov

http://oig.federalreserve.gov | http://oig.consumerfinance.gov

FR Restricted
C.3 PRG Report Distribution List
Prepared By: Kim Perteet
Reviewed By: Anna Saez

AN: For attachments, please click on the respective links.

From: John Manibusan
To: Kimberly Perteet
Subject: FW: Board-CFPB OIG Report on Board Diversity and Inclusion
Date: Tuesday, April 07, 2015 12:01:46 PM
Attachments: Delaney Transmittal Letter-Board.pdf
board-diversity-inclusion-mar2015.pdf

John Manibusan | Assistant Congressional and Media Liaison
Office of Inspector General
Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-5043 | f: 202-973-5044 | john.p.manibusan@frb.gov
OIG Hotline: 800-827-3340 | oighotline@frb.gov

http://oig.federalreserve.gov | http://oig.consumerfinance.gov

From: John Manibusan
Sent: Tuesday, March 31, 2015 5:02 PM
To: 'ben.turner2@mail.house.gov'
Subject: Board-CFPB OIG Report on Board Diversity and Inclusion

Hi Ben:

Please find attached our final report, "The Board Can Enhance Its Diversity and Inclusion Efforts," dated March 31, 2015. A hard copy will follow. This report responds to a March 24, 2014, letter requesting that we evaluate whether the Board's personnel practices and policies have created an unfair or discriminatory workplace for minorities and women at the Board and to assess the roles and operations of the Board's Office of Minority and Women Inclusion in dealing with personnel matters. This report will be posted on our website on Friday, April 3. We ask that you not release the report outside your office until it is available on our website.

Let me know if you have any questions.

Thanks,

John Manibusan | Assistant Congressional and Media Liaison
Office of Inspector General
Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-5043 | f: 202-973-5044 | john.p.manibusan@frb.gov
OIG Hotline: 800-827-3340 | oighotline@frb.gov

http://oig.federalreserve.gov | http://oig.consumerfinance.gov

FR Restricted
C.3 PRG Report Distribution List
Prepared By: Kim Perteet
Reviewed By: Anna Saez
AN: For attachments, please click on the respective links.

From: John Manibusan
To: Kimberly Perteet
Subject: FW: Board-CFPB OIG Report on Board Diversity and Inclusion
Date: Tuesday, April 07, 2015 12:02:34 PM
Attachments: Heck Transmittal Letter-Board.pdf
board-diversity-inclusion-mar2015.pdf

John Manibusan | Assistant Congressional and Media Liaison
Office of Inspector General
Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-5043 | f: 202-973-5044 | john.p.manibusan@frb.gov
OIG Hotline: 800-827-3340 | oighotline@frb.gov

http://oig.federalreserve.gov | http://oig.consumerfinance.gov

---

From: John Manibusan
Sent: Tuesday, March 31, 2015 5:03 PM
To: 'brendan.woodbury@mail.house.gov'
Subject: Board-CFPB OIG Report on Board Diversity and Inclusion

Hi Brendan:

Please find attached our final report, "The Board Can Enhance Its Diversity and Inclusion Efforts," dated March 31, 2015. A hard copy will follow. This report responds to a March 24, 2014, letter requesting that we evaluate whether the Board's personnel practices and policies have created an unfair or discriminatory workplace for minorities and women at the Board and to assess the roles and operations of the Board's Office of Minority and Women Inclusion in dealing with personnel matters. This report will be posted on our website on Friday, April 3. We ask that you not release the report outside your office until it is available on our website.

Let me know if you have any questions.

Thanks,

John Manibusan | Assistant Congressional and Media Liaison
Office of Inspector General
Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-5043 | f: 202-973-5044 | john.p.manibusan@frb.gov
OIG Hotline: 800-827-3340 | oighotline@frb.gov

http://oig.federalreserve.gov | http://oig.consumerfinance.gov

FR Restricted
C.3 PRG Report Distribution List
Prepared By: Kim Perteet
Reviewed By: Anna Saez
AN: For attachments, please click on the respective links.

From: John Manibusan
To: Kimberly Perteet
Subject: FW: Board-CFPB OIG Report on Board Diversity and Inclusion
Date: Tuesday, April 07, 2015 12:02:54 PM
Attachments: Hensarling Transmittal Letter-Board.pdf
board-diversity-inclusion-mar2015.pdf

John Manibusan | Assistant Congressional and Media Liaison
Office of Inspector General
Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-5043 | f: 202-973-5044 | john.p.manibusan@frb.gov
OIG Hotline: 800-827-3340 | oighotline@frb.gov

http://oig.federalreserve.gov | http://oig.consumerfinance.gov

From: John Manibusan
Sent: Tuesday, March 31, 2015 7:14 PM
To: 'Johnson, Brian'
Subject: Board-CFPB OIG Report on Board Diversity and Inclusion

Hi Brian:

Please find attached our final report, "The Board Can Enhance Its Diversity and Inclusion Efforts," dated March 31, 2015. A hard copy will follow. This report responds to a March 24, 2014, letter requesting that we evaluate whether the Board's personnel practices and policies have created an unfair or discriminatory workplace for minorities and women at the Board and to assess the roles and operations of the Board's Office of Minority and Women Inclusion in dealing with personnel matters. This report will be posted on our website on Friday, April 3. We ask that you not release the report outside your office until it is available on our website.

Let me know if you have any questions.

Thanks,

John Manibusan | Assistant Congressional and Media Liaison
Office of Inspector General
Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-5043 | f: 202-973-5044 | john.p.manibusan@frb.gov
OIG Hotline: 800-827-3340 | oighotline@frb.gov

http://oig.federalreserve.gov | http://oig.consumerfinance.gov

FR Restricted
C.3 PRG Report Distribution List
Prepared By: Kim Perteet
Reviewed By: Anna Saez
AN: For attachments, please click on the respective links.

From: John Manibusan
To: Kimberly Perteet
Subject: FW: Board-CFPB OIG Report on Board Diversity and Inclusion
Date: Tuesday, April 07, 2015 12:00:54 PM
Attachments: Maloney Transmittal Letter-Board.pdf
board-diversity-inclusion-mar2015.pdf

John Manibusan | Assistant Congressional and Media Liaison
Office of Inspector General
Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-5043 | f: 202-973-5044 | john.p.manibusan@frb.gov
OIG Hotline: 800-827-3340 | oighotline@frb.gov

http://oig.federalreserve.gov | http://oig.consumerfinance.gov

From: John Manibusan
Sent: Tuesday, March 31, 2015 5:02 PM
To: 'ben.harney@mail.house.gov'
Subject: Board-CFPB OIG Report on Board Diversity and Inclusion

Hi Ben:

Please find attached our final report, "The Board Can Enhance Its Diversity and Inclusion Efforts," dated March 31, 2015. A hard copy will follow. This report responds to a March 24, 2014, letter requesting that we evaluate whether the Board's personnel practices and policies have created an unfair or discriminatory workplace for minorities and women at the Board and to assess the roles and operations of the Board's Office of Minority and Women Inclusion in dealing with personnel matters. This report will be posted on our website on Friday, April 3. We ask that you not release the report outside your office until it is available on our website.

Let me know if you have any questions.

Thanks,

John Manibusan | Assistant Congressional and Media Liaison
Office of Inspector General
Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-5043 | f: 202-973-5044 | john.p.manibusan@frb.gov
OIG Hotline: 800-827-3340 | oighotline@frb.gov

http://oig.federalreserve.gov | http://oig.consumerfinance.gov

FR Restricted
C.3 PRG Report Distribution List
Prepared By: Kim Perteet
Reviewed By: Anna Saez

AN: For attachments, please click on the respective links.

From: John Manibusan
To: Kimberly Perteet
Subject: FW: Board-CFPB OIG Report on Board Diversity and Inclusion
Date: Tuesday, April 07, 2015 12:01:29 PM
Attachments: Perlmutter Transmittal Letter-Board.pdf
board-diversity-inclusion-mar2015.pdf

John Manibusan | Assistant Congressional and Media Liaison
Office of Inspector General
Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-5043 | f: 202-973-5044 | john.p.manibusan@frb.gov
OIG Hotline: 800-827-3340 | oighotline@frb.gov

http://oig.federalreserve.gov | http://oig.consumerfinance.gov

From: John Manibusan
Sent: Tuesday, March 31, 2015 5:02 PM
To: 'noah.marine@mail.house.gov'
Subject: Board-CFPB OIG Report on Board Diversity and Inclusion

Hi Noah:

Please find attached our final report, "The Board Can Enhance Its Diversity and Inclusion Efforts," dated March 31, 2015. A hard copy will follow. This report responds to a March 24, 2014, letter requesting that we evaluate whether the Board's personnel practices and policies have created an unfair or discriminatory workplace for minorities and women at the Board and to assess the roles and operations of the Board's Office of Minority and Women Inclusion in dealing with personnel matters. This report will be posted on our website on Friday, April 3. We ask that you not release the report outside your office until it is available on our website.

Let me know if you have any questions.

Thanks,

John Manibusan | Assistant Congressional and Media Liaison
Office of Inspector General
Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-5043 | f: 202-973-5044 | john.p.manibusan@frb.gov
OIG Hotline: 800-827-3340 | oighotline@frb.gov

http://oig.federalreserve.gov | http://oig.consumerfinance.gov

FR Restricted
C.3 PRG Report Distribution List
Prepared By: Kim Perteet
Reviewed By: Anna Saez

AN: For attachments, please click on the respective links.

From: John Manibusan
To: Kimberly Perteet
Subject: FW: Board-CFPB OIG Report on Board Diversity and Inclusion
Date: Tuesday, April 07, 2015 12:02:02 PM
Attachments: Sinema Transmittal Letter-Board.pdf
board-diversity-inclusion-mar2015.pdf

John Manibusan | Assistant Congressional and Media Liaison
Office of Inspector General
Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-5043 | f: 202-973-5044 | john.p.manibusan@frb.gov
OIG Hotline: 800-827-3340 | oighotline@frb.gov

http://oig.federalreserve.gov | http://oig.consumerfinance.gov

From: John Manibusan
Sent: Tuesday, March 31, 2015 5:03 PM
To: 'alyssa.marois@mail.house.gov'
Subject: Board-CFPB OIG Report on Board Diversity and Inclusion

Hi Alyssa:

Please find attached our final report, "The Board Can Enhance Its Diversity and Inclusion Efforts," dated March 31, 2015. A hard copy will follow. This report responds to a March 24, 2014, letter requesting that we evaluate whether the Board's personnel practices and policies have created an unfair or discriminatory workplace for minorities and women at the Board and to assess the roles and operations of the Board's Office of Minority and Women Inclusion in dealing with personnel matters. This report will be posted on our website on Friday, April 3. We ask that you not release the report outside your office until it is available on our website.

Let me know if you have any questions.

Thanks,

John Manibusan | Assistant Congressional and Media Liaison
Office of Inspector General
Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-5043 | f: 202-973-5044 | john.p.manibusan@frb.gov
OIG Hotline: 800-827-3340 | oighotline@frb.gov

http://oig.federalreserve.gov | http://oig.consumerfinance.gov

FR Restricted
C.3 PRG Report Distribution List
Prepared By: Kim Perteet
Reviewed By: Anna Saez
AN: For attachments, please click on the respective links.

From:	John Manibusan
To:	Kimberly Perteet
Subject:	FW: Board-CFPB OIG Report on Board Diversity and Inclusion
Date:	Tuesday, April 07, 2015 12:00:39 PM
Attachments:	Waters Transmittal Letter-Board.pdf Green Transmittal Letter-Board.pdf board-diversity-inclusion-mar2015.pdf

John Manibusan | Assistant Congressional and Media Liaison
Office of Inspector General
Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-5043 | f: 202-973-5044 | john.p.manibusan@frb.gov
OIG Hotline: 800-827-3340 | oighotline@frb.gov

http://oig.federalreserve.gov | http://oig.consumerfinance.gov

From: John Manibusan
Sent: Tuesday, March 31, 2015 5:01 PM
To: Lynch, Jason; Williams, Ola (Ola.Williams@mail.house.gov); Millison, Deanne; 'gregg.orton@mail.house.gov'
Subject: Board-CFPB OIG Report on Board Diversity and Inclusion

Hi all:

Please find attached our final report, "The Board Can Enhance Its Diversity and Inclusion Efforts," dated March 31, 2015. A hard copy will follow. This report responds to a March 24, 2014, letter requesting that we evaluate whether the Board's personnel practices and policies have created an unfair or discriminatory workplace for minorities and women at the Board and to assess the roles and operations of the Board's Office of Minority and Women Inclusion in dealing with personnel matters. This report will be posted on our website on Friday, April 3. We ask that you not release the report outside your office until it is available on our website.

Let me know if you have any questions.

Thanks,

John Manibusan | Assistant Congressional and Media Liaison
Office of Inspector General
Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-5043 | f: 202-973-5044 | john.p.manibusan@frb.gov
OIG Hotline: 800-827-3340 | oighotline@frb.gov

http://oig.federalreserve.gov | http://oig.consumerfinance.gov

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

Statement of Independence on Individual Projects

The Office of Inspector General (OIG) and its staff and contractors must be independent in all matters relating to audit, inspection, and evaluation work. OIG employees and contractors who are engaged in audits, inspections, or evaluations are to comply with the OIG policy AE-001, *Independence,* and conduct themselves in a manner consistent with the Board of Governors of the Federal Reserve System's (Board) and the OIG's core values; the Board's *Principles of Ethical Conduct*; the *Standards of Ethical Conduct for Employees of the Executive Branch*, issued by the U.S. Office of Government Ethics; the generally accepted government auditing standards (GAGAS), issued by the Comptroller General of the United States; *Quality Standards for Inspection and Evaluation*, issued by the Council of the Inspectors General on Integrity and Efficiency; and any other standards applicable to their project. OIG employees and contractors must take precautions to ensure that their conduct is perceived as being independent, professional, and appropriate and are not to become involved in situations that impair independence or give the appearance that impairment to independence exists.

Independence comprises independence of mind and independence in appearance. Independence of mind is the state of mind that permits the performance of an audit without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism. Independence in appearance is the absence of circumstances that would cause a reasonable and informed third party, having knowledge of the relevant information, to reasonably conclude that the integrity, objectivity, or professional skepticism of an audit organization or member of the audit team had been compromised (GAGAS 3.03).

GAGAS establishes the conceptual framework (see GAGAS 3.07–3.26 and appendix II) that OIG employees and contractors must use to identify and evaluate threats to independence given the circumstances of their work. Whether independence is impaired depends on the nature of the threat, whether the threat is of such significance that it would compromise an auditor's professional judgment or create the appearance that the auditor's professional judgment may be compromised, and the specific safeguards applied to eliminate the threat or reduce it to an acceptable level. GAGAS provides broad categories of threats (GAGAS 3.14) and examples of circumstances that create threats to independence (GAGAS A3.02–A3.09) and it describes safeguards that may be effective in certain circumstances (GAGAS 3.16–3.19).

Consistent with GAGAS 3.21, 3.64, and 3.65, auditors use professional judgment in applying the conceptual framework to determine independence in a given situation. When identifying and evaluating threats to independence, OIG employees and contractors must consider the broad

categories of threats to independence and the example safeguards provided in GAGAS, as well as the unique circumstances of the project. In addition to the GAGAS examples, specific situations that threaten independence and must be reported to the project manager or an appropriate official if the project manager is not available include the following:

- financial interest that is direct, or is significant or material though indirect, in the audited entity or program
- seeking employment with the division or program area to be reviewed or under review (including the time period leading up to the submission of a job application)
- preconceived ideas toward individuals, groups, organizations, or objectives of a particular program that could bias the project
- official, professional, personal, financial, or any kind of relationship that might cause an OIG employee or contractor to limit the extent of his or her inquiry, to limit disclosure, or to weaken or slant findings in any way
- external interference or influence that improperly or imprudently limits or modifies the scope of project work

When these or any other apparent or potential threats to independence are identified, the individual must immediately and fully disclose the situation to the project manager. The project manager, in consultation with the applicable Senior OIG Manager and Associate Inspector General, must determine whether identified threats to independence are significant and whether they can be reduced to an acceptable level with the imposition of safeguards. Any disclosed threats to independence and applied safeguards must be documented on this form (GAGAS 3.24). If the disclosed threats to independence are deemed insignificant, the basis for that determination must be documented on this form.

Failure to comply with the OIG's policies and procedures regarding independence may result in adverse or disciplinary action against the individual, up to and including termination, consistent with applicable Board policy.

Instructions

This form, which documents compliance with applicable independence standards, is to be completed at the start of each project by OIG or contractor project team members, as well as any OIG staff members who substantially contribute to the project in accordance with the OIG's *Independence* policy. Generally, the project's start date refers to the date the project is initiated in the audit system. A new form must be completed when circumstances change or when threats to independence arise that impact the individual's independence. In addition, this form must be completed by OIG referencers prior to their involvement in the project. The completed forms are maintained as electronic workpapers in the audit systems.

Certification

I certify that I have read and understand the above, as well as the OIG's *Independence* policy and GAGAS independence standards. With regard to the assigned project, I have evaluated threats to my independence, both independence of mind and in appearance, and attest that (select one):

☑ I have not identified any threats to my independence.

☐ I have identified threats to independence and applied safeguards, as described below.

Describe any threats to independence identified and safeguards applied (attach additional page if necessary).

☐ As a **referencer** for this project, I certify that I have not identified any threats to my independence that would prevent me from objectively performing the independent reference review.

I also agree to reevaluate my independence whenever my assignment is changed or whenever my circumstances change while working on this project. If changes affecting either my independence or my objectivity regarding this project occur subsequent to the completion of this form, I will immediately notify the project manager or an appropriate official if the project manager is not available.

Project name: 2014 Congressional Request on the Board's Personnel Practices

Individual's name: (b) (6)

Date individual started on project: 8-4-2014

Signature: (b) (6) **Date:** 8-5-2014

OFFICE OF INSPECTOR GENERAL
BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU
WASHINGTON, DC 20551

NON-DISCLOSURE AGREEMENT

I, (b) (6) understand that, in the course of performing work for the Office of Inspector General (OIG) of the Board of Governors of the Federal Reserve System (Board) and the Consumer Financial Protection Bureau (CFPB), I may come into possession of or obtain knowledge of information of the OIG, the Board, the Federal Open Market Committee (FOMC), the Federal Reserve Banks, or the CFPB that is not public or that has not and is not required by law to be made public, including, for example, information that is designated as restricted, controlled, proprietary, confidential, confidential supervisory, or personnel (collectively, "*Confidential Information*"). Confidential Information shall include, but is not limited to (1) information pertaining to the security arrangements and strategies of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB (including information describing security controls related to information technology infrastructure such as network architecture and specific systems, applications, and databases); (2) economic data; (3) financial, statistical, and personnel data pertaining to the OIG, Board, FOMC, Federal Reserve Banks, CFPB, or other financial institutions; (4) financial, statistical, personnel planning and similar information relating to past, present, or future activities of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB; (5) pre-decisional deliberative information and data; (6) law enforcement privileged information; (7) attorney-client privileged information; (8) personally identifiable information; (9) trade-secret information; and (10) non-public information included in the files of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB.

Confidential Information does not include information that (1) is public; (2) is or becomes publicly available without breach by me of this Non-Disclosure Agreement ("*NDA*"); (3) was rightfully received by me without obligation of confidentiality; or (4) was developed by me independently of any disclosures to me made by the OIG, Board, FOMC, Federal Reserve Banks, or CFPB. Except for information I receive that is not Confidential Information, I will treat all information I receive from the OIG, Board, FOMC, Federal Reserve Banks, or CFPB as Confidential Information, regardless of the manner or form in which the information is transmitted or accessible. In addition, I will also treat the advice, deliverables, products, outputs, or similar items I provide or produce while working with the OIG ("*Product Information*") as Confidential Information until such time as the OIG informs me in writing that such Product Information is public.

Thus, I agree to the following terms:

1. I will keep in confidence all Confidential Information that may be acquired in connection with or as a result of my responsibilities. I will not, at any time, either during or after my work with the OIG, make public or otherwise communicate or disclose Confidential Information to anyone other than authorized personnel of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB, without the OIG's prior written consent. (The OIG will coordinate and obtain the necessary approval(s) from the Board, the FOMC, the Federal Reserve Banks, or the CFPB, as applicable.)

2. I will use Confidential Information solely in connection with my responsibilities in working for the OIG. I will not directly or indirectly use Confidential Information for my private gain or for the private gain of another person or entity at any time, either during or after termination of my work with the OIG.

3. I will inform the OIG of any external requests or demands for disclosure of Confidential Information, and I will refer all such demands and requests for disclosures, including but not limited to subpoenas, to the OIG.

4. Should a question arise as to whether particular information is Confidential Information, I will immediately contact the OIG and seek a determination as to the information's status. Until a determination has been made by the OIG (after coordination with the Board, FOMC, Federal Reserve Banks, or CFPB, as applicable), I shall treat it as Confidential Information in accordance with this NDA.

5. At all times, including during and after my work with the OIG, I will take all necessary steps to protect Confidential Information subject to this NDA.

6. Upon completion, expiration, or termination of my services, unless I am instructed otherwise by the OIG, I will promptly dispose of all Confidential Information in my possession in whatever manner is approved by the OIG for the disposal of such information, which may include the return of Confidential Information to the OIG.

7. I understand that I am prohibited from releasing any publicity or advertising regarding the work I perform for the OIG and from using the name or insignia of the OIG, Board, FOMC, CFPB, Federal Reserve Banks, or the Federal Reserve System, or any variation or adaptation thereof, for any commercial, advertisement, promotional, or endorsement purposes, unless the OIG and the Board's Chief Operating Officer (or his/her designee) has given prior written consent for such release or use.

8. I agree and acknowledge that the disclosure or use of any Confidential Information in breach of this NDA would cause irreparable harm to the OIG, Board, FOMC, CFPB, or Federal Reserve Banks. Accordingly, in the event of such use or disclosure, I understand that I may be subject to legal or other action, which may include termination of my work with the OIG and referral for criminal prosecution, if appropriate.

9. If I suspect that any Confidential Information to which I am given access is or may have been lost or disclosed without authorization, I will immediately notify the OIG.

I understanding that this NDA, all of its terms and conditions, shall remain in effect following the expiration or termination of my work with the OIG until this NDA is terminated in writing by the OIG.

(b) (6) _____ 8-5-2014

SIGNATURE DATE

(b) (6) _____

Printed Name

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

Statement of Independence on Individual Projects

The Office of Inspector General (OIG) and its staff and contractors must be independent in all matters relating to audit, inspection, and evaluation work. OIG employees and contractors who are engaged in audits, inspections, or evaluations are to comply with the OIG policy AE-001, *Independence*, and conduct themselves in a manner consistent with the Board of Governors of the Federal Reserve System's (Board) and the OIG's core values; the Board's *Principles of Ethical Conduct*; the *Standards of Ethical Conduct for Employees of the Executive Branch*, issued by the U.S. Office of Government Ethics; the generally accepted government auditing standards (GAGAS), issued by the Comptroller General of the United States; *Quality Standards for Inspection and Evaluation*, issued by the Council of the Inspectors General on Integrity and Efficiency; and any other standards applicable to their project. OIG employees and contractors must take precautions to ensure that their conduct is perceived as being independent, professional, and appropriate and are not to become involved in situations that impair independence or give the appearance that impairment to independence exists.

Independence comprises independence of mind and independence in appearance. Independence of mind is the state of mind that permits the performance of an audit without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism. Independence in appearance is the absence of circumstances that would cause a reasonable and informed third party, having knowledge of the relevant information, to reasonably conclude that the integrity, objectivity, or professional skepticism of an audit organization or member of the audit team had been compromised (GAGAS 3.03).

GAGAS establishes the conceptual framework (see GAGAS 3.07–3.26 and appendix II) that OIG employees and contractors must use to identify and evaluate threats to independence given the circumstances of their work. Whether independence is impaired depends on the nature of the threat, whether the threat is of such significance that it would compromise an auditor's professional judgment or create the appearance that the auditor's professional judgment may be compromised, and the specific safeguards applied to eliminate the threat or reduce it to an acceptable level. GAGAS provides broad categories of threats (GAGAS 3.14) and examples of circumstances that create threats to independence (GAGAS A3.02–A3.09) and it describes safeguards that may be effective in certain circumstances (GAGAS 3.16–3.19).

Consistent with GAGAS 3.21, 3.64, and 3.65, auditors use professional judgment in applying the conceptual framework to determine independence in a given situation. When identifying and evaluating threats to independence, OIG employees and contractors must consider the broad

categories of threats to independence and the example safeguards provided in GAGAS, as well as the unique circumstances of the project. In addition to the GAGAS examples, specific situations that threaten independence and must be reported to the project manager or an appropriate official if the project manager is not available include the following:

- financial interest that is direct, or is significant or material though indirect, in the audited entity or program
- seeking employment with the division or program area to be reviewed or under review (including the time period leading up to the submission of a job application)
- preconceived ideas toward individuals, groups, organizations, or objectives of a particular program that could bias the project
- official, professional, personal, financial, or any kind of relationship that might cause an OIG employee or contractor to limit the extent of his or her inquiry, to limit disclosure, or to weaken or slant findings in any way
- external interference or influence that improperly or imprudently limits or modifies the scope of project work

When these or any other apparent or potential threats to independence are identified, the individual must immediately and fully disclose the situation to the project manager. The project manager, in consultation with the applicable Senior OIG Manager and Associate Inspector General, must determine whether identified threats to independence are significant and whether they can be reduced to an acceptable level with the imposition of safeguards. Any disclosed threats to independence and applied safeguards must be documented on this form (GAGAS 3.24). If the disclosed threats to independence are deemed insignificant, the basis for that determination must be documented on this form.

Failure to comply with the OIG's policies and procedures regarding independence may result in adverse or disciplinary action against the individual, up to and including termination, consistent with applicable Board policy.

Instructions

This form, which documents compliance with applicable independence standards, is to be completed at the start of each project by OIG or contractor project team members, as well as any OIG staff members who substantially contribute to the project in accordance with the OIG's *Independence* policy. Generally, the project's start date refers to the date the project is initiated in the audit system. A new form must be completed when circumstances change or when threats to independence arise that impact the individual's independence. In addition, this form must be completed by OIG referencers prior to their involvement in the project. The completed forms are maintained as electronic workpapers in the audit systems.

Certification

I certify that I have read and understand the above, as well as the OIG's *Independence* policy and GAGAS independence standards. With regard to the assigned project, I have evaluated threats to my independence, both independence of mind and in appearance, and attest that (select one):

☒ I have not identified any threats to my independence.

☐ I have identified threats to independence and applied safeguards, as described below.

Describe any threats to independence identified and safeguards applied (attach additional page if necessary).

☐ As a **referencer** for this project, I certify that I have not identified any threats to my independence that would prevent me from objectively performing the independent reference review.

I also agree to reevaluate my independence whenever my assignment is changed or whenever my circumstances change while working on this project. If changes affecting either my independence or my objectivity regarding this project occur subsequent to the completion of this form, I will immediately notify the project manager or an appropriate official if the project manager is not available.

Project name: 2014 Congressional Request on the Board's Personnel Practices

Individual's name: (b) (6) [redacted]

Date individual started on project: 8/4/14

Signature: (b) (6) [redacted] **Date:** 8/6/2014

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

WASHINGTON, DC 20551

NON-DISCLOSURE AGREEMENT

I, (b) (6) , understand that, in the course of performing work for the Office of Inspector General (OIG) of the Board of Governors of the Federal Reserve System (Board) and the Consumer Financial Protection Bureau (CFPB), I may come into possession of or obtain knowledge of information of the OIG, the Board, the Federal Open Market Committee (FOMC), the Federal Reserve Banks, or the CFPB that is not public or that has not and is not required by law to be made public, including, for example, information that is designated as restricted, controlled, proprietary, confidential, confidential supervisory, or personnel (collectively, "*Confidential Information*"). Confidential Information shall include, but is not limited to (1) information pertaining to the security arrangements and strategies of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB (including information describing security controls related to information technology infrastructure such as network architecture and specific systems, applications, and databases); (2) economic data; (3) financial, statistical, and personnel data pertaining to the OIG, Board, FOMC, Federal Reserve Banks, CFPB, or other financial institutions; (4) financial, statistical, personnel planning and similar information relating to past, present, or future activities of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB; (5) pre-decisional deliberative information and data; (6) law enforcement privileged information; (7) attorney-client privileged information; (8) personally identifiable information; (9) trade-secret information; and (10) non-public information included in the files of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB.

Confidential Information does not include information that (1) is public; (2) is or becomes publicly available without breach by me of this Non-Disclosure Agreement ("*NDA*"); (3) was rightfully received by me without obligation of confidentiality; or (4) was developed by me independently of any disclosures to me made by the OIG, Board, FOMC, Federal Reserve Banks, or CFPB. Except for information I receive that is not Confidential Information, I will treat all information I receive from the OIG, Board, FOMC, Federal Reserve Banks, or CFPB as Confidential Information, regardless of the manner or form in which the information is transmitted or accessible. In addition, I will also treat the advice, deliverables, products, outputs, or similar items I provide or produce while working with the OIG ("*Product Information*") as Confidential Information until such time as the OIG informs me in writing that such Product Information is public.

Thus, I agree to the following terms:

1. I will keep in confidence all Confidential Information that may be acquired in connection with or as a result of my responsibilities. I will not, at any time, either during or after my work with the OIG, make public or otherwise communicate or disclose Confidential Information to anyone other than authorized personnel of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB, without the OIG's prior written consent. (The OIG will coordinate and obtain the necessary approval(s) from the Board, the FOMC, the Federal Reserve Banks, or the CFPB, as applicable.)

2. I will use Confidential Information solely in connection with my responsibilities in working for the OIG. I will not directly or indirectly use Confidential Information for my private gain or for the private gain of another person or entity at any time, either during or after termination of my work with the OIG.

3. I will inform the OIG of any external requests or demands for disclosure of Confidential Information, and I will refer all such demands and requests for disclosures, including but not limited to subpoenas, to the OIG.

4. Should a question arise as to whether particular information is Confidential Information, I will immediately contact the OIG and seek a determination as to the information's status. Until a determination has been made by the OIG (after coordination with the Board, FOMC, Federal Reserve Banks, or CFPB, as applicable), I shall treat it as Confidential Information in accordance with this NDA.

5. At all times, including during and after my work with the OIG, I will take all necessary steps to protect Confidential Information subject to this NDA.

6. Upon completion, expiration, or termination of my services, unless I am instructed otherwise by the OIG, I will promptly dispose of all Confidential Information in my possession in whatever manner is approved by the OIG for the disposal of such information, which may include the return of Confidential Information to the OIG.

7. I understand that I am prohibited from releasing any publicity or advertising regarding the work I perform for the OIG and from using the name or insignia of the OIG, Board, FOMC, CFPB, Federal Reserve Banks, or the Federal Reserve System, or any variation or adaptation thereof, for any commercial, advertisement, promotional, or endorsement purposes, unless the OIG and the Board's Chief Operating Officer (or his/her designee) has given prior written consent for such release or use.

8. I agree and acknowledge that the disclosure or use of any Confidential Information in breach of this NDA would cause irreparable harm to the OIG, Board, FOMC, CFPB, or Federal Reserve Banks. Accordingly, in the event of such use or disclosure, I understand that I may be subject to legal or other action, which may include termination of my work with the OIG and referral for criminal prosecution, if appropriate.

9. If I suspect that any Confidential Information to which I am given access is or may have been lost or disclosed without authorization, I will immediately notify the OIG.

I understanding that this NDA, all of its terms and conditions, shall remain in effect following the expiration or termination of my work with the OIG until this NDA is terminated in writing by the OIG.

(b) (6)

8/6/2014
DATE

(b) (6)

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

Statement of Independence on Individual Projects

The Office of Inspector General (OIG) and its staff and contractors must be independent in all matters relating to audit, inspection, and evaluation work. OIG employees and contractors who are engaged in audits, inspections, or evaluations are to comply with the OIG policy AE-001, *Independence,* and conduct themselves in a manner consistent with the Board of Governors of the Federal Reserve System's (Board) and the OIG's core values; the Board's *Principles of Ethical Conduct*; the *Standards of Ethical Conduct for Employees of the Executive Branch*, issued by the U.S. Office of Government Ethics; the generally accepted government auditing standards (GAGAS), issued by the Comptroller General of the United States; *Quality Standards for Inspection and Evaluation*, issued by the Council of the Inspectors General on Integrity and Efficiency; and any other standards applicable to their project. OIG employees and contractors must take precautions to ensure that their conduct is perceived as being independent, professional, and appropriate and are not to become involved in situations that impair independence or give the appearance that impairment to independence exists.

Independence comprises independence of mind and independence in appearance. Independence of mind is the state of mind that permits the performance of an audit without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism. Independence in appearance is the absence of circumstances that would cause a reasonable and informed third party, having knowledge of the relevant information, to reasonably conclude that the integrity, objectivity, or professional skepticism of an audit organization or member of the audit team had been compromised (GAGAS 3.03).

GAGAS establishes the conceptual framework (see GAGAS 3.07–3.26 and appendix II) that OIG employees and contractors must use to identify and evaluate threats to independence given the circumstances of their work. Whether independence is impaired depends on the nature of the threat, whether the threat is of such significance that it would compromise an auditor's professional judgment or create the appearance that the auditor's professional judgment may be compromised, and the specific safeguards applied to eliminate the threat or reduce it to an acceptable level. GAGAS provides broad categories of threats (GAGAS 3.14) and examples of circumstances that create threats to independence (GAGAS A3.02–A3.09) and it describes safeguards that may be effective in certain circumstances (GAGAS 3.16–3.19).

Consistent with GAGAS 3.21, 3.64, and 3.65, auditors use professional judgment in applying the conceptual framework to determine independence in a given situation. When identifying and evaluating threats to independence, OIG employees and contractors must consider the broad

categories of threats to independence and the example safeguards provided in GAGAS, as well as the unique circumstances of the project. In addition to the GAGAS examples, specific situations that threaten independence and must be reported to the project manager or an appropriate official if the project manager is not available include the following:

- financial interest that is direct, or is significant or material though indirect, in the audited entity or program
- seeking employment with the division or program area to be reviewed or under review (including the time period leading up to the submission of a job application)
- preconceived ideas toward individuals, groups, organizations, or objectives of a particular program that could bias the project
- official, professional, personal, financial, or any kind of relationship that might cause an OIG employee or contractor to limit the extent of his or her inquiry, to limit disclosure, or to weaken or slant findings in any way
- external interference or influence that improperly or imprudently limits or modifies the scope of project work

When these or any other apparent or potential threats to independence are identified, the individual must immediately and fully disclose the situation to the project manager. The project manager, in consultation with the applicable Senior OIG Manager and Associate Inspector General, must determine whether identified threats to independence are significant and whether they can be reduced to an acceptable level with the imposition of safeguards. Any disclosed threats to independence and applied safeguards must be documented on this form (GAGAS 3.24). If the disclosed threats to independence are deemed insignificant, the basis for that determination must be documented on this form.

Failure to comply with the OIG's policies and procedures regarding independence may result in adverse or disciplinary action against the individual, up to and including termination, consistent with applicable Board policy.

Instructions

This form, which documents compliance with applicable independence standards, is to be completed at the start of each project by OIG or contractor project team members, as well as any OIG staff members who substantially contribute to the project in accordance with the OIG's *Independence* policy. Generally, the project's start date refers to the date the project is initiated in the audit system. A new form must be completed when circumstances change or when threats to independence arise that impact the individual's independence. In addition, this form must be completed by OIG referencers prior to their involvement in the project. The completed forms are maintained as electronic workpapers in the audit systems.

Certification

I certify that I have read and understand the above, as well as the OIG's *Independence* policy and GAGAS independence standards. With regard to the assigned project, I have evaluated threats to my independence, both independence of mind and in appearance, and attest that (select one):

☑ I have not identified any threats to my independence.

☐ I have identified threats to independence and applied safeguards, as described below.

Describe any threats to independence identified and safeguards applied (attach additional page if necessary).

☐ As a **referencer** for this project, I certify that I have not identified any threats to my independence that would prevent me from objectively performing the independent reference review.

I also agree to reevaluate my independence whenever my assignment is changed or whenever my circumstances change while working on this project. If changes affecting either my independence or my objectivity regarding this project occur subsequent to the completion of this form, I will immediately notify the project manager or an appropriate official if the project manager is not available.

Project name: 2014 Congressional Request on the Board's Personnel Practices

Individual's name: (b) (6)

Date individual started on project: 8/4/2014

Signature: (b) (6) **Date:** 8/7/14

OFFICE OF INSPECTOR GENERAL
BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU
WASHINGTON, DC 20551

NON-DISCLOSURE AGREEMENT

I, (b) (6) , understand that, in the course of performing work for the Office of Inspector General (OIG) of the Board of Governors of the Federal Reserve System (Board) and the Consumer Financial Protection Bureau (CFPB), I may come into possession of or obtain knowledge of information of the OIG, the Board, the Federal Open Market Committee (FOMC), the Federal Reserve Banks, or the CFPB that is not public or that has not and is not required by law to be made public, including, for example, information that is designated as restricted, controlled, proprietary, confidential, confidential supervisory, or personnel (collectively, "*Confidential Information*"). Confidential Information shall include, but is not limited to (1) information pertaining to the security arrangements and strategies of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB (including information describing security controls related to information technology infrastructure such as network architecture and specific systems, applications, and databases); (2) economic data; (3) financial, statistical, and personnel data pertaining to the OIG, Board, FOMC, Federal Reserve Banks, CFPB, or other financial institutions; (4) financial, statistical, personnel planning and similar information relating to past, present, or future activities of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB; (5) pre-decisional deliberative information and data; (6) law enforcement privileged information; (7) attorney-client privileged information; (8) personally identifiable information; (9) trade-secret information; and (10) non-public information included in the files of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB.

Confidential Information does not include information that (1) is public; (2) is or becomes publicly available without breach by me of this Non-Disclosure Agreement ("*NDA*"); (3) was rightfully received by me without obligation of confidentiality; or (4) was developed by me independently of any disclosures to me made by the OIG, Board, FOMC, Federal Reserve Banks, or CFPB. Except for information I receive that is not Confidential Information, I will treat all information I receive from the OIG, Board, FOMC, Federal Reserve Banks, or CFPB as Confidential Information, regardless of the manner or form in which the information is transmitted or accessible. In addition, I will also treat the advice, deliverables, products, outputs, or similar items I provide or produce while working with the OIG ("*Product Information*") as Confidential Information until such time as the OIG informs me in writing that such Product Information is public.

Thus, I agree to the following terms:

1. I will keep in confidence all Confidential Information that may be acquired in connection with or as a result of my responsibilities. I will not, at any time, either during or after my work with the OIG, make public or otherwise communicate or disclose Confidential Information to anyone other than authorized personnel of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB, without the OIG's prior written consent. (The OIG will coordinate and obtain the necessary approval(s) from the Board, the FOMC, the Federal Reserve Banks, or the CFPB, as applicable.)

2. I will use Confidential Information solely in connection with my responsibilities in working for the OIG. I will not directly or indirectly use Confidential Information for my private gain or for the private gain of another person or entity at any time, either during or after termination of my work with the OIG.

3. I will inform the OIG of any external requests or demands for disclosure of Confidential Information, and I will refer all such demands and requests for disclosures, including but not limited to subpoenas, to the OIG.

4. Should a question arise as to whether particular information is Confidential Information, I will immediately contact the OIG and seek a determination as to the information's status. Until a determination has been made by the OIG (after coordination with the Board, FOMC, Federal Reserve Banks, or CFPB, as applicable), I shall treat it as Confidential Information in accordance with this NDA.

5. At all times, including during and after my work with the OIG, I will take all necessary steps to protect Confidential Information subject to this NDA.

6. Upon completion, expiration, or termination of my services, unless I am instructed otherwise by the OIG, I will promptly dispose of all Confidential Information in my possession in whatever manner is approved by the OIG for the disposal of such information, which may include the return of Confidential Information to the OIG.

7. I understand that I am prohibited from releasing any publicity or advertising regarding the work I perform for the OIG and from using the name or insignia of the OIG, Board, FOMC, CFPB, Federal Reserve Banks, or the Federal Reserve System, or any variation or adaptation thereof, for any commercial, advertisement, promotional, or endorsement purposes, unless the OIG and the Board's Chief Operating Officer (or his/her designee) has given prior written consent for such release or use.

8. I agree and acknowledge that the disclosure or use of any Confidential Information in breach of this NDA would cause irreparable harm to the OIG, Board, FOMC, CFPB, or Federal Reserve Banks. Accordingly, in the event of such use or disclosure, I understand that I may be subject to legal or other action, which may include termination of my work with the OIG and referral for criminal prosecution, if appropriate.

9. If I suspect that any Confidential Information to which I am given access is or may have been lost or disclosed without authorization, I will immediately notify the OIG.

I understanding that this NDA, all of its terms and conditions, shall remain in effect following the expiration or termination of my work with the OIG until this NDA is terminated in writing by the OIG.

(b) (6)

SIGNATURE

8/7/14

DATE

(b) (6)

PRINTED NAME

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

Statement of Independence on Individual Projects

The Office of Inspector General (OIG) and its staff and contractors must be independent in all matters relating to audit, inspection, and evaluation work. OIG employees and contractors who are engaged in audits, inspections, or evaluations are to comply with the OIG policy AE-001, *Independence,* and conduct themselves in a manner consistent with the Board of Governors of the Federal Reserve System's (Board) and the OIG's core values; the Board's *Principles of Ethical Conduct*; the *Standards of Ethical Conduct for Employees of the Executive Branch*, issued by the U.S. Office of Government Ethics; the generally accepted government auditing standards (GAGAS), issued by the Comptroller General of the United States; *Quality Standards for Inspection and Evaluation*, issued by the Council of the Inspectors General on Integrity and Efficiency; and any other standards applicable to their project. OIG employees and contractors must take precautions to ensure that their conduct is perceived as being independent, professional, and appropriate and are not to become involved in situations that impair independence or give the appearance that impairment to independence exists.

Independence comprises independence of mind and independence in appearance. Independence of mind is the state of mind that permits the performance of an audit without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism. Independence in appearance is the absence of circumstances that would cause a reasonable and informed third party, having knowledge of the relevant information, to reasonably conclude that the integrity, objectivity, or professional skepticism of an audit organization or member of the audit team had been compromised (GAGAS 3.03).

GAGAS establishes the conceptual framework (see GAGAS 3.07–3.26 and appendix II) that OIG employees and contractors must use to identify and evaluate threats to independence given the circumstances of their work. Whether independence is impaired depends on the nature of the threat, whether the threat is of such significance that it would compromise an auditor's professional judgment or create the appearance that the auditor's professional judgment may be compromised, and the specific safeguards applied to eliminate the threat or reduce it to an acceptable level. GAGAS provides broad categories of threats (GAGAS 3.14) and examples of circumstances that create threats to independence (GAGAS A3.02–A3.09) and it describes safeguards that may be effective in certain circumstances (GAGAS 3.16–3.19).

Consistent with GAGAS 3.21, 3.64, and 3.65, auditors use professional judgment in applying the conceptual framework to determine independence in a given situation. When identifying and evaluating threats to independence, OIG employees and contractors must consider the broad

categories of threats to independence and the example safeguards provided in GAGAS, as well as the unique circumstances of the project. In addition to the GAGAS examples, specific situations that threaten independence and must be reported to the project manager or an appropriate official if the project manager is not available include the following:

- financial interest that is direct, or is significant or material though indirect, in the audited entity or program
- seeking employment with the division or program area to be reviewed or under review (including the time period leading up to the submission of a job application)
- preconceived ideas toward individuals, groups, organizations, or objectives of a particular program that could bias the project
- official, professional, personal, financial, or any kind of relationship that might cause an OIG employee or contractor to limit the extent of his or her inquiry, to limit disclosure, or to weaken or slant findings in any way
- external interference or influence that improperly or imprudently limits or modifies the scope of project work

When these or any other apparent or potential threats to independence are identified, the individual must immediately and fully disclose the situation to the project manager. The project manager, in consultation with the applicable Senior OIG Manager and Associate Inspector General, must determine whether identified threats to independence are significant and whether they can be reduced to an acceptable level with the imposition of safeguards. Any disclosed threats to independence and applied safeguards must be documented on this form (GAGAS 3.24). If the disclosed threats to independence are deemed insignificant, the basis for that determination must be documented on this form.

Failure to comply with the OIG's policies and procedures regarding independence may result in adverse or disciplinary action against the individual, up to and including termination, consistent with applicable Board policy.

Instructions

This form, which documents compliance with applicable independence standards, is to be completed at the start of each project by OIG or contractor project team members, as well as any OIG staff members who substantially contribute to the project in accordance with the OIG's *Independence* policy. Generally, the project's start date refers to the date the project is initiated in the audit system. A new form must be completed when circumstances change or when threats to independence arise that impact the individual's independence. In addition, this form must be completed by OIG referencers prior to their involvement in the project. The completed forms are maintained as electronic workpapers in the audit systems.

Certification

I certify that I have read and understand the above, as well as the OIG's *Independence* policy and GAGAS independence standards. With regard to the assigned project, I have evaluated threats to my independence, both independence of mind and in appearance, and attest that (select one):

I have not identified any threats to my independence.

I have identified threats to independence and applied safeguards, as described below.

Describe any threats to independence identified and safeguards applied (attach additional page if necessary).

☑ As a **referencer** for this project, I certify that I have not identified any threats to my independence that would prevent me from objectively performing the independent reference review.

I also agree to reevaluate my independence whenever my assignment is changed or whenever my circumstances change while working on this project. If changes affecting either my independence or my objectivity regarding this project occur subsequent to the completion of this form, I will immediately notify the project manager or an appropriate official if the project manager is not available.

Project name: 2014 Congressional Request on the Board's Personnel Practices

Individual's name: (b) (6) [redacted]

Date individual started on project: 8-4-2014

Signature: (b) (6) [redacted] **Date:** 9/16/14

OFFICE OF INSPECTOR GENERAL
BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU
WASHINGTON, DC 20551

NON-DISCLOSURE AGREEMENT

I, (b) (6) , understand that, in the course of performing work for the Office of Inspector General (OIG) of the Board of Governors of the Federal Reserve System (Board) and the Consumer Financial Protection Bureau (CFPB), I may come into possession of or obtain knowledge of information of the OIG, the Board, the Federal Open Market Committee (FOMC), the Federal Reserve Banks, or the CFPB that is not public or that has not and is not required by law to be made public, including, for example, information that is designated as restricted, controlled, proprietary, confidential, confidential supervisory, or personnel (collectively, "*Confidential Information*"). Confidential Information shall include, but is not limited to (1) information pertaining to the security arrangements and strategies of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB (including information describing security controls related to information technology infrastructure such as network architecture and specific systems, applications, and databases); (2) economic data; (3) financial, statistical, and personnel data pertaining to the OIG, Board, FOMC, Federal Reserve Banks, CFPB, or other financial institutions; (4) financial, statistical, personnel planning and similar information relating to past, present, or future activities of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB; (5) pre-decisional deliberative information and data; (6) law enforcement privileged information; (7) attorney-client privileged information; (8) personally identifiable information; (9) trade-secret information; and (10) non-public information included in the files of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB.

Confidential Information does not include information that (1) is public; (2) is or becomes publicly available without breach by me of this Non-Disclosure Agreement ("*NDA*"); (3) was rightfully received by me without obligation of confidentiality; or (4) was developed by me independently of any disclosures to me made by the OIG, Board, FOMC, Federal Reserve Banks, or CFPB. Except for information I receive that is not Confidential Information, I will treat all information I receive from the OIG, Board, FOMC, Federal Reserve Banks, or CFPB as Confidential Information, regardless of the manner or form in which the information is transmitted or accessible. In addition, I will also treat the advice, deliverables, products, outputs, or similar items I provide or produce while working with the OIG ("*Product Information*") as Confidential Information until such time as the OIG informs me in writing that such Product Information is public.

Thus, I agree to the following terms:

1. I will keep in confidence all Confidential Information that may be acquired in connection with or as a result of my responsibilities. I will not, at any time, either during or after my work with the OIG, make public or otherwise communicate or disclose Confidential Information to anyone other than authorized personnel of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB, without the OIG's prior written consent. (The OIG will coordinate and obtain the necessary approval(s) from the Board, the FOMC, the Federal Reserve Banks, or the CFPB, as applicable.)

2. I will use Confidential Information solely in connection with my responsibilities in working for the OIG. I will not directly or indirectly use Confidential Information for my private gain or for the private gain of another person or entity at any time, either during or after termination of my work with the OIG.

3. I will inform the OIG of any external requests or demands for disclosure of Confidential Information, and I will refer all such demands and requests for disclosures, including but not limited to subpoenas, to the OIG.

4. Should a question arise as to whether particular information is Confidential Information, I will immediately contact the OIG and seek a determination as to the information's status. Until a determination has been made by the OIG (after coordination with the Board, FOMC, Federal Reserve Banks, or CFPB, as applicable), I shall treat it as Confidential Information in accordance with this NDA.

5. At all times, including during and after my work with the OIG, I will take all necessary steps to protect Confidential Information subject to this NDA.

6. Upon completion, expiration, or termination of my services, unless I am instructed otherwise by the OIG, I will promptly dispose of all Confidential Information in my possession in whatever manner is approved by the OIG for the disposal of such information, which may include the return of Confidential Information to the OIG.

7. I understand that I am prohibited from releasing any publicity or advertising regarding the work I perform for the OIG and from using the name or insignia of the OIG, Board, FOMC, CFPB, Federal Reserve Banks, or the Federal Reserve System, or any variation or adaptation thereof, for any commercial, advertisement, promotional, or endorsement purposes, unless the OIG and the Board's Chief Operating Officer (or his/her designee) has given prior written consent for such release or use.

8. I agree and acknowledge that the disclosure or use of any Confidential Information in breach of this NDA would cause irreparable harm to the OIG, Board, FOMC, CFPB, or Federal Reserve Banks. Accordingly, in the event of such use or disclosure, I understand that I may be subject to legal or other action, which may include termination of my work with the OIG and referral for criminal prosecution, if appropriate.

9. If I suspect that any Confidential Information to which I am given access is or may have been lost or disclosed without authorization, I will immediately notify the OIG.

I understanding that this NDA, all of its terms and conditions, shall remain in effect following the expiration or termination of my work with the OIG until this NDA is terminated in writing by the OIG.

(b) (6) _____ 03/10/14

SIGNATURE DATE

(b) (6) _____

Printed Name

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

Statement of Independence on Individual Projects

The Office of Inspector General (OIG) and its staff and contractors must be independent in all matters relating to audit, inspection, and evaluation work. OIG employees and contractors who are engaged in audits, inspections, or evaluations are to comply with the OIG policy AE-001, *Independence,* and conduct themselves in a manner consistent with the Board of Governors of the Federal Reserve System's (Board) and the OIG's core values; the Board's *Principles of Ethical Conduct*; the *Standards of Ethical Conduct for Employees of the Executive Branch,* issued by the U.S. Office of Government Ethics; the generally accepted government auditing standards (GAGAS), issued by the Comptroller General of the United States; *Quality Standards for Inspection and Evaluation,* issued by the Council of the Inspectors General on Integrity and Efficiency; and any other standards applicable to their project. OIG employees and contractors must take precautions to ensure that their conduct is perceived as being independent, professional, and appropriate and are not to become involved in situations that impair independence or give the appearance that impairment to independence exists.

Independence comprises independence of mind and independence in appearance. Independence of mind is the state of mind that permits the performance of an audit without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism. Independence in appearance is the absence of circumstances that would cause a reasonable and informed third party, having knowledge of the relevant information, to reasonably conclude that the integrity, objectivity, or professional skepticism of an audit organization or member of the audit team had been compromised (GAGAS 3.03).

GAGAS establishes the conceptual framework (see GAGAS 3.07–3.26 and appendix II) that OIG employees and contractors must use to identify and evaluate threats to independence given the circumstances of their work. Whether independence is impaired depends on the nature of the threat, whether the threat is of such significance that it would compromise an auditor's professional judgment or create the appearance that the auditor's professional judgment may be compromised, and the specific safeguards applied to eliminate the threat or reduce it to an acceptable level. GAGAS provides broad categories of threats (GAGAS 3.14) and examples of circumstances that create threats to independence (GAGAS A3.02–A3.09) and it describes safeguards that may be effective in certain circumstances (GAGAS 3.16–3.19).

Consistent with GAGAS 3.21, 3.64, and 3.65, auditors use professional judgment in applying the conceptual framework to determine independence in a given situation. When identifying and evaluating threats to independence, OIG employees and contractors must consider the broad

categories of threats to independence and the example safeguards provided in GAGAS, as well as the unique circumstances of the project. In addition to the GAGAS examples, specific situations that threaten independence and must be reported to the project manager or an appropriate official if the project manager is not available include the following:

- financial interest that is direct, or is significant or material though indirect, in the audited entity or program
- seeking employment with the division or program area to be reviewed or under review (including the time period leading up to the submission of a job application)
- preconceived ideas toward individuals, groups, organizations, or objectives of a particular program that could bias the project
- official, professional, personal, financial, or any kind of relationship that might cause an OIG employee or contractor to limit the extent of his or her inquiry, to limit disclosure, or to weaken or slant findings in any way
- external interference or influence that improperly or imprudently limits or modifies the scope of project work

When these or any other apparent or potential threats to independence are identified, the individual must immediately and fully disclose the situation to the project manager. The project manager, in consultation with the applicable Senior OIG Manager and Associate Inspector General, must determine whether identified threats to independence are significant and whether they can be reduced to an acceptable level with the imposition of safeguards. Any disclosed threats to independence and applied safeguards must be documented on this form (GAGAS 3.24). If the disclosed threats to independence are deemed insignificant, the basis for that determination must be documented on this form.

Failure to comply with the OIG's policies and procedures regarding independence may result in adverse or disciplinary action against the individual, up to and including termination, consistent with applicable Board policy.

Instructions

This form, which documents compliance with applicable independence standards, is to be completed at the start of each project by OIG or contractor project team members, as well as any OIG staff members who substantially contribute to the project in accordance with the OIG's *Independence* policy. Generally, the project's start date refers to the date the project is initiated in the audit system. A new form must be completed when circumstances change or when threats to independence arise that impact the individual's independence. In addition, this form must be completed by OIG referencers prior to their involvement in the project. The completed forms are maintained as electronic workpapers in the audit systems.

Certification

I certify that I have read and understand the above, as well as the OIG's *Independence* policy and GAGAS independence standards. With regard to the assigned project, I have evaluated threats to my independence, both independence of mind and in appearance, and attest that (select one):

☒ I have not identified any threats to my independence.

☐ I have identified threats to independence and applied safeguards, as described below.

Describe any threats to independence identified and safeguards applied (attach additional page if necessary).

☐ As a **referencer** for this project, I certify that I have not identified any threats to my independence that would prevent me from objectively performing the independent reference review.

I also agree to reevaluate my independence whenever my assignment is changed or whenever my circumstances change while working on this project. If changes affecting either my independence or my objectivity regarding this project occur subsequent to the completion of this form, I will immediately notify the project manager or an appropriate official if the project manager is not available.

Project name: 2014 Congressional Request on the Board's Personnel Practices

Individual's name: (b) (6) [redacted]

Date individual started on project: 8/4/14

Signature: (b) (6) [redacted] **Date:** 8/6/14

OFFICE OF INSPECTOR GENERAL
BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU
WASHINGTON, DC 20551

NON-DISCLOSURE AGREEMENT

I, (b) (6) _____, understand that, in the course of performing work for the Office of Inspector General (OIG) of the Board of Governors of the Federal Reserve System (Board) and the Consumer Financial Protection Bureau (CFPB), I may come into possession of or obtain knowledge of information of the OIG, the Board, the Federal Open Market Committee (FOMC), the Federal Reserve Banks, or the CFPB that is not public or that has not and is not required by law to be made public, including, for example, information that is designated as restricted, controlled, proprietary, confidential, confidential supervisory, or personnel (collectively, "*Confidential Information*"). Confidential Information shall include, but is not limited to (1) information pertaining to the security arrangements and strategies of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB (including information describing security controls related to information technology infrastructure such as network architecture and specific systems, applications, and databases); (2) economic data; (3) financial, statistical, and personnel data pertaining to the OIG, Board, FOMC, Federal Reserve Banks, CFPB, or other financial institutions; (4) financial, statistical, personnel planning and similar information relating to past, present, or future activities of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB; (5) pre-decisional deliberative information and data; (6) law enforcement privileged information; (7) attorney-client privileged information; (8) personally identifiable information; (9) trade-secret information; and (10) non-public information included in the files of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB.

Confidential Information does not include information that (1) is public; (2) is or becomes publicly available without breach by me of this Non-Disclosure Agreement ("*NDA*"); (3) was rightfully received by me without obligation of confidentiality; or (4) was developed by me independently of any disclosures to me made by the OIG, Board, FOMC, Federal Reserve Banks, or CFPB. Except for information I receive that is not Confidential Information, I will treat all information I receive from the OIG, Board, FOMC, Federal Reserve Banks, or CFPB as Confidential Information, regardless of the manner or form in which the information is transmitted or accessible. In addition, I will also treat the advice, deliverables, products, outputs, or similar items I provide or produce while working with the OIG ("*Product Information*") as Confidential Information until such time as the OIG informs me in writing that such Product Information is public.

Thus, I agree to the following terms:

1. I will keep in confidence all Confidential Information that may be acquired in connection with or as a result of my responsibilities. I will not, at any time, either during or after my work with the OIG, make public or otherwise communicate or disclose Confidential Information to anyone other than authorized personnel of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB, without the OIG's prior written consent. (The OIG will coordinate and obtain the necessary approval(s) from the Board, the FOMC, the Federal Reserve Banks, or the CFPB, as applicable.)

2. I will use Confidential Information solely in connection with my responsibilities in working for the OIG. I will not directly or indirectly use Confidential Information for my private gain or for the private gain of another person or entity at any time, either during or after termination of my work with the OIG.

3. I will inform the OIG of any external requests or demands for disclosure of Confidential Information, and I will refer all such demands and requests for disclosures, including but not limited to subpoenas, to the OIG.

4. Should a question arise as to whether particular information is Confidential Information, I will immediately contact the OIG and seek a determination as to the information's status. Until a determination has been made by the OIG (after coordination with the Board, FOMC, Federal Reserve Banks, or CFPB, as applicable), I shall treat it as Confidential Information in accordance with this NDA.

5. At all times, including during and after my work with the OIG, I will take all necessary steps to protect Confidential Information subject to this NDA.

6. Upon completion, expiration, or termination of my services, unless I am instructed otherwise by the OIG, I will promptly dispose of all Confidential Information in my possession in whatever manner is approved by the OIG for the disposal of such information, which may include the return of Confidential Information to the OIG.

7. I understand that I am prohibited from releasing any publicity or advertising regarding the work I perform for the OIG and from using the name or insignia of the OIG, Board, FOMC, CFPB, Federal Reserve Banks, or the Federal Reserve System, or any variation or adaptation thereof, for any commercial, advertisement, promotional, or endorsement purposes, unless the OIG and the Board's Chief Operating Officer (or his/her designee) has given prior written consent for such release or use.

8. I agree and acknowledge that the disclosure or use of any Confidential Information in breach of this NDA would cause irreparable harm to the OIG, Board, FOMC, CFPB, or Federal Reserve Banks. Accordingly, in the event of such use or disclosure, I understand that I may be subject to legal or other action, which may include termination of my work with the OIG and referral for criminal prosecution, if appropriate.

9. If I suspect that any Confidential Information to which I am given access is or may have been lost or disclosed without authorization, I will immediately notify the OIG.

I understanding that this NDA, all of its terms and conditions, shall remain in effect following the expiration or termination of my work with the OIG until this NDA is terminated in writing by the OIG.

(b) (6) _____ 8/6/14
DATE

(b) (6) _____
Printed Name

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

Statement of Independence on Individual Projects

The Office of Inspector General (OIG) and its staff and contractors must be independent in all matters relating to audit, inspection, and evaluation work. OIG employees and contractors who are engaged in audits, inspections, or evaluations are to comply with the OIG policy AE-001, *Independence,* and conduct themselves in a manner consistent with the Board of Governors of the Federal Reserve System's (Board) and the OIG's core values; the Board's *Principles of Ethical Conduct*; the *Standards of Ethical Conduct for Employees of the Executive Branch*, issued by the U.S. Office of Government Ethics; the generally accepted government auditing standards (GAGAS), issued by the Comptroller General of the United States; *Quality Standards for Inspection and Evaluation*, issued by the Council of the Inspectors General on Integrity and Efficiency; and any other standards applicable to their project. OIG employees and contractors must take precautions to ensure that their conduct is perceived as being independent, professional, and appropriate and are not to become involved in situations that impair independence or give the appearance that impairment to independence exists.

Independence comprises independence of mind and independence in appearance. Independence of mind is the state of mind that permits the performance of an audit without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism. Independence in appearance is the absence of circumstances that would cause a reasonable and informed third party, having knowledge of the relevant information, to reasonably conclude that the integrity, objectivity, or professional skepticism of an audit organization or member of the audit team had been compromised (GAGAS 3.03).

GAGAS establishes the conceptual framework (see GAGAS 3.07–3.26 and appendix II) that OIG employees and contractors must use to identify and evaluate threats to independence given the circumstances of their work. Whether independence is impaired depends on the nature of the threat, whether the threat is of such significance that it would compromise an auditor's professional judgment or create the appearance that the auditor's professional judgment may be compromised, and the specific safeguards applied to eliminate the threat or reduce it to an acceptable level. GAGAS provides broad categories of threats (GAGAS 3.14) and examples of circumstances that create threats to independence (GAGAS A3.02–A3.09) and it describes safeguards that may be effective in certain circumstances (GAGAS 3.16–3.19).

Consistent with GAGAS 3.21, 3.64, and 3.65, auditors use professional judgment in applying the conceptual framework to determine independence in a given situation. When identifying and evaluating threats to independence, OIG employees and contractors must consider the broad

categories of threats to independence and the example safeguards provided in GAGAS, as well as the unique circumstances of the project. In addition to the GAGAS examples, specific situations that threaten independence and must be reported to the project manager or an appropriate official if the project manager is not available include the following:

- financial interest that is direct, or is significant or material though indirect, in the audited entity or program
- seeking employment with the division or program area to be reviewed or under review (including the time period leading up to the submission of a job application)
- preconceived ideas toward individuals, groups, organizations, or objectives of a particular program that could bias the project
- official, professional, personal, financial, or any kind of relationship that might cause an OIG employee or contractor to limit the extent of his or her inquiry, to limit disclosure, or to weaken or slant findings in any way
- external interference or influence that improperly or imprudently limits or modifies the scope of project work

When these or any other apparent or potential threats to independence are identified, the individual must immediately and fully disclose the situation to the project manager. The project manager, in consultation with the applicable Senior OIG Manager and Associate Inspector General, must determine whether identified threats to independence are significant and whether they can be reduced to an acceptable level with the imposition of safeguards. Any disclosed threats to independence and applied safeguards must be documented on this form (GAGAS 3.24). If the disclosed threats to independence are deemed insignificant, the basis for that determination must be documented on this form.

Failure to comply with the OIG's policies and procedures regarding independence may result in adverse or disciplinary action against the individual, up to and including termination, consistent with applicable Board policy.

Instructions

This form, which documents compliance with applicable independence standards, is to be completed at the start of each project by OIG or contractor project team members, as well as any OIG staff members who substantially contribute to the project in accordance with the OIG's *Independence* policy. Generally, the project's start date refers to the date the project is initiated in the audit system. A new form must be completed when circumstances change or when threats to independence arise that impact the individual's independence. In addition, this form must be completed by OIG referencers prior to their involvement in the project. The completed forms are maintained as electronic workpapers in the audit systems.

Certification

I certify that I have read and understand the above, as well as the OIG's *Independence* policy and GAGAS independence standards. With regard to the assigned project, I have evaluated threats to my independence, both independence of mind and in appearance, and attest that (select one):

☒ I have not identified any threats to my independence.

☐ I have identified threats to independence and applied safeguards, as described below.

Describe any threats to independence identified and safeguards applied (attach additional page if necessary).

☐ As a **referencer** for this project, I certify that I have not identified any threats to my independence that would prevent me from objectively performing the independent reference review.

I also agree to reevaluate my independence whenever my assignment is changed or whenever my circumstances change while working on this project. If changes affecting either my independence or my objectivity regarding this project occur subsequent to the completion of this form, I will immediately notify the project manager or an appropriate official if the project manager is not available.

Project name: 2014 Congressional Request on the Board's Personnel Practices

Individual's name: (b) (6)

Date individual started on project: 8/4/2014

Signature: (b) (6) **Date:** 8/7/14

OFFICE OF INSPECTOR GENERAL
BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU
WASHINGTON, DC 20551

NON-DISCLOSURE AGREEMENT

I, (b) (6) , understand that, in the course of performing work for the Office of Inspector General (OIG) of the Board of Governors of the Federal Reserve System (Board) and the Consumer Financial Protection Bureau (CFPB), I may come into possession of or obtain knowledge of information of the OIG, the Board, the Federal Open Market Committee (FOMC), the Federal Reserve Banks, or the CFPB that is not public or that has not and is not required by law to be made public, including, for example, information that is designated as restricted, controlled, proprietary, confidential, confidential supervisory, or personnel (collectively, "*Confidential Information*"). Confidential Information shall include, but is not limited to (1) information pertaining to the security arrangements and strategies of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB (including information describing security controls related to information technology infrastructure such as network architecture and specific systems, applications, and databases); (2) economic data; (3) financial, statistical, and personnel data pertaining to the OIG, Board, FOMC, Federal Reserve Banks, CFPB, or other financial institutions; (4) financial, statistical, personnel planning and similar information relating to past, present, or future activities of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB; (5) pre-decisional deliberative information and data; (6) law enforcement privileged information; (7) attorney-client privileged information; (8) personally identifiable information; (9) trade-secret information; and (10) non-public information included in the files of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB.

Confidential Information does not include information that (1) is public; (2) is or becomes publicly available without breach by me of this Non-Disclosure Agreement ("*NDA*"); (3) was rightfully received by me without obligation of confidentiality; or (4) was developed by me independently of any disclosures to me made by the OIG, Board, FOMC, Federal Reserve Banks, or CFPB. Except for information I receive that is not Confidential Information, I will treat all information I receive from the OIG, Board, FOMC, Federal Reserve Banks, or CFPB as Confidential Information, regardless of the manner or form in which the information is transmitted or accessible. In addition, I will also treat the advice, deliverables, products, outputs, or similar items I provide or produce while working with the OIG ("*Product Information*") as Confidential Information until such time as the OIG informs me in writing that such Product Information is public.

Thus, I agree to the following terms:

1. I will keep in confidence all Confidential Information that may be acquired in connection with or as a result of my responsibilities. I will not, at any time, either during or after my work with the OIG, make public or otherwise communicate or disclose Confidential Information to anyone other than authorized personnel of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB, without the OIG's prior written consent. (The OIG will coordinate and obtain the necessary approval(s) from the Board, the FOMC, the Federal Reserve Banks, or the CFPB, as applicable.)

2. I will use Confidential Information solely in connection with my responsibilities in working for the OIG. I will not directly or indirectly use Confidential Information for my private gain or for the private gain of another person or entity at any time, either during or after termination of my work with the OIG.

3. I will inform the OIG of any external requests or demands for disclosure of Confidential Information, and I will refer all such demands and requests for disclosures, including but not limited to subpoenas, to the OIG.

4. Should a question arise as to whether particular information is Confidential Information, I will immediately contact the OIG and seek a determination as to the information's status. Until a determination has been made by the OIG (after coordination with the Board, FOMC, Federal Reserve Banks, or CFPB, as applicable), I shall treat it as Confidential Information in accordance with this NDA.

5. At all times, including during and after my work with the OIG, I will take all necessary steps to protect Confidential Information subject to this NDA.

6. Upon completion, expiration, or termination of my services, unless I am instructed otherwise by the OIG, I will promptly dispose of all Confidential Information in my possession in whatever manner is approved by the OIG for the disposal of such information, which may include the return of Confidential Information to the OIG.

7. I understand that I am prohibited from releasing any publicity or advertising regarding the work I perform for the OIG and from using the name or insignia of the OIG, Board, FOMC, CFPB, Federal Reserve Banks, or the Federal Reserve System, or any variation or adaptation thereof, for any commercial, advertisement, promotional, or endorsement purposes, unless the OIG and the Board's Chief Operating Officer (or his/her designee) has given prior written consent for such release or use.

8. I agree and acknowledge that the disclosure or use of any Confidential Information in breach of this NDA would cause irreparable harm to the OIG, Board, FOMC, CFPB, or Federal Reserve Banks. Accordingly, in the event of such use or disclosure, I understand that I may be subject to legal or other action, which may include termination of my work with the OIG and referral for criminal prosecution, if appropriate.

9. If I suspect that any Confidential Information to which I am given access is or may have been lost or disclosed without authorization, I will immediately notify the OIG.

I understanding that this NDA, all of its terms and conditions, shall remain in effect following the expiration or termination of my work with the OIG until this NDA is terminated in writing by the OIG.

(b) (6)

SIGNATURE

8/7/14

DATE

(b) (6)

Printed Name

OFFICE OF INSPECTOR GENERAL
BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU

Statement of Independence on Individual Projects

The Office of Inspector General (OIG) and its staff and contractors must be independent in all matters relating to audit, inspection, and evaluation work. OIG employees and contractors who are engaged in audits, inspections, or evaluations are to comply with the OIG policy AE-001, *Independence,* and conduct themselves in a manner consistent with the Board of Governors of the Federal Reserve System's (Board) and the OIG's core values; the Board's *Principles of Ethical Conduct*; the *Standards of Ethical Conduct for Employees of the Executive Branch*, issued by the U.S. Office of Government Ethics; the generally accepted government auditing standards (GAGAS), issued by the Comptroller General of the United States; *Quality Standards for Inspection and Evaluation*, issued by the Council of the Inspectors General on Integrity and Efficiency; and any other standards applicable to their project. OIG employees and contractors must take precautions to ensure that their conduct is perceived as being independent, professional, and appropriate and are not to become involved in situations that impair independence or give the appearance that impairment to independence exists.

Independence comprises independence of mind and independence in appearance. Independence of mind is the state of mind that permits the performance of an audit without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism. Independence in appearance is the absence of circumstances that would cause a reasonable and informed third party, having knowledge of the relevant information, to reasonably conclude that the integrity, objectivity, or professional skepticism of an audit organization or member of the audit team had been compromised (GAGAS 3.03).

GAGAS establishes the conceptual framework (see GAGAS 3.07–3.26 and appendix II) that OIG employees and contractors must use to identify and evaluate threats to independence given the circumstances of their work. Whether independence is impaired depends on the nature of the threat, whether the threat is of such significance that it would compromise an auditor's professional judgment or create the appearance that the auditor's professional judgment may be compromised, and the specific safeguards applied to eliminate the threat or reduce it to an acceptable level. GAGAS provides broad categories of threats (GAGAS 3.14) and examples of circumstances that create threats to independence (GAGAS A3.02–A3.09) and it describes safeguards that may be effective in certain circumstances (GAGAS 3.16–3.19).

Consistent with GAGAS 3.21, 3.64, and 3.65, auditors use professional judgment in applying the conceptual framework to determine independence in a given situation. When identifying and evaluating threats to independence, OIG employees and contractors must consider the broad

categories of threats to independence and the example safeguards provided in GAGAS, as well as the unique circumstances of the project. In addition to the GAGAS examples, specific situations that threaten independence and must be reported to the project manager or an appropriate official if the project manager is not available include the following:

- financial interest that is direct, or is significant or material though indirect, in the audited entity or program
- seeking employment with the division or program area to be reviewed or under review (including the time period leading up to the submission of a job application)
- preconceived ideas toward individuals, groups, organizations, or objectives of a particular program that could bias the project
- official, professional, personal, financial, or any kind of relationship that might cause an OIG employee or contractor to limit the extent of his or her inquiry, to limit disclosure, or to weaken or slant findings in any way
- external interference or influence that improperly or imprudently limits or modifies the scope of project work

When these or any other apparent or potential threats to independence are identified, the individual must immediately and fully disclose the situation to the project manager. The project manager, in consultation with the applicable Senior OIG Manager and Associate Inspector General, must determine whether identified threats to independence are significant and whether they can be reduced to an acceptable level with the imposition of safeguards. Any disclosed threats to independence and applied safeguards must be documented on this form (GAGAS 3.24). If the disclosed threats to independence are deemed insignificant, the basis for that determination must be documented on this form.

Failure to comply with the OIG's policies and procedures regarding independence may result in adverse or disciplinary action against the individual, up to and including termination, consistent with applicable Board policy.

Instructions

This form, which documents compliance with applicable independence standards, is to be completed at the start of each project by OIG or contractor project team members, as well as any OIG staff members who substantially contribute to the project in accordance with the OIG's *Independence* policy. Generally, the project's start date refers to the date the project is initiated in the audit system. A new form must be completed when circumstances change or when threats to independence arise that impact the individual's independence. In addition, this form must be completed by OIG referencers prior to their involvement in the project. The completed forms are maintained as electronic workpapers in the audit systems.

Certification

I certify that I have read and understand the above, as well as the OIG's *Independence* policy and GAGAS independence standards. With regard to the assigned project, I have evaluated threats to my independence, both independence of mind and in appearance, and attest that (select one):

☑ I have not identified any threats to my independence.

☐ I have identified threats to independence and applied safeguards, as described below.

Describe any threats to independence identified and safeguards applied (attach additional page if necessary).

☐ As a **referencer** for this project, I certify that I have not identified any threats to my independence that would prevent me from objectively performing the independent reference review.

I also agree to reevaluate my independence whenever my assignment is changed or whenever my circumstances change while working on this project. If changes affecting either my independence or my objectivity regarding this project occur subsequent to the completion of this form, I will immediately notify the project manager or an appropriate official if the project manager is not available.

Project name: 2014 Congressional Request on the Board's Personnel Practices

Individual's name: (b) (6) [redacted]

Date individual started on project: 8/4/14

Signature: (b) (6) [redacted] **Date:** 8/6/2014

OFFICE OF INSPECTOR GENERAL
BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU
WASHINGTON, DC 20551

NON-DISCLOSURE AGREEMENT

I, (b) (6) , understand that, in the course of performing work for the Office of Inspector General (OIG) of the Board of Governors of the Federal Reserve System (Board) and the Consumer Financial Protection Bureau (CFPB), I may come into possession of or obtain knowledge of information of the OIG, the Board, the Federal Open Market Committee (FOMC), the Federal Reserve Banks, or the CFPB that is not public or that has not and is not required by law to be made public, including, for example, information that is designated as restricted, controlled, proprietary, confidential, confidential supervisory, or personnel (collectively, "*Confidential Information*"). Confidential Information shall include, but is not limited to (1) information pertaining to the security arrangements and strategies of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB (including information describing security controls related to information technology infrastructure such as network architecture and specific systems, applications, and databases); (2) economic data; (3) financial, statistical, and personnel data pertaining to the OIG, Board, FOMC, Federal Reserve Banks, CFPB, or other financial institutions; (4) financial, statistical, personnel planning and similar information relating to past, present, or future activities of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB; (5) pre-decisional deliberative information and data; (6) law enforcement privileged information; (7) attorney-client privileged information; (8) personally identifiable information; (9) trade-secret information; and (10) non-public information included in the files of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB.

Confidential Information does not include information that (1) is public; (2) is or becomes publicly available without breach by me of this Non-Disclosure Agreement ("*NDA*"); (3) was rightfully received by me without obligation of confidentiality; or (4) was developed by me independently of any disclosures to me made by the OIG, Board, FOMC, Federal Reserve Banks, or CFPB. Except for information I receive that is not Confidential Information, I will treat all information I receive from the OIG, Board, FOMC, Federal Reserve Banks, or CFPB as Confidential Information, regardless of the manner or form in which the information is transmitted or accessible. In addition, I will also treat the advice, deliverables, products, outputs, or similar items I provide or produce while working with the OIG ("*Product Information*") as Confidential Information until such time as the OIG informs me in writing that such Product Information is public.

Thus, I agree to the following terms:

1. I will keep in confidence all Confidential Information that may be acquired in connection with or as a result of my responsibilities. I will not, at any time, either during or after my work with the OIG, make public or otherwise communicate or disclose Confidential Information to anyone other than authorized personnel of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB, without the OIG's prior written consent. (The OIG will coordinate and obtain the necessary approval(s) from the Board, the FOMC, the Federal Reserve Banks, or the CFPB, as applicable.)

2. I will use Confidential Information solely in connection with my responsibilities in working for the OIG. I will not directly or indirectly use Confidential Information for my private gain or for the private gain of another person or entity at any time, either during or after termination of my work with the OIG.

3. I will inform the OIG of any external requests or demands for disclosure of Confidential Information, and I will refer all such demands and requests for disclosures, including but not limited to subpoenas, to the OIG.

4. Should a question arise as to whether particular information is Confidential Information, I will immediately contact the OIG and seek a determination as to the information's status. Until a determination has been made by the OIG (after coordination with the Board, FOMC, Federal Reserve Banks, or CFPB, as applicable), I shall treat it as Confidential Information in accordance with this NDA.

5. At all times, including during and after my work with the OIG, I will take all necessary steps to protect Confidential Information subject to this NDA.

6. Upon completion, expiration, or termination of my services, unless I am instructed otherwise by the OIG, I will promptly dispose of all Confidential Information in my possession in whatever manner is approved by the OIG for the disposal of such information, which may include the return of Confidential Information to the OIG.

7. I understand that I am prohibited from releasing any publicity or advertising regarding the work I perform for the OIG and from using the name or insignia of the OIG, Board, FOMC, CFPB, Federal Reserve Banks, or the Federal Reserve System, or any variation or adaptation thereof, for any commercial, advertisement, promotional, or endorsement purposes, unless the OIG and the Board's Chief Operating Officer (or his/her designee) has given prior written consent for such release or use.

8. I agree and acknowledge that the disclosure or use of any Confidential Information in breach of this NDA would cause irreparable harm to the OIG, Board, FOMC, CFPB, or Federal Reserve Banks. Accordingly, in the event of such use or disclosure, I understand that I may be subject to legal or other action, which may include termination of my work with the OIG and referral for criminal prosecution, if appropriate.

9. If I suspect that any Confidential Information to which I am given access is or may have been lost or disclosed without authorization, I will immediately notify the OIG.

I understanding that this NDA, all of its terms and conditions, shall remain in effect following the expiration or termination of my work with the OIG until this NDA is terminated in writing by the OIG.

(b) (6) [redacted]

SIGNATURE

8/6/2014

DATE

(b) (6) [redacted]

Printed Name

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

Statement of Independence on Individual Projects

The Office of Inspector General (OIG) and its staff and contractors must be independent in all matters relating to audit, inspection, and evaluation work. OIG employees and contractors who are engaged in audits, inspections, or evaluations are to comply with the OIG policy AE-001, *Independence,* and conduct themselves in a manner consistent with the Board of Governors of the Federal Reserve System's (Board) and the OIG's core values; the Board's *Principles of Ethical Conduct*; the *Standards of Ethical Conduct for Employees of the Executive Branch*, issued by the U.S. Office of Government Ethics; the generally accepted government auditing standards (GAGAS), issued by the Comptroller General of the United States; *Quality Standards for Inspection and Evaluation*, issued by the Council of the Inspectors General on Integrity and Efficiency; and any other standards applicable to their project. OIG employees and contractors must take precautions to ensure that their conduct is perceived as being independent, professional, and appropriate and are not to become involved in situations that impair independence or give the appearance that impairment to independence exists.

Independence comprises independence of mind and independence in appearance. Independence of mind is the state of mind that permits the performance of an audit without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism. Independence in appearance is the absence of circumstances that would cause a reasonable and informed third party, having knowledge of the relevant information, to reasonably conclude that the integrity, objectivity, or professional skepticism of an audit organization or member of the audit team had been compromised (GAGAS 3.03).

GAGAS establishes the conceptual framework (see GAGAS 3.07–3.26 and appendix II) that OIG employees and contractors must use to identify and evaluate threats to independence given the circumstances of their work. Whether independence is impaired depends on the nature of the threat, whether the threat is of such significance that it would compromise an auditor's professional judgment or create the appearance that the auditor's professional judgment may be compromised, and the specific safeguards applied to eliminate the threat or reduce it to an acceptable level. GAGAS provides broad categories of threats (GAGAS 3.14) and examples of circumstances that create threats to independence (GAGAS A3.02–A3.09) and it describes safeguards that may be effective in certain circumstances (GAGAS 3.16–3.19).

Consistent with GAGAS 3.21, 3.64, and 3.65, auditors use professional judgment in applying the conceptual framework to determine independence in a given situation. When identifying and evaluating threats to independence, OIG employees and contractors must consider the broad

categories of threats to independence and the example safeguards provided in GAGAS, as well as the unique circumstances of the project. In addition to the GAGAS examples, specific situations that threaten independence and must be reported to the project manager or an appropriate official if the project manager is not available include the following:

- financial interest that is direct, or is significant or material though indirect, in the audited entity or program
- seeking employment with the division or program area to be reviewed or under review (including the time period leading up to the submission of a job application)
- preconceived ideas toward individuals, groups, organizations, or objectives of a particular program that could bias the project
- official, professional, personal, financial, or any kind of relationship that might cause an OIG employee or contractor to limit the extent of his or her inquiry, to limit disclosure, or to weaken or slant findings in any way
- external interference or influence that improperly or imprudently limits or modifies the scope of project work

When these or any other apparent or potential threats to independence are identified, the individual must immediately and fully disclose the situation to the project manager. The project manager, in consultation with the applicable Senior OIG Manager and Associate Inspector General, must determine whether identified threats to independence are significant and whether they can be reduced to an acceptable level with the imposition of safeguards. Any disclosed threats to independence and applied safeguards must be documented on this form (GAGAS 3.24). If the disclosed threats to independence are deemed insignificant, the basis for that determination must be documented on this form.

Failure to comply with the OIG's policies and procedures regarding independence may result in adverse or disciplinary action against the individual, up to and including termination, consistent with applicable Board policy.

Instructions

This form, which documents compliance with applicable independence standards, is to be completed at the start of each project by OIG or contractor project team members, as well as any OIG staff members who substantially contribute to the project in accordance with the OIG's *Independence* policy. Generally, the project's start date refers to the date the project is initiated in the audit system. A new form must be completed when circumstances change or when threats to independence arise that impact the individual's independence. In addition, this form must be completed by OIG referencers prior to their involvement in the project. The completed forms are maintained as electronic workpapers in the audit systems.

Certification

I certify that I have read and understand the above, as well as the OIG's *Independence* policy and GAGAS independence standards. With regard to the assigned project, I have evaluated threats to my independence, both independence of mind and in appearance, and attest that (select one):

☒ I have not identified any threats to my independence.

☐ I have identified threats to independence and applied safeguards, as described below.

Describe any threats to independence identified and safeguards applied (attach additional page if necessary).

☐ As a **referencer** for this project, I certify that I have not identified any threats to my independence that would prevent me from objectively performing the independent reference review.

I also agree to reevaluate my independence whenever my assignment is changed or whenever my circumstances change while working on this project. If changes affecting either my independence or my objectivity regarding this project occur subsequent to the completion of this form, I will immediately notify the project manager or an appropriate official if the project manager is not available.

Project name: 2014 Congressional Request on the Board's Personnel Practices

Individual's name: (b) (6) [redacted]

Date individual started on project: 8/4/2014

Signature: (b) (6) [redacted] **Date:** 8/7/2014

OFFICE OF INSPECTOR GENERAL
BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU
WASHINGTON, DC 20551

NON-DISCLOSURE AGREEMENT

I, (b) (6) _____, understand that, in the course of performing work for the Office of Inspector General (OIG) of the Board of Governors of the Federal Reserve System (Board) and the Consumer Financial Protection Bureau (CFPB), I may come into possession of or obtain knowledge of information of the OIG, the Board, the Federal Open Market Committee (FOMC), the Federal Reserve Banks, or the CFPB that is not public or that has not and is not required by law to be made public, including, for example, information that is designated as restricted, controlled, proprietary, confidential, confidential supervisory, or personnel (collectively, "*Confidential Information*"). Confidential Information shall include, but is not limited to (1) information pertaining to the security arrangements and strategies of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB (including information describing security controls related to information technology infrastructure such as network architecture and specific systems, applications, and databases); (2) economic data; (3) financial, statistical, and personnel data pertaining to the OIG, Board, FOMC, Federal Reserve Banks, CFPB, or other financial institutions; (4) financial, statistical, personnel planning and similar information relating to past, present, or future activities of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB; (5) pre-decisional deliberative information and data; (6) law enforcement privileged information; (7) attorney-client privileged information; (8) personally identifiable information; (9) trade-secret information; and (10) non-public information included in the files of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB.

Confidential Information does not include information that (1) is public; (2) is or becomes publicly available without breach by me of this Non-Disclosure Agreement ("*NDA*"); (3) was rightfully received by me without obligation of confidentiality; or (4) was developed by me independently of any disclosures to me made by the OIG, Board, FOMC, Federal Reserve Banks, or CFPB. Except for information I receive that is not Confidential Information, I will treat all information I receive from the OIG, Board, FOMC, Federal Reserve Banks, or CFPB as Confidential Information, regardless of the manner or form in which the information is transmitted or accessible. In addition, I will also treat the advice, deliverables, products, outputs, or similar items I provide or produce while working with the OIG ("*Product Information*") as Confidential Information until such time as the OIG informs me in writing that such Product Information is public.

Thus, I agree to the following terms:

1. I will keep in confidence all Confidential Information that may be acquired in connection with or as a result of my responsibilities. I will not, at any time, either during or after my work with the OIG, make public or otherwise communicate or disclose Confidential Information to anyone other than authorized personnel of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB, without the OIG's prior written consent. (The OIG will coordinate and obtain the necessary approval(s) from the Board, the FOMC, the Federal Reserve Banks, or the CFPB, as applicable.)

2. I will use Confidential Information solely in connection with my responsibilities in working for the OIG. I will not directly or indirectly use Confidential Information for my private gain or for the private gain of another person or entity at any time, either during or after termination of my work with the OIG.

3. I will inform the OIG of any external requests or demands for disclosure of Confidential Information, and I will refer all such demands and requests for disclosures, including but not limited to subpoenas, to the OIG.

4. Should a question arise as to whether particular information is Confidential Information, I will immediately contact the OIG and seek a determination as to the information's status. Until a determination has been made by the OIG (after coordination with the Board, FOMC, Federal Reserve Banks, or CFPB, as applicable), I shall treat it as Confidential Information in accordance with this NDA.

5. At all times, including during and after my work with the OIG, I will take all necessary steps to protect Confidential Information subject to this NDA.

6. Upon completion, expiration, or termination of my services, unless I am instructed otherwise by the OIG, I will promptly dispose of all Confidential Information in my possession in whatever manner is approved by the OIG for the disposal of such information, which may include the return of Confidential Information to the OIG.

7. I understand that I am prohibited from releasing any publicity or advertising regarding the work I perform for the OIG and from using the name or insignia of the OIG, Board, FOMC, CFPB, Federal Reserve Banks, or the Federal Reserve System, or any variation or adaptation thereof, for any commercial, advertisement, promotional, or endorsement purposes, unless the OIG and the Board's Chief Operating Officer (or his/her designee) has given prior written consent for such release or use.

8. I agree and acknowledge that the disclosure or use of any Confidential Information in breach of this NDA would cause irreparable harm to the OIG, Board, FOMC, CFPB, or Federal Reserve Banks. Accordingly, in the event of such use or disclosure, I understand that I may be subject to legal or other action, which may include termination of my work with the OIG and referral for criminal prosecution, if appropriate.

9. If I suspect that any Confidential Information to which I am given access is or may have been lost or disclosed without authorization, I will immediately notify the OIG.

I understanding that this NDA, all of its terms and conditions, shall remain in effect following the expiration or termination of my work with the OIG until this NDA is terminated in writing by the OIG.

(b) (6)

SIGNATURE

8/7/2014

DATE

(b) (6)

Printed Name

OFFICE OF INSPECTOR GENERAL
BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU

Statement of Independence on Individual Projects

The Office of Inspector General (OIG) and its staff and contractors must be independent in all matters relating to audit, inspection, and evaluation work. OIG employees and contractors who are engaged in audits, inspections, or evaluations are to comply with the OIG policy AE-001, *Independence,* and conduct themselves in a manner consistent with the Board of Governors of the Federal Reserve System's (Board) and the OIG's core values; the Board's *Principles of Ethical Conduct*; the *Standards of Ethical Conduct for Employees of the Executive Branch,* issued by the U.S. Office of Government Ethics; the generally accepted government auditing standards (GAGAS), issued by the Comptroller General of the United States; *Quality Standards for Inspection and Evaluation*, issued by the Council of the Inspectors General on Integrity and Efficiency; and any other standards applicable to their project. OIG employees and contractors must take precautions to ensure that their conduct is perceived as being independent, professional, and appropriate and are not to become involved in situations that impair independence or give the appearance that impairment to independence exists.

Independence comprises independence of mind and independence in appearance. Independence of mind is the state of mind that permits the performance of an audit without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism. Independence in appearance is the absence of circumstances that would cause a reasonable and informed third party, having knowledge of the relevant information, to reasonably conclude that the integrity, objectivity, or professional skepticism of an audit organization or member of the audit team had been compromised (GAGAS 3.03).

GAGAS establishes the conceptual framework (see GAGAS 3.07–3.26 and appendix II) that OIG employees and contractors must use to identify and evaluate threats to independence given the circumstances of their work. Whether independence is impaired depends on the nature of the threat, whether the threat is of such significance that it would compromise an auditor's professional judgment or create the appearance that the auditor's professional judgment may be compromised, and the specific safeguards applied to eliminate the threat or reduce it to an acceptable level. GAGAS provides broad categories of threats (GAGAS 3.14) and examples of circumstances that create threats to independence (GAGAS A3.02–A3.09) and it describes safeguards that may be effective in certain circumstances (GAGAS 3.16–3.19).

Consistent with GAGAS 3.21, 3.64, and 3.65, auditors use professional judgment in applying the conceptual framework to determine independence in a given situation. When identifying and evaluating threats to independence, OIG employees and contractors must consider the broad

categories of threats to independence and the example safeguards provided in GAGAS, as well as the unique circumstances of the project. In addition to the GAGAS examples, specific situations that threaten independence and must be reported to the project manager or an appropriate official if the project manager is not available include the following:

- financial interest that is direct, or is significant or material though indirect, in the audited entity or program
- seeking employment with the division or program area to be reviewed or under review (including the time period leading up to the submission of a job application)
- preconceived ideas toward individuals, groups, organizations, or objectives of a particular program that could bias the project
- official, professional, personal, financial, or any kind of relationship that might cause an OIG employee or contractor to limit the extent of his or her inquiry, to limit disclosure, or to weaken or slant findings in any way
- external interference or influence that improperly or imprudently limits or modifies the scope of project work

When these or any other apparent or potential threats to independence are identified, the individual must immediately and fully disclose the situation to the project manager. The project manager, in consultation with the applicable Senior OIG Manager and Associate Inspector General, must determine whether identified threats to independence are significant and whether they can be reduced to an acceptable level with the imposition of safeguards. Any disclosed threats to independence and applied safeguards must be documented on this form (GAGAS 3.24). If the disclosed threats to independence are deemed insignificant, the basis for that determination must be documented on this form.

Failure to comply with the OIG's policies and procedures regarding independence may result in adverse or disciplinary action against the individual, up to and including termination, consistent with applicable Board policy.

Instructions

This form, which documents compliance with applicable independence standards, is to be completed at the start of each project by OIG or contractor project team members, as well as any OIG staff members who substantially contribute to the project in accordance with the OIG's *Independence* policy. Generally, the project's start date refers to the date the project is initiated in the audit system. A new form must be completed when circumstances change or when threats to independence arise that impact the individual's independence. In addition, this form must be completed by OIG referencers prior to their involvement in the project. The completed forms are maintained as electronic workpapers in the audit systems.

Certification

I certify that I have read and understand the above, as well as the OIG's *Independence* policy and GAGAS independence standards. With regard to the assigned project, I have evaluated threats to my independence, both independence of mind and in appearance, and attest that (select one):

☒ I have not identified any threats to my independence.

☐ I have identified threats to independence and applied safeguards, as described below.

Describe any threats to independence identified and safeguards applied (attach additional page if necessary).

☐ As a **referencer** for this project, I certify that I have not identified any threats to my independence that would prevent me from objectively performing the independent reference review.

I also agree to reevaluate my independence whenever my assignment is changed or whenever my circumstances change while working on this project. If changes affecting either my independence or my objectivity regarding this project occur subsequent to the completion of this form, I will immediately notify the project manager or an appropriate official if the project manager is not available.

Project name: 2014 Congressional Request on the Board's Personnel Practices

Individual's name: (b) (6) _____

Date individual started on project: 8/4/14

Signature: (b) (6) _____ **Date:** 8/6/14

OFFICE OF INSPECTOR GENERAL
BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU
WASHINGTON, DC 20551

NON-DISCLOSURE AGREEMENT

I, (b) (6) _____, understand that, in the course of performing work for the Office of Inspector General (OIG) of the Board of Governors of the Federal Reserve System (Board) and the Consumer Financial Protection Bureau (CFPB), I may come into possession of or obtain knowledge of information of the OIG, the Board, the Federal Open Market Committee (FOMC), the Federal Reserve Banks, or the CFPB that is not public or that has not and is not required by law to be made public, including, for example, information that is designated as restricted, controlled, proprietary, confidential, confidential supervisory, or personnel (collectively, "*Confidential Information*"). Confidential Information shall include, but is not limited to (1) information pertaining to the security arrangements and strategies of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB (including information describing security controls related to information technology infrastructure such as network architecture and specific systems, applications, and databases); (2) economic data; (3) financial, statistical, and personnel data pertaining to the OIG, Board, FOMC, Federal Reserve Banks, CFPB, or other financial institutions; (4) financial, statistical, personnel planning and similar information relating to past, present, or future activities of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB; (5) pre-decisional deliberative information and data; (6) law enforcement privileged information; (7) attorney-client privileged information; (8) personally identifiable information; (9) trade-secret information; and (10) non-public information included in the files of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB.

Confidential Information does not include information that (1) is public; (2) is or becomes publicly available without breach by me of this Non-Disclosure Agreement ("*NDA*"); (3) was rightfully received by me without obligation of confidentiality; or (4) was developed by me independently of any disclosures to me made by the OIG, Board, FOMC, Federal Reserve Banks, or CFPB. Except for information I receive that is not Confidential Information, I will treat all information I receive from the OIG, Board, FOMC, Federal Reserve Banks, or CFPB as Confidential Information, regardless of the manner or form in which the information is transmitted or accessible. In addition, I will also treat the advice, deliverables, products, outputs, or similar items I provide or produce while working with the OIG ("*Product Information*") as Confidential Information until such time as the OIG informs me in writing that such Product Information is public.

Thus, I agree to the following terms:

1. I will keep in confidence all Confidential Information that may be acquired in connection with or as a result of my responsibilities. I will not, at any time, either during or after my work with the OIG, make public or otherwise communicate or disclose Confidential Information to anyone other than authorized personnel of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB, without the OIG's prior written consent. (The OIG will coordinate and obtain the necessary approval(s) from the Board, the FOMC, the Federal Reserve Banks, or the CFPB, as applicable.)

2. I will use Confidential Information solely in connection with my responsibilities in working for the OIG. I will not directly or indirectly use Confidential Information for my private gain or for the private gain of another person or entity at any time, either during or after termination of my work with the OIG.

3. I will inform the OIG of any external requests or demands for disclosure of Confidential Information, and I will refer all such demands and requests for disclosures, including but not limited to subpoenas, to the OIG.

4. Should a question arise as to whether particular information is Confidential Information, I will immediately contact the OIG and seek a determination as to the information's status. Until a determination has been made by the OIG (after coordination with the Board, FOMC, Federal Reserve Banks, or CFPB, as applicable), I shall treat it as Confidential Information in accordance with this NDA.

5. At all times, including during and after my work with the OIG, I will take all necessary steps to protect Confidential Information subject to this NDA.

6. Upon completion, expiration, or termination of my services, unless I am instructed otherwise by the OIG, I will promptly dispose of all Confidential Information in my possession in whatever manner is approved by the OIG for the disposal of such information, which may include the return of Confidential Information to the OIG.

7. I understand that I am prohibited from releasing any publicity or advertising regarding the work I perform for the OIG and from using the name or insignia of the OIG, Board, FOMC, CFPB, Federal Reserve Banks, or the Federal Reserve System, or any variation or adaptation thereof, for any commercial, advertisement, promotional, or endorsement purposes, unless the OIG and the Board's Chief Operating Officer (or his/her designee) has given prior written consent for such release or use.

8. I agree and acknowledge that the disclosure or use of any Confidential Information in breach of this NDA would cause irreparable harm to the OIG, Board, FOMC, CFPB, or Federal Reserve Banks. Accordingly, in the event of such use or disclosure, I understand that I may be subject to legal or other action, which may include termination of my work with the OIG and referral for criminal prosecution, if appropriate.

9. If I suspect that any Confidential Information to which I am given access is or may have been lost or disclosed without authorization, I will immediately notify the OIG.

I understanding that this NDA, all of its terms and conditions, shall remain in effect following the expiration or termination of my work with the OIG until this NDA is terminated in writing by the OIG.

(b) (6) _____ 8/11/14

SIGNATURE DATE

(b) (6) _____

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

Statement of Independence on Individual Projects

The Office of Inspector General (OIG) and its staff and contractors must be independent in all matters relating to audit, inspection, and evaluation work. OIG employees and contractors who are engaged in audits, inspections, or evaluations are to comply with the OIG policy AE-001, *Independence,* and conduct themselves in a manner consistent with the Board of Governors of the Federal Reserve System's (Board) and the OIG's core values; the Board's *Principles of Ethical Conduct*; the *Standards of Ethical Conduct for Employees of the Executive Branch*, issued by the U.S. Office of Government Ethics; the generally accepted government auditing standards (GAGAS), issued by the Comptroller General of the United States; *Quality Standards for Inspection and Evaluation*, issued by the Council of the Inspectors General on Integrity and Efficiency; and any other standards applicable to their project. OIG employees and contractors must take precautions to ensure that their conduct is perceived as being independent, professional, and appropriate and are not to become involved in situations that impair independence or give the appearance that impairment to independence exists.

Independence comprises independence of mind and independence in appearance. Independence of mind is the state of mind that permits the performance of an audit without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism. Independence in appearance is the absence of circumstances that would cause a reasonable and informed third party, having knowledge of the relevant information, to reasonably conclude that the integrity, objectivity, or professional skepticism of an audit organization or member of the audit team had been compromised (GAGAS 3.03).

GAGAS establishes the conceptual framework (see GAGAS 3.07–3.26 and appendix II) that OIG employees and contractors must use to identify and evaluate threats to independence given the circumstances of their work. Whether independence is impaired depends on the nature of the threat, whether the threat is of such significance that it would compromise an auditor's professional judgment or create the appearance that the auditor's professional judgment may be compromised, and the specific safeguards applied to eliminate the threat or reduce it to an acceptable level. GAGAS provides broad categories of threats (GAGAS 3.14) and examples of circumstances that create threats to independence (GAGAS A3.02–A3.09) and it describes safeguards that may be effective in certain circumstances (GAGAS 3.16–3.19).

Consistent with GAGAS 3.21, 3.64, and 3.65, auditors use professional judgment in applying the conceptual framework to determine independence in a given situation. When identifying and evaluating threats to independence, OIG employees and contractors must consider the broad

categories of threats to independence and the example safeguards provided in GAGAS, as well as the unique circumstances of the project. In addition to the GAGAS examples, specific situations that threaten independence and must be reported to the project manager or an appropriate official if the project manager is not available include the following:

- financial interest that is direct, or is significant or material though indirect, in the audited entity or program
- seeking employment with the division or program area to be reviewed or under review (including the time period leading up to the submission of a job application)
- preconceived ideas toward individuals, groups, organizations, or objectives of a particular program that could bias the project
- official, professional, personal, financial, or any kind of relationship that might cause an OIG employee or contractor to limit the extent of his or her inquiry, to limit disclosure, or to weaken or slant findings in any way
- external interference or influence that improperly or imprudently limits or modifies the scope of project work

When these or any other apparent or potential threats to independence are identified, the individual must immediately and fully disclose the situation to the project manager. The project manager, in consultation with the applicable Senior OIG Manager and Associate Inspector General, must determine whether identified threats to independence are significant and whether they can be reduced to an acceptable level with the imposition of safeguards. Any disclosed threats to independence and applied safeguards must be documented on this form (GAGAS 3.24). If the disclosed threats to independence are deemed insignificant, the basis for that determination must be documented on this form.

Failure to comply with the OIG's policies and procedures regarding independence may result in adverse or disciplinary action against the individual, up to and including termination, consistent with applicable Board policy.

Instructions

This form, which documents compliance with applicable independence standards, is to be completed at the start of each project by OIG or contractor project team members, as well as any OIG staff members who substantially contribute to the project in accordance with the OIG's *Independence* policy. Generally, the project's start date refers to the date the project is initiated in the audit system. A new form must be completed when circumstances change or when threats to independence arise that impact the individual's independence. In addition, this form must be completed by OIG referencers prior to their involvement in the project. The completed forms are maintained as electronic workpapers in the audit systems.

Certification

I certify that I have read and understand the above, as well as the OIG's *Independence* policy and GAGAS independence standards. With regard to the assigned project, I have evaluated threats to my independence, both independence of mind and in appearance, and attest that (select one):

☑ I have not identified any threats to my independence.

☐ I have identified threats to independence and applied safeguards, as described below.

Describe any threats to independence identified and safeguards applied (attach additional page if necessary).

☐ As a **referencer** for this project, I certify that I have not identified any threats to my independence that would prevent me from objectively performing the independent reference review.

I also agree to reevaluate my independence whenever my assignment is changed or whenever my circumstances change while working on this project. If changes affecting either my independence or my objectivity regarding this project occur subsequent to the completion of this form, I will immediately notify the project manager or an appropriate official if the project manager is not available.

Project name: 2014 Congressional Request on the Board's Personnel Practices

Individual's name: (b) (6) [redacted]

Date individual started on project: 08/04/2014

Signature: (b) (6) [redacted] **Date:** 08/07/2014

OFFICE OF INSPECTOR GENERAL
BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU
WASHINGTON, DC 20551

NON-DISCLOSURE AGREEMENT

I, (b) (6) _____, understand that, in the course of performing work for the Office of Inspector General (OIG) of the Board of Governors of the Federal Reserve System (Board) and the Consumer Financial Protection Bureau (CFPB), I may come into possession of or obtain knowledge of information of the OIG, the Board, the Federal Open Market Committee (FOMC), the Federal Reserve Banks, or the CFPB that is not public or that has not and is not required by law to be made public, including, for example, information that is designated as restricted, controlled, proprietary, confidential, confidential supervisory, or personnel (collectively, "*Confidential Information*"). Confidential Information shall include, but is not limited to (1) information pertaining to the security arrangements and strategies of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB (including information describing security controls related to information technology infrastructure such as network architecture and specific systems, applications, and databases); (2) economic data; (3) financial, statistical, and personnel data pertaining to the OIG, Board, FOMC, Federal Reserve Banks, CFPB, or other financial institutions; (4) financial, statistical, personnel planning and similar information relating to past, present, or future activities of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB; (5) pre-decisional deliberative information and data; (6) law enforcement privileged information; (7) attorney-client privileged information; (8) personally identifiable information; (9) trade-secret information; and (10) non-public information included in the files of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB.

Confidential Information does not include information that (1) is public; (2) is or becomes publicly available without breach by me of this Non-Disclosure Agreement ("*NDA*"); (3) was rightfully received by me without obligation of confidentiality; or (4) was developed by me independently of any disclosures to me made by the OIG, Board, FOMC, Federal Reserve Banks, or CFPB. Except for information I receive that is not Confidential Information, I will treat all information I receive from the OIG, Board, FOMC, Federal Reserve Banks, or CFPB as Confidential Information, regardless of the manner or form in which the information is transmitted or accessible. In addition, I will also treat the advice, deliverables, products, outputs, or similar items I provide or produce while working with the OIG ("*Product Information*") as Confidential Information until such time as the OIG informs me in writing that such Product Information is public.

Thus, I agree to the following terms:

1. I will keep in confidence all Confidential Information that may be acquired in connection with or as a result of my responsibilities. I will not, at any time, either during or after my work with the OIG, make public or otherwise communicate or disclose Confidential Information to anyone other than authorized personnel of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB, without the OIG's prior written consent. (The OIG will coordinate and obtain the necessary approval(s) from the Board, the FOMC, the Federal Reserve Banks, or the CFPB, as applicable.)

2. I will use Confidential Information solely in connection with my responsibilities in working for the OIG. I will not directly or indirectly use Confidential Information for my private gain or for the private gain of another person or entity at any time, either during or after termination of my work with the OIG.

3. I will inform the OIG of any external requests or demands for disclosure of Confidential Information, and I will refer all such demands and requests for disclosures, including but not limited to subpoenas, to the OIG.

4. Should a question arise as to whether particular information is Confidential Information, I will immediately contact the OIG and seek a determination as to the information's status. Until a determination has been made by the OIG (after coordination with the Board, FOMC, Federal Reserve Banks, or CFPB, as applicable), I shall treat it as Confidential Information in accordance with this NDA.

5. At all times, including during and after my work with the OIG, I will take all necessary steps to protect Confidential Information subject to this NDA.

6. Upon completion, expiration, or termination of my services, unless I am instructed otherwise by the OIG, I will promptly dispose of all Confidential Information in my possession in whatever manner is approved by the OIG for the disposal of such information, which may include the return of Confidential Information to the OIG.

7. I understand that I am prohibited from releasing any publicity or advertising regarding the work I perform for the OIG and from using the name or insignia of the OIG, Board, FOMC, CFPB, Federal Reserve Banks, or the Federal Reserve System, or any variation or adaptation thereof, for any commercial, advertisement, promotional, or endorsement purposes, unless the OIG and the Board's Chief Operating Officer (or his/her designee) has given prior written consent for such release or use.

8. I agree and acknowledge that the disclosure or use of any Confidential Information in breach of this NDA would cause irreparable harm to the OIG, Board, FOMC, CFPB, or Federal Reserve Banks. Accordingly, in the event of such use or disclosure, I understand that I may be subject to legal or other action, which may include termination of my work with the OIG and referral for criminal prosecution, if appropriate.

9. If I suspect that any Confidential Information to which I am given access is or may have been lost or disclosed without authorization, I will immediately notify the OIG.

I understanding that this NDA, all of its terms and conditions, shall remain in effect following the expiration (b) (6) this NDA is terminated in writing by the OIG.

(b) (6)

08/07/2014
DATE

(b) (6)

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

Statement of Independence on Individual Projects

The Office of Inspector General (OIG) and its staff and contractors must be independent in all matters relating to audit, inspection, and evaluation work. OIG employees and contractors who are engaged in audits, inspections, or evaluations are to comply with the OIG policy AE-001, *Independence,* and conduct themselves in a manner consistent with the Board of Governors of the Federal Reserve System's (Board) and the OIG's core values; the Board's *Principles of Ethical Conduct*; the *Standards of Ethical Conduct for Employees of the Executive Branch*, issued by the U.S. Office of Government Ethics; the generally accepted government auditing standards (GAGAS), issued by the Comptroller General of the United States; *Quality Standards for Inspection and Evaluation*, issued by the Council of the Inspectors General on Integrity and Efficiency; and any other standards applicable to their project. OIG employees and contractors must take precautions to ensure that their conduct is perceived as being independent, professional, and appropriate and are not to become involved in situations that impair independence or give the appearance that impairment to independence exists.

Independence comprises independence of mind and independence in appearance. Independence of mind is the state of mind that permits the performance of an audit without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism. Independence in appearance is the absence of circumstances that would cause a reasonable and informed third party, having knowledge of the relevant information, to reasonably conclude that the integrity, objectivity, or professional skepticism of an audit organization or member of the audit team had been compromised (GAGAS 3.03).

GAGAS establishes the conceptual framework (see GAGAS 3.07–3.26 and appendix II) that OIG employees and contractors must use to identify and evaluate threats to independence given the circumstances of their work. Whether independence is impaired depends on the nature of the threat, whether the threat is of such significance that it would compromise an auditor's professional judgment or create the appearance that the auditor's professional judgment may be compromised, and the specific safeguards applied to eliminate the threat or reduce it to an acceptable level. GAGAS provides broad categories of threats (GAGAS 3.14) and examples of circumstances that create threats to independence (GAGAS A3.02–A3.09) and it describes safeguards that may be effective in certain circumstances (GAGAS 3.16–3.19).

Consistent with GAGAS 3.21, 3.64, and 3.65, auditors use professional judgment in applying the conceptual framework to determine independence in a given situation. When identifying and evaluating threats to independence, OIG employees and contractors must consider the broad

categories of threats to independence and the example safeguards provided in GAGAS, as well as the unique circumstances of the project. In addition to the GAGAS examples, specific situations that threaten independence and must be reported to the project manager or an appropriate official if the project manager is not available include the following:

- financial interest that is direct, or is significant or material though indirect, in the audited entity or program
- seeking employment with the division or program area to be reviewed or under review (including the time period leading up to the submission of a job application)
- preconceived ideas toward individuals, groups, organizations, or objectives of a particular program that could bias the project
- official, professional, personal, financial, or any kind of relationship that might cause an OIG employee or contractor to limit the extent of his or her inquiry, to limit disclosure, or to weaken or slant findings in any way
- external interference or influence that improperly or imprudently limits or modifies the scope of project work

When these or any other apparent or potential threats to independence are identified, the individual must immediately and fully disclose the situation to the project manager. The project manager, in consultation with the applicable Senior OIG Manager and Associate Inspector General, must determine whether identified threats to independence are significant and whether they can be reduced to an acceptable level with the imposition of safeguards. Any disclosed threats to independence and applied safeguards must be documented on this form (GAGAS 3.24). If the disclosed threats to independence are deemed insignificant, the basis for that determination must be documented on this form.

Failure to comply with the OIG's policies and procedures regarding independence may result in adverse or disciplinary action against the individual, up to and including termination, consistent with applicable Board policy.

Instructions

This form, which documents compliance with applicable independence standards, is to be completed at the start of each project by OIG or contractor project team members, as well as any OIG staff members who substantially contribute to the project in accordance with the OIG's *Independence* policy. Generally, the project's start date refers to the date the project is initiated in the audit system. A new form must be completed when circumstances change or when threats to independence arise that impact the individual's independence. In addition, this form must be completed by OIG referencers prior to their involvement in the project. The completed forms are maintained as electronic workpapers in the audit systems.

Certification

I certify that I have read and understand the above, as well as the OIG's *Independence* policy and GAGAS independence standards. With regard to the assigned project, I have evaluated threats to my independence, both independence of mind and in appearance, and attest that (select one):

☒ I have not identified any threats to my independence.

☐ I have identified threats to independence and applied safeguards, as described below.

Describe any threats to independence identified and safeguards applied (attach additional page if necessary).

☐ As a **referencer** for this project, I certify that I have not identified any threats to my independence that would prevent me from objectively performing the independent reference review.

I also agree to reevaluate my independence whenever my assignment is changed or whenever my circumstances change while working on this project. If changes affecting either my independence or my objectivity regarding this project occur subsequent to the completion of this form, I will immediately notify the project manager or an appropriate official if the project manager is not available.

Project name: 2014 Congressional Request on the Board's Personnel Practices

Individual's name: (b) (6)

Date individual started on project: August 4, 2014

Signature: (b) (6) **Date:** 8/6/14

OFFICE OF INSPECTOR GENERAL
BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU
WASHINGTON, DC 20551

NON-DISCLOSURE AGREEMENT

I, (b) (6) _____, understand that, in the course of performing work for the Office of Inspector General (OIG) of the Board of Governors of the Federal Reserve System (Board) and the Consumer Financial Protection Bureau (CFPB), I may come into possession of or obtain knowledge of information of the OIG, the Board, the Federal Open Market Committee (FOMC), the Federal Reserve Banks, or the CFPB that is not public or that has not and is not required by law to be made public, including, for example, information that is designated as restricted, controlled, proprietary, confidential, confidential supervisory, or personnel (collectively, "*Confidential Information*"). Confidential Information shall include, but is not limited to (1) information pertaining to the security arrangements and strategies of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB (including information describing security controls related to information technology infrastructure such as network architecture and specific systems, applications, and databases); (2) economic data; (3) financial, statistical, and personnel data pertaining to the OIG, Board, FOMC, Federal Reserve Banks, CFPB, or other financial institutions; (4) financial, statistical, personnel planning and similar information relating to past, present, or future activities of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB; (5) pre-decisional deliberative information and data; (6) law enforcement privileged information; (7) attorney-client privileged information; (8) personally identifiable information; (9) trade-secret information; and (10) non-public information included in the files of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB.

Confidential Information does not include information that (1) is public; (2) is or becomes publicly available without breach by me of this Non-Disclosure Agreement ("*NDA*"); (3) was rightfully received by me without obligation of confidentiality; or (4) was developed by me independently of any disclosures to me made by the OIG, Board, FOMC, Federal Reserve Banks, or CFPB. Except for information I receive that is not Confidential Information, I will treat all information I receive from the OIG, Board, FOMC, Federal Reserve Banks, or CFPB as Confidential Information, regardless of the manner or form in which the information is transmitted or accessible. In addition, I will also treat the advice, deliverables, products, outputs, or similar items I provide or produce while working with the OIG ("*Product Information*") as Confidential Information until such time as the OIG informs me in writing that such Product Information is public.

Thus, I agree to the following terms:

1. I will keep in confidence all Confidential Information that may be acquired in connection with or as a result of my responsibilities. I will not, at any time, either during or after my work with the OIG, make public or otherwise communicate or disclose Confidential Information to anyone other than authorized personnel of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB, without the OIG's prior written consent. (The OIG will coordinate and obtain the necessary approval(s) from the Board, the FOMC, the Federal Reserve Banks, or the CFPB, as applicable.)

2. I will use Confidential Information solely in connection with my responsibilities in working for the OIG. I will not directly or indirectly use Confidential Information for my private gain or for the private gain of another person or entity at any time, either during or after termination of my work with the OIG.

3. I will inform the OIG of any external requests or demands for disclosure of Confidential Information, and I will refer all such demands and requests for disclosures, including but not limited to subpoenas, to the OIG.

4. Should a question arise as to whether particular information is Confidential Information, I will immediately contact the OIG and seek a determination as to the information's status. Until a determination has been made by the OIG (after coordination with the Board, FOMC, Federal Reserve Banks, or CFPB, as applicable), I shall treat it as Confidential Information in accordance with this NDA.

5. At all times, including during and after my work with the OIG, I will take all necessary steps to protect Confidential Information subject to this NDA.

6. Upon completion, expiration, or termination of my services, unless I am instructed otherwise by the OIG, I will promptly dispose of all Confidential Information in my possession in whatever manner is approved by the OIG for the disposal of such information, which may include the return of Confidential Information to the OIG.

7. I understand that I am prohibited from releasing any publicity or advertising regarding the work I perform for the OIG and from using the name or insignia of the OIG, Board, FOMC, CFPB, Federal Reserve Banks, or the Federal Reserve System, or any variation or adaptation thereof, for any commercial, advertisement, promotional, or endorsement purposes, unless the OIG and the Board's Chief Operating Officer (or his/her designee) has given prior written consent for such release or use.

8. I agree and acknowledge that the disclosure or use of any Confidential Information in breach of this NDA would cause irreparable harm to the OIG, Board, FOMC, CFPB, or Federal Reserve Banks. Accordingly, in the event of such use or disclosure, I understand that I may be subject to legal or other action, which may include termination of my work with the OIG and referral for criminal prosecution, if appropriate.

9. If I suspect that any Confidential Information to which I am given access is or may have been lost or disclosed without authorization, I will immediately notify the OIG.

I understanding that this NDA, all of its terms and conditions, shall remain in effect following the expiration or termination of my work with the OIG until this NDA is terminated in writing by the OIG.

(b) (6)

SIGNATURE

8/6/14
DATE

(b) (6)

Printed Name

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

Statement of Independence on Individual Projects

The Office of Inspector General (OIG) and its staff and contractors must be independent in all matters relating to audit, inspection, and evaluation work. OIG employees and contractors who are engaged in audits, inspections, or evaluations are to comply with the OIG policy AE-001, *Independence*, and conduct themselves in a manner consistent with the Board of Governors of the Federal Reserve System's (Board) and the OIG's core values; the Board's *Principles of Ethical Conduct*; the *Standards of Ethical Conduct for Employees of the Executive Branch*, issued by the U.S. Office of Government Ethics; the generally accepted government auditing standards (GAGAS), issued by the Comptroller General of the United States; *Quality Standards for Inspection and Evaluation*, issued by the Council of the Inspectors General on Integrity and Efficiency; and any other standards applicable to their project. OIG employees and contractors must take precautions to ensure that their conduct is perceived as being independent, professional, and appropriate and are not to become involved in situations that impair independence or give the appearance that impairment to independence exists.

Independence comprises independence of mind and independence in appearance. Independence of mind is the state of mind that permits the performance of an audit without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism. Independence in appearance is the absence of circumstances that would cause a reasonable and informed third party, having knowledge of the relevant information, to reasonably conclude that the integrity, objectivity, or professional skepticism of an audit organization or member of the audit team had been compromised (GAGAS 3.03).

GAGAS establishes the conceptual framework (see GAGAS 3.07–3.26 and appendix II) that OIG employees and contractors must use to identify and evaluate threats to independence given the circumstances of their work. Whether independence is impaired depends on the nature of the threat, whether the threat is of such significance that it would compromise an auditor's professional judgment or create the appearance that the auditor's professional judgment may be compromised, and the specific safeguards applied to eliminate the threat or reduce it to an acceptable level. GAGAS provides broad categories of threats (GAGAS 3.14) and examples of circumstances that create threats to independence (GAGAS A3.02–A3.09) and it describes safeguards that may be effective in certain circumstances (GAGAS 3.16–3.19).

Consistent with GAGAS 3.21, 3.64, and 3.65, auditors use professional judgment in applying the conceptual framework to determine independence in a given situation. When identifying and evaluating threats to independence, OIG employees and contractors must consider the broad

categories of threats to independence and the example safeguards provided in GAGAS, as well as the unique circumstances of the project. In addition to the GAGAS examples, specific situations that threaten independence and must be reported to the project manager or an appropriate official if the project manager is not available include the following:

- financial interest that is direct, or is significant or material though indirect, in the audited entity or program
- seeking employment with the division or program area to be reviewed or under review (including the time period leading up to the submission of a job application)
- preconceived ideas toward individuals, groups, organizations, or objectives of a particular program that could bias the project
- official, professional, personal, financial, or any kind of relationship that might cause an OIG employee or contractor to limit the extent of his or her inquiry, to limit disclosure, or to weaken or slant findings in any way
- external interference or influence that improperly or imprudently limits or modifies the scope of project work

When these or any other apparent or potential threats to independence are identified, the individual must immediately and fully disclose the situation to the project manager. The project manager, in consultation with the applicable Senior OIG Manager and Associate Inspector General, must determine whether identified threats to independence are significant and whether they can be reduced to an acceptable level with the imposition of safeguards. Any disclosed threats to independence and applied safeguards must be documented on this form (GAGAS 3.24). If the disclosed threats to independence are deemed insignificant, the basis for that determination must be documented on this form.

Failure to comply with the OIG's policies and procedures regarding independence may result in adverse or disciplinary action against the individual, up to and including termination, consistent with applicable Board policy.

Instructions

This form, which documents compliance with applicable independence standards, is to be completed at the start of each project by OIG or contractor project team members, as well as any OIG staff members who substantially contribute to the project in accordance with the OIG's *Independence* policy. Generally, the project's start date refers to the date the project is initiated in the audit system. A new form must be completed when circumstances change or when threats to independence arise that impact the individual's independence. In addition, this form must be completed by OIG referencers prior to their involvement in the project. The completed forms are maintained as electronic workpapers in the audit systems.

Certification

I certify that I have read and understand the above, as well as the OIG's *Independence* policy and GAGAS independence standards. With regard to the assigned project, I have evaluated threats to my independence, both independence of mind and in appearance, and attest that (select one):

☑ I have not identified any threats to my independence.

☐ I have identified threats to independence and applied safeguards, as described below.

Describe any threats to independence identified and safeguards applied (attach additional page if necessary).

☐ As a **referencer** for this project, I certify that I have not identified any threats to my independence that would prevent me from objectively performing the independent reference review.

I also agree to reevaluate my independence whenever my assignment is changed or whenever my circumstances change while working on this project. If changes affecting either my independence or my objectivity regarding this project occur subsequent to the completion of this form, I will immediately notify the project manager or an appropriate official if the project manager is not available.

Project name: 2014 Congressional Request on the Board's Personnel Practices

Individual's name: (b) (6)

Date individual started on project: 8/4/14

Signature: (b) (6) **Date:** 8/5/14

OFFICE OF INSPECTOR GENERAL
BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU
WASHINGTON, DC 20551

NON-DISCLOSURE AGREEMENT

I, (b) (6) _____, understand that, in the course of performing work for the Office of Inspector General (OIG) of the Board of Governors of the Federal Reserve System (Board) and the Consumer Financial Protection Bureau (CFPB), I may come into possession of or obtain knowledge of information of the OIG, the Board, the Federal Open Market Committee (FOMC), the Federal Reserve Banks, or the CFPB that is not public or that has not and is not required by law to be made public, including, for example, information that is designated as restricted, controlled, proprietary, confidential, confidential supervisory, or personnel (collectively, "*Confidential Information*"). Confidential Information shall include, but is not limited to (1) information pertaining to the security arrangements and strategies of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB (including information describing security controls related to information technology infrastructure such as network architecture and specific systems, applications, and databases); (2) economic data; (3) financial, statistical, and personnel data pertaining to the OIG, Board, FOMC, Federal Reserve Banks, CFPB, or other financial institutions; (4) financial, statistical, personnel planning and similar information relating to past, present, or future activities of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB; (5) pre-decisional deliberative information and data; (6) law enforcement privileged information; (7) attorney-client privileged information; (8) personally identifiable information; (9) trade-secret information; and (10) non-public information included in the files of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB.

Confidential Information does not include information that (1) is public; (2) is or becomes publicly available without breach by me of this Non-Disclosure Agreement ("*NDA*"); (3) was rightfully received by me without obligation of confidentiality; or (4) was developed by me independently of any disclosures to me made by the OIG, Board, FOMC, Federal Reserve Banks, or CFPB. Except for information I receive that is not Confidential Information, I will treat all information I receive from the OIG, Board, FOMC, Federal Reserve Banks, or CFPB as Confidential Information, regardless of the manner or form in which the information is transmitted or accessible. In addition, I will also treat the advice, deliverables, products, outputs, or similar items I provide or produce while working with the OIG ("*Product Information*") as Confidential Information until such time as the OIG informs me in writing that such Product Information is public.

Thus, I agree to the following terms:

1. I will keep in confidence all Confidential Information that may be acquired in connection with or as a result of my responsibilities. I will not, at any time, either during or after my work with the OIG, make public or otherwise communicate or disclose Confidential Information to anyone other than authorized personnel of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB, without the OIG's prior written consent. (The OIG will coordinate and obtain the necessary approval(s) from the Board, the FOMC, the Federal Reserve Banks, or the CFPB, as applicable.)

2. I will use Confidential Information solely in connection with my responsibilities in working for the OIG. I will not directly or indirectly use Confidential Information for my private gain or for the private gain of another person or entity at any time, either during or after termination of my work with the OIG.

3. I will inform the OIG of any external requests or demands for disclosure of Confidential Information, and I will refer all such demands and requests for disclosures, including but not limited to subpoenas, to the OIG.

4. Should a question arise as to whether particular information is Confidential Information, I will immediately contact the OIG and seek a determination as to the information's status. Until a determination has been made by the OIG (after coordination with the Board, FOMC, Federal Reserve Banks, or CFPB, as applicable), I shall treat it as Confidential Information in accordance with this NDA.

5. At all times, including during and after my work with the OIG, I will take all necessary steps to protect Confidential Information subject to this NDA.

6. Upon completion, expiration, or termination of my services, unless I am instructed otherwise by the OIG, I will promptly dispose of all Confidential Information in my possession in whatever manner is approved by the OIG for the disposal of such information, which may include the return of Confidential Information to the OIG.

7. I understand that I am prohibited from releasing any publicity or advertising regarding the work I perform for the OIG and from using the name or insignia of the OIG, Board, FOMC, CFPB, Federal Reserve Banks, or the Federal Reserve System, or any variation or adaptation thereof, for any commercial, advertisement, promotional, or endorsement purposes, unless the OIG and the Board's Chief Operating Officer (or his/her designee) has given prior written consent for such release or use.

8. I agree and acknowledge that the disclosure or use of any Confidential Information in breach of this NDA would cause irreparable harm to the OIG, Board, FOMC, CFPB, or Federal Reserve Banks. Accordingly, in the event of such use or disclosure, I understand that I may be subject to legal or other action, which may include termination of my work with the OIG and referral for criminal prosecution, if appropriate.

9. If I suspect that any Confidential Information to which I am given access is or may have been lost or disclosed without authorization, I will immediately notify the OIG.

I understanding that this NDA, all of its terms and conditions, shall remain in effect following the expiration or termination of my work with the OIG until this NDA is terminated in writing by the OIG.

(b) (6)

8/5/14
DATE

(b) (6)

Printed Name

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

Statement of Independence on Individual Projects

The Office of Inspector General (OIG) and its staff and contractors must be independent in all matters relating to audit, inspection, and evaluation work. OIG employees and contractors who are engaged in audits, inspections, or evaluations are to comply with the OIG policy AE-001, *Independence,* and conduct themselves in a manner consistent with the Board of Governors of the Federal Reserve System's (Board) and the OIG's core values; the Board's *Principles of Ethical Conduct*; the *Standards of Ethical Conduct for Employees of the Executive Branch,* issued by the U.S. Office of Government Ethics; the generally accepted government auditing standards (GAGAS), issued by the Comptroller General of the United States; *Quality Standards for Inspection and Evaluation*, issued by the Council of the Inspectors General on Integrity and Efficiency; and any other standards applicable to their project. OIG employees and contractors must take precautions to ensure that their conduct is perceived as being independent, professional, and appropriate and are not to become involved in situations that impair independence or give the appearance that impairment to independence exists.

Independence comprises independence of mind and independence in appearance. Independence of mind is the state of mind that permits the performance of an audit without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism. Independence in appearance is the absence of circumstances that would cause a reasonable and informed third party, having knowledge of the relevant information, to reasonably conclude that the integrity, objectivity, or professional skepticism of an audit organization or member of the audit team had been compromised (GAGAS 3.03).

GAGAS establishes the conceptual framework (see GAGAS 3.07–3.26 and appendix II) that OIG employees and contractors must use to identify and evaluate threats to independence given the circumstances of their work. Whether independence is impaired depends on the nature of the threat, whether the threat is of such significance that it would compromise an auditor's professional judgment or create the appearance that the auditor's professional judgment may be compromised, and the specific safeguards applied to eliminate the threat or reduce it to an acceptable level. GAGAS provides broad categories of threats (GAGAS 3.14) and examples of circumstances that create threats to independence (GAGAS A3.02–A3.09) and it describes safeguards that may be effective in certain circumstances (GAGAS 3.16–3.19).

Consistent with GAGAS 3.21, 3.64, and 3.65, auditors use professional judgment in applying the conceptual framework to determine independence in a given situation. When identifying and evaluating threats to independence, OIG employees and contractors must consider the broad

categories of threats to independence and the example safeguards provided in GAGAS, as well as the unique circumstances of the project. In addition to the GAGAS examples, specific situations that threaten independence and must be reported to the project manager or an appropriate official if the project manager is not available include the following:

- financial interest that is direct, or is significant or material though indirect, in the audited entity or program
- seeking employment with the division or program area to be reviewed or under review (including the time period leading up to the submission of a job application)
- preconceived ideas toward individuals, groups, organizations, or objectives of a particular program that could bias the project
- official, professional, personal, financial, or any kind of relationship that might cause an OIG employee or contractor to limit the extent of his or her inquiry, to limit disclosure, or to weaken or slant findings in any way
- external interference or influence that improperly or imprudently limits or modifies the scope of project work

When these or any other apparent or potential threats to independence are identified, the individual must immediately and fully disclose the situation to the project manager. The project manager, in consultation with the applicable Senior OIG Manager and Associate Inspector General, must determine whether identified threats to independence are significant and whether they can be reduced to an acceptable level with the imposition of safeguards. Any disclosed threats to independence and applied safeguards must be documented on this form (GAGAS 3.24). If the disclosed threats to independence are deemed insignificant, the basis for that determination must be documented on this form.

Failure to comply with the OIG's policies and procedures regarding independence may result in adverse or disciplinary action against the individual, up to and including termination, consistent with applicable Board policy.

Instructions

This form, which documents compliance with applicable independence standards, is to be completed at the start of each project by OIG or contractor project team members, as well as any OIG staff members who substantially contribute to the project in accordance with the OIG's *Independence* policy. Generally, the project's start date refers to the date the project is initiated in the audit system. A new form must be completed when circumstances change or when threats to independence arise that impact the individual's independence. In addition, this form must be completed by OIG referencers prior to their involvement in the project. The completed forms are maintained as electronic workpapers in the audit systems.

Certification

I certify that I have read and understand the above, as well as the OIG's *Independence* policy and GAGAS independence standards. With regard to the assigned project, I have evaluated threats to my independence, both independence of mind and in appearance, and attest that (select one):

☑ I have not identified any threats to my independence.

☐ I have identified threats to independence and applied safeguards, as described below.

Describe any threats to independence identified and safeguards applied (attach additional page if necessary).

☐ As a **referencer** for this project, I certify that I have not identified any threats to my independence that would prevent me from objectively performing the independent reference review.

I also agree to reevaluate my independence whenever my assignment is changed or whenever my circumstances change while working on this project. If changes affecting either my independence or my objectivity regarding this project occur subsequent to the completion of this form, I will immediately notify the project manager or an appropriate official if the project manager is not available.

Project name: 2014 Congressional Request on the Board's Personnel Practices

Individual's name: (b) (6)

Date individual started on project: 8/4/14

Signatur (b) (6) **Date:** 8/6/14

OFFICE OF INSPECTOR GENERAL
BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU
WASHINGTON, DC 20551

NON-DISCLOSURE AGREEMENT

I, (b) (6) _____, understand that, in the course of performing work for the Office of Inspector General (OIG) of the Board of Governors of the Federal Reserve System (Board) and the Consumer Financial Protection Bureau (CFPB), I may come into possession of or obtain knowledge of information of the OIG, the Board, the Federal Open Market Committee (FOMC), the Federal Reserve Banks, or the CFPB that is not public or that has not and is not required by law to be made public, including, for example, information that is designated as restricted, controlled, proprietary, confidential, confidential supervisory, or personnel (collectively, "*Confidential Information*"). Confidential Information shall include, but is not limited to (1) information pertaining to the security arrangements and strategies of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB (including information describing security controls related to information technology infrastructure such as network architecture and specific systems, applications, and databases); (2) economic data; (3) financial, statistical, and personnel data pertaining to the OIG, Board, FOMC, Federal Reserve Banks, CFPB, or other financial institutions; (4) financial, statistical, personnel planning and similar information relating to past, present, or future activities of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB; (5) pre-decisional deliberative information and data; (6) law enforcement privileged information; (7) attorney-client privileged information; (8) personally identifiable information; (9) trade-secret information; and (10) non-public information included in the files of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB.

Confidential Information does not include information that (1) is public; (2) is or becomes publicly available without breach by me of this Non-Disclosure Agreement ("*NDA*"); (3) was rightfully received by me without obligation of confidentiality; or (4) was developed by me independently of any disclosures to me made by the OIG, Board, FOMC, Federal Reserve Banks, or CFPB. Except for information I receive that is not Confidential Information, I will treat all information I receive from the OIG, Board, FOMC, Federal Reserve Banks, or CFPB as Confidential Information, regardless of the manner or form in which the information is transmitted or accessible. In addition, I will also treat the advice, deliverables, products, outputs, or similar items I provide or produce while working with the OIG ("*Product Information*") as Confidential Information until such time as the OIG informs me in writing that such Product Information is public.

Thus, I agree to the following terms:

1. I will keep in confidence all Confidential Information that may be acquired in connection with or as a result of my responsibilities. I will not, at any time, either during or after my work with the OIG, make public or otherwise communicate or disclose Confidential Information to anyone other than authorized personnel of the OIG, Board, FOMC, Federal Reserve Banks, or CFPB, without the OIG's prior written consent. (The OIG will coordinate and obtain the necessary approval(s) from the Board, the FOMC, the Federal Reserve Banks, or the CFPB, as applicable.)

2. I will use Confidential Information solely in connection with my responsibilities in working for the OIG. I will not directly or indirectly use Confidential Information for my private gain or for the private gain of another person or entity at any time, either during or after termination of my work with the OIG.

3. I will inform the OIG of any external requests or demands for disclosure of Confidential Information, and I will refer all such demands and requests for disclosures, including but not limited to subpoenas, to the OIG.

4. Should a question arise as to whether particular information is Confidential Information, I will immediately contact the OIG and seek a determination as to the information's status. Until a determination has been made by the OIG (after coordination with the Board, FOMC, Federal Reserve Banks, or CFPB, as applicable), I shall treat it as Confidential Information in accordance with this NDA.

5. At all times, including during and after my work with the OIG, I will take all necessary steps to protect Confidential Information subject to this NDA.

6. Upon completion, expiration, or termination of my services, unless I am instructed otherwise by the OIG, I will promptly dispose of all Confidential Information in my possession in whatever manner is approved by the OIG for the disposal of such information, which may include the return of Confidential Information to the OIG.

7. I understand that I am prohibited from releasing any publicity or advertising regarding the work I perform for the OIG and from using the name or insignia of the OIG, Board, FOMC, CFPB, Federal Reserve Banks, or the Federal Reserve System, or any variation or adaptation thereof, for any commercial, advertisement, promotional, or endorsement purposes, unless the OIG and the Board's Chief Operating Officer (or his/her designee) has given prior written consent for such release or use.

8. I agree and acknowledge that the disclosure or use of any Confidential Information in breach of this NDA would cause irreparable harm to the OIG, Board, FOMC, CFPB, or Federal Reserve Banks. Accordingly, in the event of such use or disclosure, I understand that I may be subject to legal or other action, which may include termination of my work with the OIG and referral for criminal prosecution, if appropriate.

9. If I suspect that any Confidential Information to which I am given access is or may have been lost or disclosed without authorization, I will immediately notify the OIG.

I understanding that this NDA, all of its terms and conditions, shall remain in effect following the expiration or termination of my work with the OIG until this NDA is terminated in writing by the OIG.

(b) (6)

SIGNATURE

8/6/14

DATE

(b) (6)

Printed Name

From: Laura Polly
To: Sean Newman
Subject: FW: Final Audit Report on Board Diversity and Inclusion Efforts [FRSONLY]
Date: Wednesday, April 01, 2015 3:36:42 PM
Attachments: board-diversity-inclusion-mar2015.pdf

INTERNAL FR

Thanks,
Laura

Laura Polly | Supervisory Writer-Editor
Office of Inspector General
Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-6118 | c: 202-380-7687 | f: 202-973-5044 | laura.a.polly@frb.gov
OIG Hotline: 800-827-3340 | oighotline@frb.gov

http://oig.federalreserve.gov | http://oig.consumerfinance.gov

---

From: Melissa Heist
Sent: Tuesday, March 31, 2015 2:42 PM
To: Donald Hammond; Steven Kamin; Thomas Laubach; Nellie Liang; David Wilcox
Cc: Michell Clark; David Harmon; Sheila Clark; Lil Shewmaker; Tony Ogden; Tim Rogers; Mark Bialek; Scott Alvarez; Bill Mitchell
Subject: Final Audit Report on Board Diversity and Inclusion Efforts [FRSONLY]

INTERNAL FR

Good afternoon,

Attached is our final report titled *The Board Can Enhance Its Diversity and Inclusion Efforts*, OIG Report No. 2015-MO-B-006. It includes recommendations designed to improve the monitoring and promotion of diversity and inclusion at the Board, as well as strengthen related controls.

We will be providing the report to the requesters and the Chairman of the House Financial Services Committee later today and plan to post the report on our public website on April 3, 2015.

We appreciate the cooperation that we received during the audit. If you have any questions or wish to discuss this report further, please contact me at 202-973-5024, or Timothy Rogers, Senior OIG Manager for Management and Operations at 202-973-5042.

Melissa

Melissa M. Heist | Associate Inspector General for Audits and Evaluations
Office of Inspector General

Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-5024 | c: 202-689-9189 | f: 202-973-5044 | melissa.m.heist@frb.gov
OIG Hotline: 800-827-3340 | oighotline@frb.gov

www.federalreserve.gov/oig

(b) (5)

From:	Melissa Heist
To:	Donald Hammond; Steven Kamin; Thomas Laubach; Nellie Liang; David Wilcox
Cc:	Michell Clark; David Harmon; Sheila Clark; Lil Shewmaker; Tony Ogden; Tim Rogers; Mark Bialek; Scott Alvarez; Bill Mitchell
Subject:	Final Audit Report on Board Diversity and Inclusion Efforts [FRSONLY]
Date:	Tuesday, March 31, 2015 2:41:51 PM
Attachments:	board-diversity-inclusion-mar2015.pdf

INTERNAL FR

Good afternoon,

Attached is our final report titled *The Board Can Enhance Its Diversity and Inclusion Efforts*, OIG Report No. 2015-MO-B-006. It includes recommendations designed to improve the monitoring and promotion of diversity and inclusion at the Board, as well as strengthen related controls.

We will be providing the report to the requesters and the Chairman of the House Financial Services Committee later today and plan to post the report on our public website on April 3, 2015.

We appreciate the cooperation that we received during the audit. If you have any questions or wish to discuss this report further, please contact me at 202-973-5024, or Timothy Rogers, Senior OIG Manager for Management and Operations at 202-973-5042.

Melissa

Melissa M. Heist | Associate Inspector General for Audits and Evaluations
Office of Inspector General
Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-5024 | c: 202-689-9189 | f: 202-973-5044 | melissa.m.heist@frb.gov
OIG Hotline: 800-827-3340 | oighotline@frb.gov

www.federalreserve.gov/oig

(b) (5)

From:	Tim Rogers
To:	Donald Hammond; Steven Kamin; Thomas Laubach; Nellie Liang; David Wilcox
Cc:	Michell Clark; David Harmon; Sheila Clark; Lil Shewmaker; Tony Ogden; Melissa Heist; Mark Bialek; Anna Saez; Kimberly Perteet
Subject:	OIG Discussion Draft Report - Board Diversity and Inclusion [FRSONLY]
Date:	Wednesday, March 04, 2015 4:35:24 PM
Attachments:	OIG Board Discussion Draft Report Diversity and Inclusion 3_4_2015.pdf

RESTRICTED FR

Restricted-FR

Good afternoon,

We are providing the attached discussion draft report on our audit related to the Board's diversity and inclusion efforts, *The Board Can Enhance its Diversity and Inclusion Efforts,* for your review. Our report is in response to the congressional letter that we received in March 2014 requesting our review of areas within the Board related to diversity and inclusion, including performance management, employee complaint handling, and recruiting and hiring, among others. The report includes recommendations designed to enhance and promote diversity and inclusion, as well as to strengthen related controls. The discussion draft will be used to facilitate our exit conference, to be scheduled for next week. Should you have any questions, please contact Anna Saez, OIG Manager, at 202-973-5027, or me at 202-973-5042.

Because the draft report is still subject to revision, please appropriately safeguard the report to prevent premature disclosure. We appreciate the cooperation we have received from many staff throughout the Board, and look forward to meeting with you to discuss the diversity and inclusion draft report.

Regards,

Tim Rogers

Timothy Rogers | Sr. OIG Manager for Management and Operations
Audits and Evaluations
Office of Inspector General
Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-5042 | c: 202-450-7792 | timothy.p.rogers@frb.gov

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

September 2, 2014

MEMORANDUM

TO: Distribution List

FROM: Timothy Rogers
Senior OIG Manager for Management and Operations
Office of Audits and Evaluations

SUBJECT: The OIG's Audit of Workplace Diversity at the Board: Request for Input on Factors Related to Ensuring Diversity

The Office of Inspector General is conducting an audit in response to a letter from the House Committee on Financial Services. The letter requests that our office review activities related to workplace diversity and inclusion at the Board. Our audit objective is to assess the Board's personnel operations and other efforts to provide for equal employment opportunities, including equal opportunity for minorities and women to obtain senior management positions, and for racial, ethnic, and gender diversity in the workforce. Our announcement memorandum, with the committee's request letter attached, is provided as an attachment to this memorandum.

As part of our review, we are identifying factors that may affect the Board's ability to increase diversity in senior management, as well as understanding the role and involvement of the Office of Minority and Women Inclusion (OMWI) in monitoring the effect of the Board's personnel policies on minorities and women. We have been working with OMWI, the Equal Employment Opportunity (EEO) office, and human resources directly, but we also believe that our audit would be enhanced if we obtained the views of the agency's senior management on the following questions:

(b) (5)

(b) (5)

[redacted]

Because of the limited time we have to respond to the House Committee on Financial Services, our team would like to schedule a meeting in early September to discuss these questions with you or your designee. Should a meeting not be feasible, a conference call or an e-mail with responses to our questions is also suitable. Ideally, we would like your input on the questions above by September 9, 2014. Anna Saez, OIG Manager, is overseeing the project. Should you have any questions, feel free to contact Anna at 202-973-5027 or me at 202-973-5042.

Thank you for your assistance with this effort.

Attachment
cc: Melissa Heist, Associate Inspector General for Audits and Evaluations

Distribution:
Eric Belsky, Director, Division on Consumer and Community Affairs
Michell Clark, Director, Management Division
Robert Frierson, Secretary of the Board, Office of the Secretary
Michael Gibson, Director, Division of Banking Supervision and Regulation
Donald Hammond, Chief Operating Officer, Office of the Chief Operating Officer
William Mitchell, Director and Chief Financial Officer, Division of Financial Management
Sharon Mowry, Director, Division of Information Technology
Michelle Smith, Director, Office of Board Members
Louise Roseman, Director, Division of Reserve Bank Operations and Payment Systems

Attachment

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

April 25, 2014

MEMORANDUM

TO: Donald Hammond
Chief Operating Officer

FROM: Timothy Rogers
Senior OIG Manager for Management and Operations
Office of Audits and Evaluations

SUBJECT: Congressional Request Regarding the Board's Diversity and Inclusion Processes

In response to a recent letter from the House Committee on Financial Services (attachment A), the Office of Inspector General is initiating an audit of the Board of Governors of the Federal Reserve System's (Board) activities related to diversity and inclusion processes. The objective of this audit is to assess the Board's personnel operations and other efforts to provide for equal employment opportunities, including equal opportunity for minorities and women to obtain senior management positions, and for racial, ethnic, and gender diversity in the workforce.

To answer our objective, we plan to

- analyze information related to trend statistics, such as performance management results and promotions for minority and women employees, informal and formal equal employment opportunity complaint statistics, and employee satisfaction survey results

- review relevant Board personnel operations, policies, and procedures, such as those related to performance management, to determine whether adequate controls are established to prevent and detect bias or discrimination

- assess the Board's efforts to respond to complaints, employee satisfaction survey results, or other potential indications of bias and to increase diversity in management

- evaluate the Office of Minority and Women Inclusion's role and involvement in monitoring the impact of the Board's personnel policies on minorities and women, as well as monitoring the agency's efforts to increase diversity in senior management positions

- identify any factors that may impact the Board's ability to increase diversity in senior management positions

Our scope will include personnel activities that took place from January 2011 through December 2013, as well as changes to policies and procedures since December 2013.

We will contact your office shortly to schedule an entrance conference to further discuss our planned work in more detail. Attachment B contains our initial list of documents that we are requesting to assist us in addressing our objective. Please provide the documents at your earliest convenience. If you have any questions concerning this audit, please contact Anna Saez, OIG Manager, at 202-973-5027 or me at 202-973-5042.

Attachments
cc: Michell Clark, Director, Management Division
David Harmon, Chief Human Capital Officer
Sheila Clark, Program Director, Office of Minority and Women Inclusion
William Mitchell, Chief Financial Officer and Director, Division of Financial Management
Orice Williams Brown, U.S. Government Accountability Office
Mark Bialek, Inspector General
J. Anthony Ogden, Deputy Inspector General
Melissa Heist, Associate Inspector General for Audits and Evaluations
Andrew Patchan Jr., Associate Inspector General for Information Technology

Attachment A

JEB HENSARLING, TX, CHAIRMAN

MAXINE WATERS, CA, RANKING MEMBER

United States House of Representatives
Committee on Financial Services
Washington, D.C. 20515

March 24, 2014

Inspector General Mark Bialek
Board of Governors of the Federal Reserve System
Office of Inspector General
20th and C Streets N.W.
Mail Stop 300
Washington, DC 20551

Dear Inspector General Bialek:

We write to request that the Office of the Inspector General (OIG) for the Board of Governors of the Federal Reserve System (FRS) review the agency's internal operations to determine whether any personnel practices have created a discriminatory workplace or otherwise systematically disadvantaged minorities from obtaining senior management positions.

Section 342 of the Dodd-Frank Wall Street Reform and Consumer Protection Act established an Office of Minority and Women Inclusion (OMWI) at most of the federal financial regulatory agencies, responsible for matters relating to diversity in management, employment, and business activities. Despite this statutory mandate, the Government Accountability Office (GAO) concluded in a report released last year that management-level representation of minorities and women among federal financial agencies and Federal Reserve Banks has not changed substantially from 2007 through 2011. In fact, across all federal financial regulators, agency representation of minorities was as low as 6 percent and dropped as low as zero percent at one of the Reserve Banks. In light of these findings and the concerns raised by employee performance evaluations at the Consumer Financial Protection Bureau (CFPB), we believe the OIG should work in cooperation with Federal Reserve System's OMWI Director to assess current personnel practices and make recommendations necessary to ensure full compliance with the law.

The 2013 GAO report, entitled "Trends and Practices in the Financial Industry and Agencies after the Recent Financial Crisis," documented the extremely poor representation of women and minorities in leadership positions within the financial services industry and among federal financial regulators. According to GAO, industry representation of minorities in 2011 was higher in lower-level management positions – approximately 20 percent – as compared to about 11 percent of senior-level manager positions.

While public attention is currently and justifiably focused on the CFPB, the most recent OMWI reports suggest the disparities impeding internal upward mobility for minorities may be endemic throughout all the agencies regulating the financial services industry. According to the Treasury Department's 2013 OMWI report, among its senior executive management, 86 percent are white men, compared to 7 percent Black men, 4 percent Hispanic men, and 3 percent Asian men. Among the agency's GS-15 employees, which serves as a pipeline to senior level management, white men are once again overrepresented at 86 percent, compared to 6 percent Black men, 2 percent Hispanic men, and 6 percent Asian men.

At the Federal Reserve, white men represent 50 percent of executive senior level managers, compared to just 28.7 percent represented by white women. Along ethnic categories, black and Hispanic men represent, respectively, roughly 5 percent and 1 percent of executive senior level managers. Black women represent roughly 6 percent and Hispanic women represent nearly 2 percent of senior managers.

According to the most recent information from the GAO, at the National Credit Union Administration (NCUA), whites represent 88 percent of senior level management positions, compared to 4 percent represented by blacks and 4 percent by Hispanics. At the Office of the Comptroller of the Currency (OCC), whites represent 82 percent of senior level managers, compared to 9 percent black and 5 percent Hispanic. Whites represent 89 percent of senior level management positions at the Securities and Exchange Commission, compared to 2 percent black and 5 percent Hispanic. Minorities appear to fair best at the Federal Housing Finance Agency, where whites represent 76 percent of senior level management positions, compared to 16 percent black and 8 percent Hispanic. However, more comprehensive analysis is still needed from the agency to fully assess the racial and gender employment of minorities in senior positions beyond the GAO's limited information.

Accordingly, we request that the OIG examine any employee complaints, formal or informal, related to personnel practices, workplace policies and the findings from any employee satisfaction surveys, whether conducted by the Federal Reserve System or an outside entity. If the OIG identifies any individuals or groups of individuals who have exhibited discriminatory behaviors or patterns of unfair or unequal treatment, we ask that the OIG provide recommendations about appropriate actions, including remedial training or removal from employment with the agency. Furthermore, we request that the OIG assess the agency's OMWI operations, and ensure corrective actions are taken within the agency with regard to employee compensation, rating systems, retention, and promotion of women and minorities.

Sincerely,

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

September 2, 2014

MEMORANDUM

TO: Scott Alvarez
General Counsel, Legal Division
Board of Governors of the Federal Reserve System

FROM: Timothy Rogers
Senior OIG Manager for Management and Operations
Office of Audits and Evaluations

SUBJECT: The OIG's Audit of Workplace Diversity at the Board: Request for Input on Factors Related to Ensuring Diversity

The Office of Inspector General is conducting an audit in response to a letter from the House Committee on Financial Services. The letter requests that our office review activities related to workplace diversity and inclusion at the Board. Our audit objective is to assess the Board's personnel operations and other efforts to provide for equal employment opportunities, including equal opportunity for minorities and women to obtain senior management positions, and for racial, ethnic, and gender diversity in the workforce. Our announcement memorandum, with the committee's request letter attached, is provided as an attachment to this memorandum.

As part of our review, we are identifying factors that may affect the Board's ability to increase diversity in senior management, as well as understanding the role and involvement of the Office of Minority and Women Inclusion (OMWI) in monitoring the effect of the Board's personnel policies on minorities and women. We have been working with OMWI, the Equal Employment Opportunity (EEO) office, and human resources directly, but we also believe that our audit would be enhanced if we obtained the views of the agency's senior management on the following questions:

(b) (5)

(b) (5)

Because of the limited time we have to respond to the House Committee on Financial Services, our team would like to schedule a meeting in early September to discuss these questions with you or your designee. Should a meeting not be feasible, a conference call or an e-mail response to our questions is also suitable. Ideally, we would like your input on the questions above by September 9, 2014. Anna Saez, OIG Manager, is overseeing the project. Should you have any questions, feel free to contact Anna at 202-973-5027 or me at 202-973-5042.

Thank you for your assistance with this effort.

Attachment
cc: Melissa Heist, Associate Inspector General for Audits and Evaluations

Attachment

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

April 25, 2014

MEMORANDUM

TO: Donald Hammond
Chief Operating Officer

FROM: Timothy Rogers
Senior OIG Manager for Management and Operations
Office of Audits and Evaluations

SUBJECT: Congressional Request Regarding the Board's Diversity and Inclusion Processes

In response to a recent letter from the House Committee on Financial Services (attachment A), the Office of Inspector General is initiating an audit of the Board of Governors of the Federal Reserve System's (Board) activities related to diversity and inclusion processes. The objective of this audit is to assess the Board's personnel operations and other efforts to provide for equal employment opportunities, including equal opportunity for minorities and women to obtain senior management positions, and for racial, ethnic, and gender diversity in the workforce.

To answer our objective, we plan to

- analyze information related to trend statistics, such as performance management results and promotions for minority and women employees, informal and formal equal employment opportunity complaint statistics, and employee satisfaction survey results

- review relevant Board personnel operations, policies, and procedures, such as those related to performance management, to determine whether adequate controls are established to prevent and detect bias or discrimination

- assess the Board's efforts to respond to complaints, employee satisfaction survey results, or other potential indications of bias and to increase diversity in management

- evaluate the Office of Minority and Women Inclusion's role and involvement in monitoring the impact of the Board's personnel policies on minorities and women, as well as monitoring the agency's efforts to increase diversity in senior management positions

- identify any factors that may impact the Board's ability to increase diversity in senior management positions

Our scope will include personnel activities that took place from January 2011 through December 2013, as well as changes to policies and procedures since December 2013.

We will contact your office shortly to schedule an entrance conference to further discuss our planned work in more detail. Attachment B contains our initial list of documents that we are requesting to assist us in addressing our objective. Please provide the documents at your earliest convenience. If you have any questions concerning this audit, please contact Anna Saez, OIG Manager, at 202-973-5027 or me at 202-973-5042.

Attachments
cc: Michell Clark, Director, Management Division
David Harmon, Chief Human Capital Officer
Sheila Clark, Program Director, Office of Minority and Women Inclusion
William Mitchell, Chief Financial Officer and Director, Division of Financial Management
Orice Williams Brown, U.S. Government Accountability Office
Mark Bialek, Inspector General
J. Anthony Ogden, Deputy Inspector General
Melissa Heist, Associate Inspector General for Audits and Evaluations
Andrew Patchan Jr., Associate Inspector General for Information Technology

Attachment A

JEB HENSARLING, TX, CHAIRMAN

MAXINE WATERS, CA, RANKING MEMBER

United States House of Representatives
Committee on Financial Services
Washington, D.C. 20515

March 24, 2014

Inspector General Mark Bialek
Board of Governors of the Federal Reserve System
Office of Inspector General
20th and C Streets N.W.
Mail Stop 300
Washington, DC 20551

Dear Inspector General Bialek:

We write to request that the Office of the Inspector General (OIG) for the Board of Governors of the Federal Reserve System (FRS) review the agency's internal operations to determine whether any personnel practices have created a discriminatory workplace or otherwise systematically disadvantaged minorities from obtaining senior management positions.

Section 342 of the Dodd-Frank Wall Street Reform and Consumer Protection Act established an Office of Minority and Women Inclusion (OMWI) at most of the federal financial regulatory agencies, responsible for matters relating to diversity in management, employment, and business activities. Despite this statutory mandate, the Government Accountability Office (GAO) concluded in a report released last year that management-level representation of minorities and women among federal financial agencies and Federal Reserve Banks has not changed substantially from 2007 through 2011. In fact, across all federal financial regulators, agency representation of minorities was as low as 6 percent and dropped as low as zero percent at one of the Reserve Banks. In light of these findings and the concerns raised by employee performance evaluations at the Consumer Financial Protection Bureau (CFPB), we believe the OIG should work in cooperation with Federal Reserve System's OMWI Director to assess current personnel practices and make recommendations necessary to ensure full compliance with the law.

The 2013 GAO report, entitled "Trends and Practices in the Financial Industry and Agencies after the Recent Financial Crisis," documented the extremely poor representation of women and minorities in leadership positions within the financial services industry and among federal financial regulators. According to GAO, industry representation of minorities in 2011 was higher in lower-level management positions – approximately 20 percent – as compared to about 11 percent of senior-level manager positions.

While public attention is currently and justifiably focused on the CFPB, the most recent OMWI reports suggest the disparities impeding internal upward mobility for minorities may be endemic throughout all the agencies regulating the financial services industry. According to the Treasury Department's 2013 OMWI report, among its senior executive management, 86 percent are white men, compared to 7 percent Black men, 4 percent Hispanic men, and 3 percent Asian men. Among the agency's GS-15 employees, which serves as a pipeline to senior level management, white men are once again overrepresented at 86 percent, compared to 6 percent Black men, 2 percent Hispanic men, and 6 percent Asian men.

At the Federal Reserve, white men represent 50 percent of executive senior level managers, compared to just 28.7 percent represented by white women. Along ethnic categories, black and Hispanic men represent, respectively, roughly 5 percent and 1 percent of executive senior level managers. Black women represent roughly 6 percent and Hispanic women represent nearly 2 percent of senior managers.

According to the most recent information from the GAO, at the National Credit Union Administration (NCUA), whites represent 88 percent of senior level management positions, compared to 4 percent represented by blacks and 4 percent by Hispanics. At the Office of the Comptroller of the Currency (OCC), whites represent 82 percent of senior level managers, compared to 9 percent black and 5 percent Hispanic. Whites represent 89 percent of senior level management positions at the Securities and Exchange Commission, compared to 2 percent black and 5 percent Hispanic. Minorities appear to fair best at the Federal Housing Finance Agency, where whites represent 76 percent of senior level management positions, compared to 16 percent black and 8 percent Hispanic. However, more comprehensive analysis is still needed from the agency to fully assess the racial and gender employment of minorities in senior positions beyond the GAO's limited information.

Accordingly, we request that the OIG examine any employee complaints, formal or informal, related to personnel practices, workplace policies and the findings from any employee satisfaction surveys, whether conducted by the Federal Reserve System or an outside entity. If the OIG identifies any individuals or groups of individuals who have exhibited discriminatory behaviors or patterns of unfair or unequal treatment, we ask that the OIG provide recommendations about appropriate actions, including remedial training or removal from employment with the agency. Furthermore, we request that the OIG assess the agency's OMWI operations, and ensure corrective actions are taken within the agency with regard to employee compensation, rating systems, retention, and promotion of women and minorities.

Sincerely,

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

September 2, 2014

MEMORANDUM

TO: Distribution List

FROM: Timothy Rogers
Senior OIG Manager for Management and Operations
Office of Audits and Evaluations

SUBJECT: The OIG's Audit of Workplace Diversity at the Board: Request for Input on Factors Related to Ensuring Diversity

The Office of Inspector General is conducting an audit in response to a letter from the House Committee on Financial Services. The letter requests that our office review activities related to workplace diversity and inclusion at the Board. Our audit objective is to assess the Board's personnel operations and other efforts to provide for equal employment opportunities, including equal opportunity for minorities and women to obtain senior management positions, and for racial, ethnic, and gender diversity in the workforce. Our announcement memorandum, with the committee's request letter attached, is provided as an attachment to this memorandum.

As part of our review, we are identifying factors that may affect the Board's ability to increase diversity in senior management, as well as understanding the role and involvement of the Office of Minority and Women Inclusion (OMWI) in monitoring the effect of the Board's personnel policies on minorities and women. We have been working with OMWI, the Equal Employment Opportunity (EEO) office, and human resources directly, but we also believe that our audit would be enhanced if we obtained the views of the agency's senior management on the following questions:

(b) (5)

[redacted]

(b) (5)

Because of the limited time we have to respond to the House Committee on Financial Services, our team would like to schedule a meeting in early September to discuss these questions with you or your designee. Should a meeting not be feasible, a conference call or an e-mail response to our questions is also suitable. Ideally, we would like your input on the questions above by September 9, 2014. Anna Saez, OIG Manager, is overseeing the project. Should you have any questions, feel free to contact Anna at 202-973-5027 or me at 202-973-5042.

Thank you for your assistance with this effort.

Attachment
cc: Melissa Heist, Associate Inspector General for Audits and Evaluations

Distribution:
William English, Director, Division of Monetary Affairs
Steven Kamin, Director, Division of International Finance
Nellie Liang, Director, Office of Financial Stability Policy & Research
David Wilcox, Director, Division of Research and Statistics

Attachment

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

April 25, 2014

MEMORANDUM

TO: Donald Hammond
Chief Operating Officer

FROM: Timothy Rogers
Senior OIG Manager for Management and Operations
Office of Audits and Evaluations

SUBJECT: Congressional Request Regarding the Board's Diversity and Inclusion Processes

In response to a recent letter from the House Committee on Financial Services (attachment A), the Office of Inspector General is initiating an audit of the Board of Governors of the Federal Reserve System's (Board) activities related to diversity and inclusion processes. The objective of this audit is to assess the Board's personnel operations and other efforts to provide for equal employment opportunities, including equal opportunity for minorities and women to obtain senior management positions, and for racial, ethnic, and gender diversity in the workforce.

To answer our objective, we plan to

- analyze information related to trend statistics, such as performance management results and promotions for minority and women employees, informal and formal equal employment opportunity complaint statistics, and employee satisfaction survey results

- review relevant Board personnel operations, policies, and procedures, such as those related to performance management, to determine whether adequate controls are established to prevent and detect bias or discrimination

- assess the Board's efforts to respond to complaints, employee satisfaction survey results, or other potential indications of bias and to increase diversity in management

- evaluate the Office of Minority and Women Inclusion's role and involvement in monitoring the impact of the Board's personnel policies on minorities and women, as well as monitoring the agency's efforts to increase diversity in senior management positions

- identify any factors that may impact the Board's ability to increase diversity in senior management positions

Our scope will include personnel activities that took place from January 2011 through December 2013, as well as changes to policies and procedures since December 2013.

We will contact your office shortly to schedule an entrance conference to further discuss our planned work in more detail. Attachment B contains our initial list of documents that we are requesting to assist us in addressing our objective. Please provide the documents at your earliest convenience. If you have any questions concerning this audit, please contact Anna Saez, OIG Manager, at 202-973-5027 or me at 202-973-5042.

Attachments
cc: Michell Clark, Director, Management Division
David Harmon, Chief Human Capital Officer
Sheila Clark, Program Director, Office of Minority and Women Inclusion
William Mitchell, Chief Financial Officer and Director, Division of Financial Management
Orice Williams Brown, U.S. Government Accountability Office
Mark Bialek, Inspector General
J. Anthony Ogden, Deputy Inspector General
Melissa Heist, Associate Inspector General for Audits and Evaluations
Andrew Patchan Jr., Associate Inspector General for Information Technology

Attachment A

JEB HENSARLING, TX, CHAIRMAN

MAXINE WATERS, CA, RANKING MEMBER

United States House of Representatives
Committee on Financial Services
Washington, D.C. 20515

March 24, 2014

Inspector General Mark Bialek
Board of Governors of the Federal Reserve System
Office of Inspector General
20th and C Streets N.W.
Mail Stop 300
Washington, DC 20551

Dear Inspector General Bialek:

We write to request that the Office of the Inspector General (OIG) for the Board of Governors of the Federal Reserve System (FRS) review the agency's internal operations to determine whether any personnel practices have created a discriminatory workplace or otherwise systematically disadvantaged minorities from obtaining senior management positions.

Section 342 of the Dodd-Frank Wall Street Reform and Consumer Protection Act established an Office of Minority and Women Inclusion (OMWI) at most of the federal financial regulatory agencies, responsible for matters relating to diversity in management, employment, and business activities. Despite this statutory mandate, the Government Accountability Office (GAO) concluded in a report released last year that management-level representation of minorities and women among federal financial agencies and Federal Reserve Banks has not changed substantially from 2007 through 2011. In fact, across all federal financial regulators, agency representation of minorities was as low as 6 percent and dropped as low as zero percent at one of the Reserve Banks. In light of these findings and the concerns raised by employee performance evaluations at the Consumer Financial Protection Bureau (CFPB), we believe the OIG should work in cooperation with Federal Reserve System's OMWI Director to assess current personnel practices and make recommendations necessary to ensure full compliance with the law.

The 2013 GAO report, entitled "Trends and Practices in the Financial Industry and Agencies after the Recent Financial Crisis," documented the extremely poor representation of women and minorities in leadership positions within the financial services industry and among federal financial regulators. According to GAO, industry representation of minorities in 2011 was higher in lower-level management positions – approximately 20 percent – as compared to about 11 percent of senior-level manager positions.

While public attention is currently and justifiably focused on the CFPB, the most recent OMWI reports suggest the disparities impeding internal upward mobility for minorities may be endemic throughout all the agencies regulating the financial services industry. According to the Treasury Department's 2013 OMWI report, among its senior executive management, 86 percent are white men, compared to 7 percent Black men, 4 percent Hispanic men, and 3 percent Asian men. Among the agency's GS-15 employees, which serves as a pipeline to senior level management, white men are once again overrepresented at 86 percent, compared to 6 percent Black men, 2 percent Hispanic men, and 6 percent Asian men.

At the Federal Reserve, white men represent 50 percent of executive senior level managers, compared to just 28.7 percent represented by white women. Along ethnic categories, black and Hispanic men represent, respectively, roughly 5 percent and 1 percent of executive senior level managers. Black women represent roughly 6 percent and Hispanic women represent nearly 2 percent of senior managers.

According to the most recent information from the GAO, at the National Credit Union Administration (NCUA), whites represent 88 percent of senior level management positions, compared to 4 percent represented by blacks and 4 percent by Hispanics. At the Office of the Comptroller of the Currency (OCC), whites represent 82 percent of senior level managers, compared to 9 percent black and 5 percent Hispanic. Whites represent 89 percent of senior level management positions at the Securities and Exchange Commission, compared to 2 percent black and 5 percent Hispanic. Minorities appear to fair best at the Federal Housing Finance Agency, where whites represent 76 percent of senior level management positions, compared to 16 percent black and 8 percent Hispanic. However, more comprehensive analysis is still needed from the agency to fully assess the racial and gender employment of minorities in senior positions beyond the GAO's limited information.

Accordingly, we request that the OIG examine any employee complaints, formal or informal, related to personnel practices, workplace policies and the findings from any employee satisfaction surveys, whether conducted by the Federal Reserve System or an outside entity. If the OIG identifies any individuals or groups of individuals who have exhibited discriminatory behaviors or patterns of unfair or unequal treatment, we ask that the OIG provide recommendations about appropriate actions, including remedial training or removal from employment with the agency. Furthermore, we request that the OIG assess the agency's OMWI operations, and ensure corrective actions are taken within the agency with regard to employee compensation, rating systems, retention, and promotion of women and minorities.

Sincerely,

PSSC:D.1 PRG

Purpose: (b) (5)

[redacted]

Source: OIG

From:	Melissa Heist
To:	Tim Rogers; Anna Saez; Kimberly Perteet; Brian Murphy; Sean Newman; Sopeany
Cc:	Matt Simber
Subject:	FW: OIG Draft Report on Board Diversity and Inclusion Efforts [FRSONLY]
Date:	Thursday, March 19, 2015 3:59:10 PM
Attachments:	OIG Draft Report for Official Comment_Board Diversity_03-19-15.pdf

INTERNAL FR

double click attachment to open

Prepared by: Kimberly Perteet, SR Auditor

Thank you so much! I hope you'll now be able to have the really great weekend you all deserve.

Reviewed by: Anna Saez, SR Manager

Melissa

Melissa M. Heist | Associate Inspector General for Audits and Evaluations
Office of Inspector General
Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-5024 | c: 202-689-9189 | f: 202-973-5044 | melissa.m.heist@frb.gov
OIG Hotline: 800-827-3340 | oighotline@frb.gov

www.federalreserve.gov/oig

From: Melissa Heist
Sent: Thursday, March 19, 2015 3:53 PM
To: Donald Hammond; Steven Kamin; Thomas Laubach; Nellie Liang; David Wilcox
Cc: David Harmon; Sheila Clark; Michell Clark; Lil Shewmaker; Scott Alvarez; Tony Ogden; Kit Wheatley
Subject: OIG Draft Report on Board Diversity and Inclusion Efforts [FRSONLY]

INTERNAL FR

Good Afternoon,

We are providing for your comment the attached draft report on our audit of the Board's diversity and inclusion efforts. We greatly appreciate the cooperation and support provided by you and your staff during this audit. The Congressional requestor for this audit has asked that we issue this report by March 31, so we are requesting you provide your written comments by Thursday, March 26, 2015. If you or your staff have any questions, please feel free to contact me or Tim Rogers, Senior OIG Manager, at 202-973-5042.

Thank you,
Melissa

Melissa M. Heist | Associate Inspector General for Audits and Evaluations
Office of Inspector General
Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-5024 | c: 202-689-9189 | f: 202-973-5044 | melissa.m.heist@frb.gov
OIG Hotline: 800-827-3340 | oighotline@frb.gov

www.federalreserve.gov/oig

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

March 12, 2015

MEMORANDUM

TO: Audit of the Board's Diversity and Inclusion Processes Audit File

FROM: Kimberly Perteet

CC: Anna Saez

SUBJECT: OIG's Analysis of the Board's MD 715 Requirements for Barrier Analysis

The MD-715 states that agencies must regularly evaluate their employment practices to identify barriers to equality of opportunity for all individuals. Where such barriers are identified, agencies must take measures to eliminate them. With these steps, agencies will ensure that all persons are provided opportunities to participate in the full range of employment opportunities and achieve to their fullest potential.

We identified in the Board's annual MD-715 reports for 2011-2013, the Board reports its identification of barriers to equal employment opportunity and its plans to eliminate such barriers. See pages 5- 48 ,2011 E.3.58 2012 E.3.59 2013 E.3.60 .
Draft for Official Comment_Part5_Survey_ODI

Brian Murphy

From: Kimberly Perteet
Sent: Wednesday, September 03, 2014 8:20 AM
To: Brian Murphy
Subject: FW: OIG Audit of Workplace Diversity at the Board -FRSONLY-
Attachments: OIG Memo Board Diversity Factors Div 09 02 14.pdf

---

From: Tim Rogers
Sent: Tuesday, September 02, 2014 6:36 PM
To: Eric Belsky; Michell Clark; Bob Frierson; Michael Gibson; Donald Hammond; Bill Mitchell; Sharon Mowry; Michelle Smith; Louise Roseman
Cc: Melissa M. Heist; Anna Saez; Kimberly Perteet
Subject: OIG Audit of Workplace Diversity at the Board -FRSONLY-

Good afternoon,

The Office of Inspector General is conducting an audit in response to a letter from the House Committee on Financial Services. The letter requests that our office review activities related to workplace diversity and inclusion at the Board. As described in the attached memorandum, we are seeking input from the Board's division directors on factors that may affect the Board's ability to increase diversity in senior management, to include the role of the Office of Minority and Women Inclusion. Included in the attached is a copy of our original announcement letter, as well the congressional request. Should you have any questions you may contact Anna Saez, OIG Manager, at 202-973-5027, or me at 202-973-5042. We appreciate your assistance in this effort.

Regards,

Tim Rogers

Timothy Rogers | Sr. OIG Manager for Management and Operations
Audits and Evaluations
Office of Inspector General
Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-5042 | c: 202-450-7792 | timothy.p.rogers@frb.gov

www.federalreserve.gov/oig

Brian Murphy

From: Kimberly Perteet
Sent: Wednesday, September 03, 2014 8:20 AM
To: Brian Murphy
Subject: FW: OIG Audit of Workplace Diversity at the Board -FRSONLY-
Attachments: OIG Memo Board Diversity Factors Legal Div 09 02 14.pdf

---

From: Tim Rogers
Sent: Tuesday, September 02, 2014 6:39 PM
To: Scott Alvarez
Cc: Melissa M. Heist; Anna Saez; Kimberly Perteet
Subject: OIG Audit of Workplace Diversity at the Board -FRSONLY-

Good afternoon Scott,

The Office of Inspector General is conducting an audit in response to a letter from the House Committee on Financial Services. The letter requests that our office review activities related to workplace diversity and inclusion at the Board. As described in the attached memorandum, we are seeking input from the Board's division directors on factors that may affect the Board's ability to increase diversity in senior management, to include the role of the Office of Minority and Women Inclusion. Included in the attached is a copy of our original announcement letter, as well the congressional request. Should you have any questions you may contact Anna Saez, OIG Manager, at 202-973-5027, or me at 202-973-5042. We appreciate your assistance in this effort.

Regards,

Tim Rogers

Timothy Rogers | Sr. OIG Manager for Management and Operations
Audits and Evaluations
Office of Inspector General
Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-5042 | c: 202-450-7792 | timothy.p.rogers@frb.gov

www.federalreserve.gov/oig

Brian Murphy

From: Kimberly Perteet
Sent: Wednesday, September 03, 2014 8:11 AM
To: Brian Murphy
Subject: FW: OIG Audit of Workplace Diversity at the Board -FRSONLY-
Attachments: OIG Memo Board Diversity Res Div 09 02 14.pdf

Please save this correspondence along with the attach for your workpaper (analysis/procedure steps)

From: Tim Rogers
Sent: Tuesday, September 02, 2014 6:31 PM
To: William English; Steven Kamin; Nellie Liang; David Wilcox
Cc: Melissa M. Heist; Anna Saez; Kimberly Perteet
Subject: OIG Audit of Workplace Diversity at the Board -FRSONLY-

Good afternoon,

The Office of Inspector General is conducting an audit in response to a letter from the House Committee on Financial Services. The letter requests that our office review activities related to workplace diversity and inclusion at the Board. As described in the attached memorandum, we are seeking input from the Board's division directors on factors that may affect the Board's ability to increase diversity in senior management, to include the role of the Office of Minority and Women Inclusion. Included in the attached is a copy of our original announcement letter, as well the congressional request. Should you have any questions you may contact Anna Saez, OIG Manager, at 202-973-5027, or me at 202-973-5042. We appreciate your assistance in this effort.

Regards,

Tim Rogers

Timothy Rogers | Sr. OIG Manager for Management and Operations
Audits and Evaluations
Office of Inspector General
Board of Governors of the Federal Reserve System | Consumer Financial Protection Bureau
202-973-5042 | c: 202-450-7792 | timothy.p.rogers@frb.gov

www.federalreserve.gov/oig

The Board Can Enhance Its Diversity and Inclusion Efforts

Profile

General

Code: 2015-MO-B-006

Name: The Board Can Enhance Its Diversity and Inclusion Efforts

Audit Plan: 2014

Entities:

Name	*Breadcrumb*
Federal Reserve Board (FRB)	Organizations > Federal Reserve Board (FRB)

Unit:

Group: Audits & Evaluations

Type: Management & Operations

Location: FRB

Scope: Other

Origin:

Team

Lead: Kimberly Perteet

Manager:

Staff Type:

The Board Can Enhance Its Diversity and Inclusion Efforts

Schedule

(b) (5)

(b) (5)

Actual Start Date: 4/4/2014

Actual End Date:

(b) (5)

(b) (5)

Actual Hours: 0

(b) (5)

(b) (5)

Actual Resource Costs:

(b) (5)

Actual External Costs: $0.00

(b) (5)

Actual Expenses:

The Board Can Enhance Its Diversity and Inclusion Efforts

Risk

Risk:

Total Risk Score: 0

Inherent Risk: 0

Residual Risk: 0

Objective(s)

2014 Congressional Request on the Board’s Personnel Practices in Team Mate

Background

Planning

Scope

General

The Board Can Enhance Its Diversity and Inclusion Efforts

Contact

Primary

Other

Summary

Final Risk:	
Opinion:	
Cost Savings:	$0.00
Cost Avoidance:	$0.00
Rating:	
Summary:	

Tracking

(b) (5)	
Actual Draft Date:	3/19/2015

(b) (5)	
Actual Response Date:	3/19/2015

The Board Can Enhance Its Diversity and Inclusion Efforts

(b) (5)

Actual Issue Date: 3/31/2015

Milestones

Category	(b) (5)	Act. Date	Comments
Blank			
Entrance Meeting		5/12/2014	
Midpoint Meeting		9/3/2014	
Project Design Meeting		5/12/2014	
Message Development Meeting		10/2/2014	
AIG-Approved Draft Report		3/4/2015	
Discussion Draft Report		3/4/2015	
Exit Meeting		3/13/2015	
Formal Draft Report		3/19/2015	
Final Report		3/31/2015	

Custom Properties

Custom Property Name	Value

Procedures

Summary	Detail
A.1.PRG - OIG Team Meetings *Procedure Step:* (b) (5) CR Meetings with Senior Management *Type:* Fieldwork *Assigned To:* *Prepared By:* SMN, 10/8/2014 *Reviewed By:* (None) PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	*Purpose:* Conduct periodic meetings with senior OIG management (i.e., Senior Managers and above) as necessary. (If items critical to the audit, such as termination of the audit prior to completion, deviations from GAGAS, etc. are discussed, they should be documented.) *Criteria:* GAGAS 6.50 and 6.53-6.55 6.50 If an audit is terminated before it is completed and an audit report is not issued, auditors should document the results of the work to the date of termination and why the audit was terminated. Determining whether and how to communicate the reason for terminating the audit to those charged with governance, appropriate officials of the audited entity, the entity contracting for or requesting the audit, and other appropriate officials will depend on the facts and circumstances and, therefore, is a matter of professional judgment. 6.53 Audit supervisors or those designated to supervise auditors must properly supervise audit staff. 6.54 Audit supervision involves providing sufficient guidance and direction to staff assigned to the audit to address the audit objectives and follow applicable requirements, while staying informed about significant problems encountered, reviewing the work performed, and providing effective on-the-job training. 6.55 The nature and extent of the supervision of staff and the review of audit work may vary depending on a number of factors, such as the size of the audit organization, the significance of the work, and the experience of the staff.

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Source: Auditor's Notes Taken During the Meeting *Scope:* The purpose of the meeting was to discuss the project status with senior leadership *Details:* *Record of Work Done:* (b) (5) [redacted]

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted]
	Conclusion: (b) (5) [redacted]

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Notes: *Results 4:*
A.1.PRG - OIG Team Meetings *Procedure Step:* 04/14/14 Meeting with Senior Management and Other OIGs *Type:* Fieldwork *Assigned To:* *Prepared By:* SMN, 7/9/2014 *Reviewed By:* (None) PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:*	*Purpose:* (b) (5) [redacted] *Criteria:* <P style="MARGIN-TOP: 0px; DIRECTION: ltr; MARGIN-BOTTOM: 0px"><SPAN style="FONT-FAMILY: Tahoma; FONT-SIZE: 12pt">GAGAS </SPAN>6.50 and 6.53-6.55 </P> <P style="MARGIN-TOP: 0px; DIRECTION: ltr; MARGIN-BOTTOM: 0px"> </P>

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
Sample Size:	<P style="MARGIN-TOP: 0px; DIRECTION: ltr; MARGIN-BOTTOM: 0px"></SPAN></P> <P></P><SPAN style="FONT-SIZE: 12pt; FONT-WEIGHT: bold"> <P><SPAN style="FONT-FAMILY: Tahoma; FONT-SIZE: 12pt">6.50 </SPAN></SPAN><SPAN style="FONT-FAMILY: Tahoma; FONT-SIZE: 12pt">If an audit is terminated before it is completed and an audit report is not issued, auditors should document the results of the work to the date of termination and why the audit was terminated. Determining whether and how to communicate the reason for terminating the audit to those charged with governance, appropriate officials of the audited entity, the entity contracting for or requesting the audit, and other appropriate officials will d</SPAN><SPAN style="FONT-FAMILY: Tahoma; FONT-SIZE: 12pt">epend on the facts and circumstances and, therefore, is a matter of professional judgment.</P></SPAN></SPAN></SPAN> <P></P> <P></P><SPAN style="FONT-FAMILY: Tahoma; FONT-SIZE: 12pt; FONT-WEIGHT: bold"> <P>6.53 </SPAN><SPAN style="FONT-FAMILY: Tahoma; FONT-SIZE: 12pt">Audit supervisors or those designated to supervise auditors must properly supervise audit staff.</SPAN><SPAN style="FONT-FAMILY: Tahoma; FONT-SIZE: 12pt"> </P></SPAN> <P></P> <P style="MARGIN-TOP: 0px; MARGIN-BOTTOM: 0px"></SPAN></P> <P style="MARGIN-TOP: 0px; MARGIN-BOTTOM: 0px"></SPAN></P> <P></P> <P> <P></P> <P></P><SPAN style="FONT-SIZE: 12pt; FONT-WEIGHT: bold">

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	<P>6.54 </SPAN><SPAN style="FONT-FAMILY: Arial,Arial; FONT-SIZE: 12pt">Audit supervision involves providing sufficient guidance and direction to staff assigned to the audit to address the audit objectives and follow applicable requirements, while staying informed about significant problems encountered, reviewing the work performed, and providing effective on-the-job training.</SPAN></P><SPAN style="FONT-SIZE: 12pt; FONT-WEIGHT: bold"> <P>6.55 </SPAN><SPAN style="FONT-FAMILY: Arial,Arial; FONT-SIZE: 12pt">The nature and extent of the supervision of staff and the review of audit work may vary depending on a number of factors, such as the size of the audit organization, the significance of the work, and the experience of the staff.</SPAN></P> *Source:* </SPAN> <P></P> <P></P><SPAN style="FONT-FAMILY: Microsoft Sans Serif; FONT-SIZE: 8pt"> <P style="MARGIN: 0in 0in 0pt"><SPAN style="FONT-FAMILY: 'Microsoft Sans Serif','sans-serif'; FONT-SIZE: 11pt">Auditor's Notes Taken During the Meeting</SPAN></P></SPAN> *Scope:* The purpose of the meeting was to discuss the project status with senior leadership and other OIGS. *Details:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Record of Work Done: See: 04-14-14 Conference Call Writeup *Conclusion:* For next steps, see: 04-14-14 Conference Call Writeup *Notes:* *Results 4:*
A.1.PRG - OIG Team Meetings *Procedure Step:* (b) (5) *Type:* Fieldwork *Assigned To:* *Prepared By:* SMN, 7/9/2014 *Reviewed By:* (None) **PROPERTIES:** *Location:* *Frequency:* *Category 4:* *User Category:*	*Purpose:* (b) (5) *Criteria:* <P style="MARGIN-TOP: 0px; DIRECTION: ltr; MARGIN-BOTTOM: 0px"><SPAN style="FONT-FAMILY: Tahoma; FONT-SIZE: 12pt">GAGAS 6.53-6.55</SPAN></P><SPAN style="FONT-SIZE: 12pt; FONT-WEIGHT: bold"> <P>6.53 </SPAN><SPAN style="FONT-FAMILY: Arial,Arial; FONT-SIZE: 12pt">Audit supervisors or those designated to supervise auditors must properly supervise audit staff.</SPAN><SPAN style="FONT-FAMILY: Arial,Arial; FONT-SIZE: 10pt">

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
Category 5 *Category 6* SCORECARD: *Rating:* *Sample Size:*	<P style="MARGIN-TOP: 0px; MARGIN-BOTTOM: 0px"></SPAN></P> <P></P> <P style="MARGIN-TOP: 0px; MARGIN-BOTTOM: 0px"></SPAN></P> <P style="MARGIN-TOP: 0px; MARGIN-BOTTOM: 0px"></SPAN></P> <P></P> <P> <P></P> <P></P><SPAN style="FONT-SIZE: 12pt; FONT-WEIGHT: bold"> <P>6.54 </SPAN><SPAN style="FONT-FAMILY: Arial,Arial; FONT-SIZE: 12pt">Audit supervision involves providing sufficient guidance and direction to staff assigned to the audit to address the audit objectives and follow applicable requirements, while staying informed about significant problems encountered, reviewing the work performed, and providing effective on-the-job training.</SPAN></P><SPAN style="FONT-SIZE: 12pt; FONT-WEIGHT: bold"> <P>6.55 </SPAN><SPAN style="FONT-FAMILY: Arial,Arial; FONT-SIZE: 12pt">The nature and extent of the supervision of staff and the review of audit work may vary depending on a number of factors, such as the size of the audit organization, the significance of the work, and the experience of the staff.</SPAN></P> *Source:* Auditor's notes taken during the meeting. *Scope:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Details: *Record of Work Done:* (b) (5) *Notes:* *Results 4:*
A.1.PRG - OIG Team Meetings *Procedure Step:* 09/03/14 Meeting with Federal Financial Regulators *Type:* Fieldwork *Assigned To:* SMN *Prepared By:* SMN, 9/8/2014 *Reviewed By:* (None) **PROPERTIES:** *Location:*	*Purpose:* Conduct periodic meetings with senior OIG management (i.e., Senior Managers and above) as necessary. (If items critical to the audit, such as termination of the audit prior to completion, deviations from GAGAS, etc. are discussed, they should be documented.) The purpose of the meeting was to discuss the ongoing diversity and inclusion audit with the other federal financial regulators. *Criteria:* <P style="MARGIN-TOP: 0px; DIRECTION: ltr; MARGIN-BOTTOM: 0px"><SPAN style="FONT-FAMILY: Tahoma; FONT-

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
Frequency: *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	SIZE: 12pt">GAGAS </SPAN>6.50 and 6.53- 6.55 </P> <P style="MARGIN-TOP: 0px; DIRECTION: ltr; MARGIN- BOTTOM: 0px"> </P> <P style="MARGIN-TOP: 0px; DIRECTION: ltr; MARGIN- BOTTOM: 0px"></SPAN></P> <P></P><SPAN style="FONT-SIZE: 12pt; FONT-WEIGHT: bold"> <P><SPAN style="FONT-FAMILY: Tahoma; FONT-SIZE: 12pt">6.50 </SPAN></SPAN><SPAN style="FONT-FAMILY: Tahoma; FONT-SIZE: 12pt">If an audit is terminated before it is completed and an audit report is not issued, auditors should document the results of the work to the date of termination and why the audit was terminated. Determining whether and how to communicate the reason for terminating the audit to those charged with governance, appropriate officials of the audited entity, the entity contracting for or requesting the audit, and other appropriate officials will d</SPAN><SPAN style="FONT-FAMILY: Tahoma; FONT-SIZE: 12pt">epend on the facts and circumstances and, therefore, is a matter of professional judgment.</P></SPAN></SPAN></SPAN> <P></P> <P></P><SPAN style="FONT-FAMILY: Tahoma; FONT-SIZE: 12pt; FONT-WEIGHT: bold"> <P>6.53 </SPAN><SPAN style="FONT-FAMILY: Tahoma; FONT- SIZE: 12pt">Audit supervisors or those designated to supervise auditors must properly supervise audit staff.</SPAN><SPAN style="FONT-FAMILY: Tahoma; FONT- SIZE: 12pt"> </P></SPAN> <P></P> <P style="MARGIN-TOP: 0px; MARGIN-BOTTOM: 0px"></SPAN></P> <P style="MARGIN-TOP: 0px; MARGIN-BOTTOM: 0px"></SPAN></P> <P></P>

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	<P> <P></P> <P></P><SPAN style="FONT-SIZE: 12pt; FONT-WEIGHT: bold"> <P>6.54 </SPAN><SPAN style="FONT-FAMILY: Arial,Arial; FONT-SIZE: 12pt">Audit supervision involves providing sufficient guidance and direction to staff assigned to the audit to address the audit objectives and follow applicable requirements, while staying informed about significant problems encountered, reviewing the work performed, and providing effective on-the-job training.</SPAN></P><SPAN style="FONT-SIZE: 12pt; FONT-WEIGHT: bold"> <P>6.55 </SPAN><SPAN style="FONT-FAMILY: Arial,Arial; FONT-SIZE: 12pt">The nature and extent of the supervision of staff and the review of audit work may vary depending on a number of factors, such as the size of the audit organization, the significance of the work, and the experience of the staff.</SPAN></P> *Source:* Auditor's Notes Taken During the Meeting Other Agency Participants: FDIC Treasury SEC NCUA FHFA OIG Participants: Melissa Heist, AIG of Audits and Evaluations Tim Rogers, Senior OIG Manager Anna Saez, Project Manager Kim Perteet, Sr. Auditor and Board Project Leader Megan Taylor, Auditor

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Scope: The purpose of the meeting was to discuss the project status with senior leadership and other federal financial regulators. *Details:* *Record of Work Done:* 09-03-14 Interagency Conference Call with Federal Financial Regulators *Conclusion:* *Notes:* *Results 4:*
A.1.PRG - OIG Team Meetings *Procedure Step:* 10/02/14 Message Development Meeting *Type:* Fieldwork *Assigned To:* SMN *Prepared By:* SMN, 3/17/2015 *Reviewed By:* KLP, 3/24/2015 PROPERTIES:	*Purpose:* Conduct a message development meeting with senior OIG management. *Criteria:* Criteria: GAGAS 6.53-6.55 6.53 Audit supervisors or those designated to supervise auditors must properly supervise audit staff. 6.54 Audit supervision involves providing sufficient guidance and direction to staff assigned to the audit to address the audit objectives and follow applicable requirements, while staying informed about significant problems

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
Location: *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	encountered, reviewing the work performed, and providing effective on-the-job training. 6.55 The nature and extent of the supervision of staff and the review of audit work may vary depending on a number of factors, such as the size of the audit organization, the significance of the work, and the experience of the staff. *Source:* Auditor's Notes Taken During the Meeting *Scope:* The purpose of the meeting was to discuss the project status with senior leadership. *Details:* *Record of Work Done:* (b) (5) *Conclusion:* The OIG condiucted its MDM as noted and documented in the record of work completed. *Notes:* *Results 4:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail

The Board Can Enhance Its Diversity and Inclusion Efforts

Profile

General

Code: 2015-MO-B-006

Name: The Board Can Enhance Its Diversity and Inclusion Efforts

Audit Plan: 2014

Entities:

Name	*Breadcrumb*
Federal Reserve Board (FRB)	Organizations > Federal Reserve Board (FRB)

Unit:

Group: Audits & Evaluations

Type: Management & Operations

Location: FRB

Scope: Other

Origin:

Team

Lead: Kimberly Perteet

Manager:

Staff Type:

The Board Can Enhance Its Diversity and Inclusion Efforts

Schedule

(b) (5)

(b) (5)

Actual Start Date: 4/4/2014

Actual End Date:

(b) (5)

Actual Hours: 0

(b) (5)

Actual Resource Costs:

(b) (5)

Actual External Costs: $0.00

(b) (5)

Actual Expenses:

The Board Can Enhance Its Diversity and Inclusion Efforts

Risk

Risk:

Total Risk Score: 0

Inherent Risk: 0

Residual Risk: 0

Objective(s)

2014 Congressional Request on the Board’s Personnel Practices in Team Mate

Background

Planning

Scope

General

The Board Can Enhance Its Diversity and Inclusion Efforts

Contact

Primary

Other

Summary

Final Risk:	
Opinion:	
Cost Savings:	$0.00
Cost Avoidance:	$0.00
Rating:	
Summary:	

Tracking

(b) (5)	
Actual Draft Date:	3/19/2015
(b) (5)	
Actual Response Date:	3/19/2015

The Board Can Enhance Its Diversity and Inclusion Efforts

(b) (5)

Actual Issue Date: 3/31/2015

Milestones

Category	(b) (5)	Act. Date	Comments
Blank			
Entrance Meeting		5/12/2014	
Midpoint Meeting		9/3/2014	
Project Design Meeting		5/12/2014	
Message Development Meeting		10/2/2014	
AIG-Approved Draft Report		3/4/2015	
Discussion Draft Report		3/4/2015	
Exit Meeting		3/13/2015	
Formal Draft Report		3/19/2015	
Final Report		3/31/2015	

Custom Properties

Custom Property Name	Value

Procedures

Summary		Detail
E.3.PRG - Data Analyses		(b) (5)
Procedure Step:	Workforce Demographics - Data Collection	
Type:		
Assigned To:	BPM	*Criteria:*
Prepared By:	SMN, 3/3/2015	N/A - See record of work done for OIG data analyses.
Reviewed By:	KLP, 3/16/2015	*Source:*
		Board total workforce demographic data obtained from the HRASO office point of contact listed below:
PROPERTIES:		
Location:		Jack Martin, Sr. Information Systems Specialist, jack.martin@frb.gov, 202-263-4830
Frequency:		
Category 4:		
User Category:		
Category 5		*Scope:*
Category 6		Collecting Board workforce demographic data for CY11-CY13
SCORECARD:		*Details:*
Rating:		
Sample Size:		(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted] *Conclusion:* The OIG obtained the Board's workforce data from HR analytics. *Notes:* *Results 4:*
E.3.PRG - Data Analyses	*Purpose:* (b) (5) [redacted]

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
Procedure Step:	Workforce Demographics - Data Reliability	(b) (5)
Type:		
Assigned To:	SMN	*Criteria:*
Prepared By:	SMN, 3/12/2015	OIG audit program
Reviewed By:	KLP, 3/18/2015	*Source:*
		Board total workforce demographic data obtained from both the HRASO and OD&I Office points of contact listed below:
PROPERTIES:		
Location:		Jack Martin, Sr. Information Systems Specialist, jack.martin@frb.gov, 202-263-4830
Frequency:		
Category 4:		Johanna Bruce, Diversity and Inclusion Specialist Supervisor, johanna.c.bruce@frb.gov , 202-452-2787
User Category:		
Category 5		
Category 6		*Scope:*
		Data Reliability of Board workforce demographic data for CY11-CY13
SCORECARD:		
Rating:		*Details:*
Sample Size:		(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
	Notes: *Results 4:*
E.3.PRG - Data Analyses	*Purpose:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
Procedure Step:	Workforce Demographics - Data Analyses	(b) (5)
Type:		
Assigned To:	SMN	*Criteria:*
Prepared By:	SMN, 3/16/2015	</SPAN> <P></P> <P></P><SPAN style="FONT-FAMILY: Microsoft Sans Serif; FONT-SIZE: 8pt"> <P style="MARGIN: 0in 0in 0pt"><SPAN style="FONT-FAMILY: 'Arial','sans-serif'; FONT-SIZE: 10pt">N/A - See record of work done for OIG data analyses.</SPAN></P></SPAN>
Reviewed By:	KLP, 3/16/2015	
PROPERTIES:		
Location:		*Source:*
Frequency:		
Category 4:		*Scope:*
User Category:		Board workforce demographic data for FY11-FY13
Category 5		
Category 6		*Details:*
SCORECARD:		(b) (5)
Rating:		
Sample Size:		

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted]
	Conclusion: Data analyses is consistent with the OIG's policies and procedures. *Notes:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Results 4:
E.3.PRG - Data Analyses *Procedure Step:* Hiring - Data Collection *Type:* *Assigned To:* BPM *Prepared By:* SMN, 11/18/2014 *Reviewed By:* KLP, 1/21/2015 **PROPERTIES:** *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* **SCORECARD:** *Rating:* *Sample Size:*	(b) (5) *Criteria:* </SPAN> <P></P> <P></P><SPAN style="FONT-FAMILY: Microsoft Sans Serif; FONT-SIZE: 8pt"> <P style="MARGIN: 0in 0in 0pt"><SPAN style="FONT-FAMILY: 'Arial','sans-serif'; FONT-SIZE: 10pt">N/A - See record of work done for OIG data analyses.</SPAN></P></SPAN> *Source:* Board total new hire data obtained from the HRASO office point of contact listed below: Jack Martin, Sr. Information Systems Specialist, jack.martin@frb.gov, 202-263-4830 *Scope:* Collecting Board new hires data for CY11-CY13 *Details:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) (b) (5) *Conclusion:* This collection is consistent with OIG policies and procedures. *Notes:* *Results 4:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
E.3.PRG - Data Analyses *Procedure Step:* Hiring - Data Reliability *Type:* *Assigned To:* BPM *Prepared By:* SMN, 11/18/2014 *Reviewed By:* KLP, 1/21/2015 PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	(b) (5) *Criteria:* </SPAN> <P></P> <P></P><SPAN style="FONT-FAMILY: Microsoft Sans Serif; FONT-SIZE: 8pt"> <P style="MARGIN: 0in 0in 0pt"><SPAN style="FONT-FAMILY: 'Arial','sans-serif'; FONT-SIZE: 10pt">N/A - See record of work done for OIG data analyses.</SPAN></P></SPAN> *Source:* Board total new hire data obtained from both the HRASO and OD&I Office points of contact listed below: Jack Martin, Sr. Information Systems Specialist, jack.martin@frb.gov, 202-263-4830 Johanna Bruce, Diversity and Inclusion Specialist Supervisor, johanna.c.bruce@frb.gov , 202-452-2787 *Scope:* Data Reliability of Board new hire data for CY11-CY13 *Details:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Conclusion: Data reliability is consistent with OIG policies and procedures. *Notes:* *Results 4:*

E.3.PRG - Data Analyses
 	
Procedure Step: Hiring - Data Analyses
Type:
Assigned To: BPM
Prepared By: SMN, 3/3/2015
Reviewed By: KLP, 3/16/2015
 	
PROPERTIES:
Location:
Frequency:
Category 4:
User Category:
Category 5
Category 6
	Purpose:
	(b) (5)
	
	Criteria:
	`</SPAN>`
	`<P></P>`
	`<P></P><SPAN style="FONT-FAMILY: Microsoft Sans Serif; FONT-SIZE: 8pt">`
	`<P style="MARGIN: 0in 0in 0pt"><SPAN style="FONT-FAMILY: 'Arial','sans-serif'; FONT-SIZE: 10pt">N/A - See record of work done for OIG data analyses.</SPAN></P></SPAN>`
	
	Source:
	
	Scope:
	Board hiring data for FY11-FY13

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
SCORECARD: *Rating:* *Sample Size:*	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted] *Notes:* *Results 4:*

E.3.PRG - Data Analyses
 	
Procedure Step: Performance Management - Data Collection
Type:
Assigned To: BPM
Prepared By: SMN, 3/3/2015
Reviewed By: KLP, 3/16/2015
 	
PROPERTIES:
Location:
Frequency:
Category 4:
User Category:
Category 5
Category 6
	Purpose:
	(b) (5) [redacted]
	
	Criteria:
	`</SPAN>`
	`<P></P>`
	`<P></P><SPAN style="FONT-FAMILY: Microsoft Sans Serif; FONT-SIZE: 8pt">`
	`<P style="MARGIN: 0in 0in 0pt"><SPAN style="FONT-FAMILY: 'Arial','sans-serif'; FONT-SIZE: 10pt">N/A - See record of work done for OIG data analyses.</SPAN></P></SPAN>`
	
	Source:
	
	Scope:
	Board performance management data for FY11-FY13
	
	Details:

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
SCORECARD: *Rating:* *Sample Size:*	(b) (5) *Conclusion:* This collection is consistent with OIG policies and procedures. *Notes:* *Results 4:*
E.3.PRG - Data Analyses *Procedure Step:* Performance Management - Data Reliability	*Purpose:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
Type:		*Criteria:*
Assigned To:	BPM	</SPAN> <P></P> <P></P><SPAN style="FONT-FAMILY: Microsoft Sans Serif; FONT-SIZE: 8pt"> <P style="MARGIN: 0in 0in 0pt"><SPAN style="FONT-FAMILY: 'Arial','sans-serif'; FONT-SIZE: 10pt">N/A - See record of work done for OIG data analyses.</SPAN></P></SPAN>
Prepared By:	SMN, 3/25/2015	
Reviewed By:	KLP, 3/26/2015	
PROPERTIES:		*Source:*
Location:		PMP Data provided by Jack Martin, HRASO Sr Information Systems Specialist, jack.martin@frb.gov, 202-263-4830 OIG Trace and Verification Performed by: Fay Tang, Statistician, 202-872-4947 and Chris Lyons, Senior Auditor, 202-973-7405
Frequency:		
Category 4:		
User Category:		
Category 5		
Category 6		
SCORECARD:		*Scope:*
Rating:		Board performance management data for FY11-FY13
Sample Size:		*Details:*
		Record of Work Done:
		(b) (5) [redacted]

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
	Notes:
	Results 4:
E.3.PRG - Data Analyses	*Purpose:*
Procedure Step: Performance Management - Data Analyses *Type:* *Assigned To:* SMN *Prepared By:* BPM, 3/16/2015 *Reviewed By:* KLP, 3/16/2015	*Criteria:* </SPAN> <P></P> <P></P><SPAN style="FONT-FAMILY: Microsoft Sans Serif; FONT-SIZE: 8pt"> <P style="MARGIN: 0in 0in 0pt"><SPAN style="FONT-FAMILY: 'Arial','sans-serif'; FONT-SIZE: 10pt">N/A - See record of work done for OIG data analyses.</SPAN></P></SPAN>
PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6*	*Source:* *Scope:* Board performance management data for FY11-FY13 *Details:* *Record of Work Done:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
SCORECARD: *Rating:* *Sample Size:*	(b) (5) *Conclusion:* This analysis is consistent with OIG policies and procedures. *Notes:* *Results 4:*
E.3.PRG - Data Analyses	*Purpose:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
Procedure Step:	Promotions - Data Collection	(b) (5)
Type:		
Assigned To:	BPM	
Prepared By:	SMN, 2/4/2015	
Reviewed By:	KLP, 3/16/2015	
PROPERTIES:		
Location:		
Frequency:		
Category 4:		
User Category:		
Category 5		
Category 6		
SCORECARD:		
Rating:		
Sample Size:		

Criteria:

```
</SPAN>
<P></P>
<P></P><SPAN style="FONT-FAMILY: Microsoft Sans Serif;
FONT-SIZE: 8pt">
<P style="MARGIN: 0in 0in 0pt"><SPAN style="FONT-FAMILY:
'Arial','sans-serif'; FONT-SIZE: 10pt">N/A - See record
of work done for OIG data analyses.</SPAN></P></SPAN>
```

Source:

Board total promotions data obtained from the HRASO office point of contact listed below:
Jack Martin, Sr. Information Systems Specialist, jack.martin@frb.gov, 202-263-4830

Scope:

Collecting Board promotions data for CY11-CY13

Details:

(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted]
	Conclusion:
	Notes:
	Results 4:
E.3.PRG - Data Analyses ***Procedure Step:*** Promotions - Data Reliability ***Type:*** ***Assigned To:*** BPM ***Prepared By:*** SMN, 3/12/2015 ***Reviewed By:*** KLP, 3/18/2015	*Purpose:* (b) (5) [redacted] *Criteria:* </SPAN> <P></P> <P></P><SPAN style="FONT-FAMILY: Microsoft Sans Serif; FONT-SIZE: 8pt">

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	<P style="MARGIN: 0in 0in 0pt"><SPAN style="FONT-FAMILY: 'Arial','sans-serif'; FONT-SIZE: 10pt">N/A - See record of work done for OIG data analyses.</SPAN></P></SPAN> *Source:* Board total promotions data obtained from both the HRASO and OD&I Office points of contact listed below: Jack Martin, Sr. Information Systems Specialist, jack.martin@frb.gov, 202-263-4830 Johanna Bruce, Diversity and Inclusion Specialist Supervisor, johanna.c.bruce@frb.gov , 202-452-2787 *Scope:* Data Reliability of Board promotions data for CY11-CY13 *Details:* *Record of Work Done:* Refer to Data Reliability Promotions Data for our full data reliability assessment as it relates to promotions for calendar years 2011 - 2013. (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
	Conclusion: This data reliability assessment is consistent with OIG policies and procedures.

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Notes: *Results 4:*
E.3.PRG - Data Analyses *Procedure Step:* Promotions - Data Analyses *Type:* *Assigned To:* BPM *Prepared By:* SMN, 3/3/2015 *Reviewed By:* KLP, 3/18/2015 **PROPERTIES:** *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* **SCORECARD:** *Rating:*	*Purpose:* (b) (5) *Criteria:* </SPAN> <P></P> <P></P><SPAN style="FONT-FAMILY: Microsoft Sans Serif; FONT-SIZE: 8pt"> <P style="MARGIN: 0in 0in 0pt"><SPAN style="FONT-FAMILY: 'Arial','sans-serif'; FONT-SIZE: 10pt">N/A - See record of work done for OIG data analyses.</SPAN></P></SPAN> *Source:* *Scope:* Board promotions data for FY11-FY13 *Details:* *Record of Work Done:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
Sample Size:	(b) (5)
	Notes: *Results 4:*
E.3.PRG - Data Analyses	*Purpose:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
Procedure Step: Employee Satisfaction Surveys - Data Collection and Analyses	(b) (5) [redacted]
Type:	
Assigned To: BPM	
Prepared By: KLP, 3/3/2015	
Reviewed By: (None)	
PROPERTIES:	*Criteria:*
Location:	</SPAN> <P></P> <P></P><SPAN style="FONT-FAMILY: Microsoft Sans Serif; FONT-SIZE: 8pt"> <P style="MARGIN: 0in 0in 0pt"><SPAN style="FONT-FAMILY: 'Arial','sans-serif'; FONT-SIZE: 10pt">N/A - See record of work done for OIG data analyses.</SPAN></P></SPAN>
Frequency:	*Source:*
Category 4:	
User Category:	*Scope:*
Category 5	Board employee satisfaction survey data for FY11-FY13
Category 6	*Details:*
SCORECARD:	(b) (5) [redacted]
Rating:	
Sample Size:	

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted] *Notes:* *Results 4:*
E.3.PRG - Data Analyses *Procedure Step:* EEO Complaints - Data Collection *Type:* *Assigned To:* BPM *Prepared By:* BPM, 11/6/2014 *Reviewed By:* KLP, 11/14/2014 PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD:	*Purpose:* (b) (5) [redacted] *Criteria:* </SPAN> <P></P> <P></P><SPAN style="FONT-FAMILY: Microsoft Sans Serif; FONT-SIZE: 8pt"> <P style="MARGIN: 0in 0in 0pt"><SPAN style="FONT-FAMILY: 'Arial','sans-serif'; FONT-SIZE: 10pt">N/A - See record of work done for OIG data analyses.</SPAN></P></SPAN> *Source:* Board EEO complaint data obtained from the OD&I Office points of contact listed below: Andre Smith, Senior Diversity and Inclusion Specialist, andre.m.smith@frb.gov , 202-728-5876 Johanna Bruce, Diversity and Inclusion Specialist Supervisor, johanna.c.bruce@frb.gov , 202-452-2787

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
Rating: *Sample Size:*	*Scope:* Collecting Board EEO complaint data for FY 2011-FY 2013 *Details:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted]
	Notes:
	Results 4:
E.3.PRG - Data Analyses	*Purpose:* (b) (5) [redacted]
Procedure Step: EEO Complaints - Data Reliability	
Type:	
Assigned To: BPM	*Criteria:*
Prepared By: BPM, 10/27/2014	</SPAN> <P></P> <P></P><SPAN style="FONT-FAMILY: Microsoft Sans Serif; FONT-SIZE: 8pt"> <P style="MARGIN: 0in 0in 0pt"><SPAN style="FONT-FAMILY: 'Arial','sans-serif'; FONT-SIZE: 10pt">N/A - See record of work done for OIG data analyses.</SPAN></P></SPAN>
Reviewed By: KLP, 3/18/2015	
PROPERTIES:	
Location:	*Source:*
Frequency:	Board EEO complaint data obtained from the OD&I Office points of contact listed below: Andre Smith, Senior Diversity and Inclusion Specialist, andre.m.smith@frb.gov , 202-728-5876 Johanna Bruce, Diversity and Inclusion Specialist Supervisor, johanna.c.bruce@frb.gov , 202-452-2787
Category 4:	
User Category:	
Category 5	
Category 6	

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
SCORECARD: *Rating:* *Sample Size:*	*Scope:* Data Reliability of Board EEO complaint data for FY11-FY13 *Details:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted] *Notes:* *Results 4:*
E.3.PRG - Data Analyses ***Procedure Step:*** EEO Complaints - Data Analyses ***Type:*** ***Assigned To:*** BPM ***Prepared By:*** SMN, 3/26/2015 ***Reviewed By:*** KLP, 3/26/2015	*Purpose:* (b) (5) [redacted] *Criteria:* </SPAN> <P></P> <P></P><SPAN style="FONT-FAMILY: Microsoft Sans Serif; FONT-SIZE: 8pt">

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	<P style="MARGIN: 0in 0in 0pt"><SPAN style="FONT-FAMILY: 'Arial','sans-serif'; FONT-SIZE: 10pt">N/A - See record of work done for OIG data analyses.</SPAN></P></SPAN> *Source:* Board EEO complaint data obtained from the OD&I Office points of contact listed below: Andre Smith, Senior Diversity and Inclusion Specialist, andre.m.smith@frb.gov , 202-728-5876 Johanna Bruce, Diversity and Inclusion Specialist Supervisor, johanna.c.bruce@frb.gov , 202-452-2787 *Scope:* Board EEO complaint data for FY11-FY13 *Details:* *Record of Work Done:* Board EEO Complaints Analysis for Fiscal Years 2011-2013 (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted] *Notes:* *Results 4:*

E.3.PRG - Data Analyses
 	
Procedure Step: Non-EEO Complaints - Data Collection
Type:
Assigned To: BPM
Prepared By: BPM, 11/7/2014
Reviewed By: (None)
 	
PROPERTIES:
Location:
	Purpose:
	(b) (5) [redacted]
	
	Criteria:
	`</SPAN>`
	`<P></P>`
	`<P></P><SPAN style="FONT-FAMILY: Microsoft Sans Serif; FONT-SIZE: 8pt">`
	`<P style="MARGIN: 0in 0in 0pt"><SPAN style="FONT-FAMILY: 'Arial','sans-serif'; FONT-SIZE: 10pt">N/A - See record of work done for OIG data analyses.</SPAN></P></SPAN>`

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
Frequency: *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	*Source:* Allison Dichoso, Employee Relations Supervisor, 202-452-6402 *Scope:* Board non-EEO complaint data for FY11-FY13 *Details:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted] *Notes:* *Results 4:*
E.3.PRG - Data Analyses ***Procedure Step:*** Non-EEO Complaints - Data Reliability ***Type:*** ***Assigned To:*** BPM	*Purpose:* (b) (5) [redacted] *Criteria:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
Prepared By:	BPM, 11/7/2014	</SPAN> <P></P> <P></P><SPAN style="FONT-FAMILY: Microsoft Sans Serif; FONT-SIZE: 8pt"> <P style="MARGIN: 0in 0in 0pt"><SPAN style="FONT-FAMILY: 'Arial','sans-serif'; FONT-SIZE: 10pt">N/A - See record of work done for OIG data analyses.</SPAN></P></SPAN>
Reviewed By:	KLP, 3/18/2015	
PROPERTIES:		
Location:		
Frequency:		*Source:* Allison Dichoso, Employee Relations Supervisor, 202-452-6402
Category 4:		
User Category:		
Category 5		*Scope:* Board non-EEO complaint data for FY11-FY13
Category 6		
SCORECARD:		*Details:*
Rating:		
Sample Size:		(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted] *Notes:* *Results 4:*
E.3.PRG - Data Analyses *Procedure Step:* Non-EEO Complaints - Data Analyses *Type:* *Assigned To:* BPM *Prepared By:* BPM, 2/10/2015 *Reviewed By:* KLP, 3/18/2015 **PROPERTIES:** *Location:* *Frequency:* *Category 4:*	*Purpose:* (b) (5) [redacted] *Criteria:* </SPAN> <P></P> <P></P><SPAN style="FONT-FAMILY: Microsoft Sans Serif; FONT-SIZE: 8pt"> <P style="MARGIN: 0in 0in 0pt"><SPAN style="FONT-FAMILY: 'Arial','sans-serif'; FONT-SIZE: 10pt">N/A - See record of work done for OIG data analyses.</SPAN></P></SPAN> *Source:* We obtained data from the Employee Relations group in the Management

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
User Category: *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	Division: E.3.79, E.3.80, and E.3.81 (b) (5) *Scope:* Board non-EEO complaint data for CY11-CY13 *Details:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
	Notes:

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Results 4:
E.3.PRG - Data Analyses *Procedure Step:* Separation - Data Collection *Type:* *Assigned To:* BPM *Prepared By:* SMN, 11/18/2014 *Reviewed By:* KLP, 1/21/2015 PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	(b) (5) *Criteria:* </SPAN> <P></P> <P></P><SPAN style="FONT-FAMILY: Microsoft Sans Serif; FONT-SIZE: 8pt"> <P style="MARGIN: 0in 0in 0pt"><SPAN style="FONT-FAMILY: 'Arial','sans-serif'; FONT-SIZE: 10pt">N/A - See record of work done for OIG data analyses.</SPAN></P></SPAN> *Source:* Board total promotions data obtained from the HRASO office point of contact listed below: Jack Martin, Sr. Information Systems Specialist, jack.martin@frb.gov, 202-263-4830 *Scope:* Collecting Board promotions data for CY11-CY13 *Details:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) *Conclusion:* This data collection is consistent with OIG policies and procedures. *Notes:* *Results 4:*
E.3.PRG - Data Analyses *Procedure Step:* Separation - Data Reliability	*Purpose:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
Type:		
Assigned To:	BPM	
Prepared By:	SMN, 11/18/2014	
Reviewed By:	KLP, 1/21/2015	
PROPERTIES:		
Location:		
Frequency:		
Category 4:		
User Category:		
Category 5		
Category 6		
SCORECARD:		
Rating:		
Sample Size:		

Criteria:

```
</SPAN>
<P></P>
<P></P><SPAN style="FONT-FAMILY: Microsoft Sans Serif;
FONT-SIZE: 8pt">
<P style="MARGIN: 0in 0in 0pt"><SPAN style="FONT-FAMILY:
'Arial','sans-serif'; FONT-SIZE: 10pt">N/A - See record
of work done for OIG data analyses.</SPAN></P></SPAN>
```

Source:

Board total separations data obtained from both the HRASO and OD&I Office points of contact listed below:

Jack Martin, Sr. Information Systems Specialist, jack.martin@frb.gov, 202-263-4830

Johanna Bruce, Diversity and Inclusion Specialist Supervisor, johanna.c.bruce@frb.gov , 202-452-2787

Scope:

Data Reliability of Board separations data for CY11-CY13

Details:

(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

Summary	Detail
	Conclusion: This data reliability assessment is consistent with OIG policies and procedures. *Notes:* *Results 4:*
E.3.PRG - Data Analyses *Procedure Step:* Separation - Data Analyses *Type:* *Assigned To:* BPM *Prepared By:* SMN, 3/3/2015 *Reviewed By:* KLP, 3/16/2015 PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5*	*Purpose:* (b) (5) *Criteria:* </SPAN> <P></P> <P></P><SPAN style="FONT-FAMILY: Microsoft Sans Serif; FONT-SIZE: 8pt"> <P style="MARGIN: 0in 0in 0pt"><SPAN style="FONT-FAMILY: 'Arial','sans-serif'; FONT-SIZE: 10pt">N/A - See record of work done for OIG data analyses.</SPAN></P></SPAN> *Source:* *Scope:* Board separation data for FY11-FY13

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
Category 6 SCORECARD: *Rating:* *Sample Size:*	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
	Notes:
	Results 4:

The Board Can Enhance Its Diversity and Inclusion Efforts

Profile

General

Code: 2015-MO-B-006

Name: The Board Can Enhance Its Diversity and Inclusion Efforts

Audit Plan: 2014

Entities:

Name	*Breadcrumb*
Federal Reserve Board (FRB)	Organizations > Federal Reserve Board (FRB)

Unit:

Group: Audits & Evaluations

Type: Management & Operations

Location: FRB

Scope: Other

Origin:

Team

Lead: Kimberly Perteet

Manager:

Staff Type:

The Board Can Enhance Its Diversity and Inclusion Efforts

Schedule

(b) (5)

(b) (5)

Actual Start Date: 4/4/2014

Actual End Date:

(b) (5)

Actual Hours: 0

(b) (5)

Actual Resource Costs:

(b) (5)

Actual External Costs: $0.00

(b) (5)

Actual Expenses:

The Board Can Enhance Its Diversity and Inclusion Efforts

Risk

Risk:

Total Risk Score: 0

Inherent Risk: 0

Residual Risk: 0

Objective(s)

2014 Congressional Request on the Board’s Personnel Practices in Team Mate

Background

Planning

Scope

General

The Board Can Enhance Its Diversity and Inclusion Efforts

Contact

Primary

Other

Summary

Final Risk:	
Opinion:	
Cost Savings:	$0.00
Cost Avoidance:	$0.00
Rating:	
Summary:	

Tracking

(b) (5)	
Actual Draft Date:	3/19/2015
(b) (5)	
Actual Response Date:	3/19/2015

The Board Can Enhance Its Diversity and Inclusion Efforts

(b) (5)

Actual Issue Date: 3/31/2015

Milestones

Category	(b) (5)	Act. Date	Comments
Blank			
Entrance Meeting		5/12/2014	
Midpoint Meeting		9/3/2014	
Project Design Meeting		5/12/2014	
Message Development Meeting		10/2/2014	
AIG-Approved Draft Report		3/4/2015	
Discussion Draft Report		3/4/2015	
Exit Meeting		3/13/2015	
Formal Draft Report		3/19/2015	
Final Report		3/31/2015	

Custom Properties

Custom Property Name	Value

Procedures

Summary		Detail
E.6.PRG - Diversity Factors		*Purpose:* (b) (5)
Procedure Step:	(b) (5)	
Type:		*Criteria:*
Assigned To:	BPM	(b) (5)
Prepared By:	BPM, 3/26/2015	
Reviewed By:	KLP, 3/26/2015	
PROPERTIES:		
Location:		
Frequency:		*Source:*
Category 4:		Board policies and procedures related to diversity efforts and industry best practices.
User Category:		
Category 5		
Category 6		*Scope:* (b) (5)
SCORECARD:		
Rating:		*Details:*
Sample Size:		(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted] *Conclusion:* See record of work done. *Notes:* *Results 4:*
E.6.PRG - Diversity Factors *Procedure Step:* (b) (5) [redacted]	*Purpose:* (b) (5) [redacted]

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
Type:		
Assigned To:	BPM	(b) (5)
Prepared By:	SPK, 3/26/2015	
Reviewed By:	KLP, 3/26/2015	
PROPERTIES:		
Location:		*Source:*
Frequency:		OHC and relevant supporting documents.
Category 4:		
User Category:		*Scope:*
Category 5		(b) (5)
Category 6		
		Details:
SCORECARD:		(b) (5)
Rating:		
Sample Size:		

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted]
	Conclusion: See record of work done. No exceptions noted. *Notes:* *Results 4:*
E.6.PRG - Diversity Factors *Procedure Step:* (b) (5) *Type:* *Assigned To:* BPM *Prepared By:* BPM, 3/26/2015 *Reviewed By:* KLP, 3/26/2015	*Purpose:* (b) (5) [redacted]

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	*Source:* Board policies and procedures related to diversity efforts and industry best practices. *Scope:* (b) (5) *Details:* *Record of Work Done:* This assessment can be reviewed in workstep E.5.PRG. (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted] *Notes:* *Results 4:*
E.6.PRG - Diversity Factors *Procedure Step:* (b) (5) [redacted] *Type:* *Assigned To:* BPM *Prepared By:* BPM, 3/26/2015 *Reviewed By:* KLP, 3/26/2015 PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5*	*Purpose:* (b) (5) [redacted] *Criteria:* (b) (5) [redacted] *Source:* (b) (5) [redacted] *Scope:* (b) (5) [redacted]

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
Category 6 SCORECARD: *Rating:* *Sample Size:*	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted]
	Notes: *Results 4:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Profile

General

Code: 2015-MO-B-006

Name: The Board Can Enhance Its Diversity and Inclusion Efforts

Audit Plan: 2014

Entities:

Name	*Breadcrumb*
Federal Reserve Board (FRB)	Organizations > Federal Reserve Board (FRB)

Unit:

Group: Audits & Evaluations

Type: Management & Operations

Location: FRB

Scope: Other

Origin:

Team

Lead: Kimberly Perteet

Manager:

Staff Type:

The Board Can Enhance Its Diversity and Inclusion Efforts

Schedule

(b) (5)

(b) (5)

Actual Start Date: 4/4/2014

Actual End Date:

(b) (5)

Actual Hours: 0

(b) (5)

Actual Resource Costs:

(b) (5)

Actual External Costs: $0.00

(b) (5)

Actual Expenses:

The Board Can Enhance Its Diversity and Inclusion Efforts

Risk

Risk:

Total Risk Score: 0

Inherent Risk: 0

Residual Risk: 0

Objective(s)

2014 Congressional Request on the Board’s Personnel Practices in Team Mate

Background

Planning

Scope

General

The Board Can Enhance Its Diversity and Inclusion Efforts

Contact

Primary

Other

Summary

Final Risk:	
Opinion:	
Cost Savings:	$0.00
Cost Avoidance:	$0.00
Rating:	
Summary:	

Tracking

(b) (5)	
Actual Draft Date:	3/19/2015
(b) (5)	
Actual Response Date:	3/19/2015

The Board Can Enhance Its Diversity and Inclusion Efforts

(b) (5)

Actual Issue Date: 3/31/2015

Milestones

Category	(b) (5)	Act. Date	Comments
Blank			
Entrance Meeting		5/12/2014	
Midpoint Meeting		9/3/2014	
Project Design Meeting		5/12/2014	
Message Development Meeting		10/2/2014	
AIG-Approved Draft Report		3/4/2015	
Discussion Draft Report		3/4/2015	
Exit Meeting		3/13/2015	
Formal Draft Report		3/19/2015	
Final Report		3/31/2015	

Custom Properties

Custom Property Name	Value

Procedures

Summary	Detail
E.4.PRG - Management's Efforts *Procedure Step:* Efforts to Respond to Complaints - EEO *Type:* *Assigned To:* *Prepared By:* SPK, 3/26/2015 *Reviewed By:* KLP, 3/26/2015 PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	*Purpose:* Assess the EEO's efforts to respond to complaints. *Criteria:* N/A - Documenting EEO's processes to identify and respond to trends in EEO complaints. *Source:* See record of work done *Scope:* Board EEO complaints for FY11-FY13. *Details:* (b) (5) [redacted]

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) *Conclusion:* See record of work done. No exceptions noted. *Notes:* *Results 4:*
E.4.PRG - Management's Efforts ***Procedure Step:*** Efforts to Respond to Employee Satisfaction Survey Results - EEO ***Type:*** ***Assigned To:*** ***Prepared By:*** SPK, 3/26/2015 ***Reviewed By:*** KLP, 3/26/2015 **PROPERTIES:** ***Location:*** ***Frequency:*** ***Category 4:*** ***User Category:***	*Purpose:* Assess the EEO's efforts to respond to employee satisfaction survey results. *Criteria:* Audit Program (B.1.101) *Source:* See record of work done. *Scope:* Board Employee Satisfaction Survey Results for CY11-CY13. *Details:* *Record of Work Done:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
Category 5 *Category 6* SCORECARD: *Rating:* *Sample Size:*	(b) (5) *Conclusion:* See record of work done. No exceptions noted. *Notes:* *Results 4:*
E.4.PRG - Management's Efforts *Procedure Step:* (b) (5) *Type:* *Assigned To:* *Prepared By:* SPK, 3/26/2015 *Reviewed By:* KLP, 3/26/2015	*Purpose:* (b) (5) *Criteria:* Audit Program (B.1.101) *Source:* See record of work done.

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	*Scope:* EEO diversity programs and activities for CY11-CY13. (b) (5) *Conclusion:* See record of work done.

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Notes: *Results 4:*
E.4.PRG - Management's Efforts ***Procedure Step:*** Diversity Training - EEO ***Type:*** ***Assigned To:*** ***Prepared By:*** SPK, 3/26/2015 ***Reviewed By:*** KLP, 3/26/2015 **PROPERTIES:** ***Location:*** ***Frequency:*** ***Category 4:*** ***User Category:*** ***Category 5*** ***Category 6*** **SCORECARD:** ***Rating:***	*Purpose:* Assess the EEO's diversity training. *Criteria:* Audit Program (B.1.101) *Source:* See record of work done. *Scope:* EEO diversity training materials for FY11-FY13. *Details:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
Sample Size:	(b) (5) [redacted] *Conclusion:* See record of work done. *Notes:* *Results 4:*
E.4.PRG - Management's Efforts *Procedure Step:* (b) (5) [redacted] *Type:* *Assigned To:* KLP *Prepared By:* KLP, 3/19/2015 *Reviewed By:* (None) PROPERTIES: *Location:* *Frequency:*	*Purpose:* (b) (5) [redacted] (b) (5) [redacted] *Source:* Board officials

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
Category 4: *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	*Scope:* Board OHC complaints for FY11-FY13. *Details:* (b) (5) *Notes:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Results 4:
E.4.PRG - Management's Efforts (b) (5) [redacted] *Type:* Fieldwork *Assigned To:* SMN *Prepared By:* SMN, 3/4/2015 *Reviewed By:* KLP, 3/4/2015 PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	*Purpose:* (b) (5) [redacted] *Criteria:* (b) (5) [redacted] *Source:* OHC Sioux THompson Organizational Learning and Development *Scope:* Board Employee Satisfaction Survey results for FY11-FY13. *Details:* (b) (5) [redacted]

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
	Notes: *Results 4:*
E.4.PRG - Management's Efforts	*Purpose:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
		(b) (5)
Procedure Step:	(b) (5)	(b) (5)
Type:		
Assigned To:		
Prepared By:	BPM, 3/3/2015	
Reviewed By:	KLP, 3/3/2015	*Source:*
		(b) (5)
PROPERTIES:		
Location:		
Frequency:		
Category 4:		
User Category:		
Category 5		
Category 6		
SCORECARD:		*Details:*
Rating:		
Sample Size:		(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted] *Notes:* *Results 4:*
E.4.PRG - Management's Efforts *Procedure Step:* (b) (5) [redacted] *Type:* *Assigned To:* *Prepared By:* SPK, 3/26/2015 *Reviewed By:* KLP, 3/26/2015	*Purpose:* (b) (5) [redacted]. *Criteria:* (b) (5) [redacted] *Source:* Board

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	*Scope:* (b) (5) *Details:* (b) (5) *Conclusion:* See record of work done. No exception noted. *Notes:* *Results 4:*
E.4.PRG - Management's Efforts	*Purpose:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
Procedure Step:	(b) (5)	(b) (5)
Type:	Fieldwork	*Criteria:*
Assigned To:	KLP	(b) (5)
Prepared By:	KLP, 3/3/2015	*Source:*
Reviewed By:	(None)	Don Hammond, COO Michell Clark, Mgt Division Lewis Andrews, HR Analytics Manager
PROPERTIES:		*Scope:*
Location:		CY 2011-2013
Frequency:		*Details:*
Category 4:		(b) (5)
User Category:		
Category 5		
Category 6		
SCORECARD:		
Rating:		
Sample Size:		

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Notes: *Results 4:*
E.4.PRG - Management's Efforts *Procedure Step:* (b) (5) *Type:* Fieldwork *Assigned To:* SMN *Prepared By:* SPK, 3/26/2015 *Reviewed By:* KLP, 3/26/2015 PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD:	*Purpose:* (b) (5) *Criteria:* Board's PMP policy,; (b) (5) *Source:* Sioux Thompson, ODL *Scope:* (b) (5) *Details:* *Record of Work Done:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
Rating: *Sample Size:*	(b) (5)
	Notes: *Results 4:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Profile

General

Code: 2015-MO-B-006

Name: The Board Can Enhance Its Diversity and Inclusion Efforts

Audit Plan: 2014

Entities:

Name	*Breadcrumb*
Federal Reserve Board (FRB)	Organizations > Federal Reserve Board (FRB)

Unit:

Group: Audits & Evaluations

Type: Management & Operations

Location: FRB

Scope: Other

Origin:

Team

Lead: Kimberly Perteet

Manager:

Staff Type:

The Board Can Enhance Its Diversity and Inclusion Efforts

Schedule

(b) (5)

(b) (5)

Actual Start Date: 4/4/2014

Actual End Date:

(b) (5)

Actual Hours: 0

(b) (5)

Actual Resource Costs:

(b) (5)

Actual External Costs: $0.00

(b) (5)

Actual Expenses:

The Board Can Enhance Its Diversity and Inclusion Efforts

Risk

Risk:

Total Risk Score: 0

Inherent Risk: 0

Residual Risk: 0

Objective(s)

2014 Congressional Request on the Board’s Personnel Practices in Team Mate

Background

Planning

Scope

General

The Board Can Enhance Its Diversity and Inclusion Efforts

Contact

Primary

Other

Summary

Final Risk:	
Opinion:	
Cost Savings:	$0.00
Cost Avoidance:	$0.00
Rating:	
Summary:	

Tracking

(b) (5)	
Actual Draft Date:	3/19/2015
(b) (5)	
Actual Response Date:	3/19/2015

The Board Can Enhance Its Diversity and Inclusion Efforts

(b) (5)

Actual Issue Date: 3/31/2015

Milestones

Category	(b) (5)	Act. Date	Comments
Blank			
Entrance Meeting		5/12/2014	
Midpoint Meeting		9/3/2014	
Project Design Meeting		5/12/2014	
Message Development Meeting		10/2/2014	
AIG-Approved Draft Report		3/4/2015	
Discussion Draft Report		3/4/2015	
Exit Meeting		3/13/2015	
Formal Draft Report		3/19/2015	
Final Report		3/31/2015	

Custom Properties

Custom Property Name	Value

Procedures

Summary		Detail
E.5.PRG - OD&I		*Purpose:* (b) (5)
Procedure Step:	(b) (5)	
Type:		*Criteria:*
Assigned To:	SMN	Board policies and procedures.
Prepared By:	BPM, 3/17/2015	
Reviewed By:	KLP, 3/17/2015	*Source:*
		OD&I officials, documents, reports and annual reports to Congress, MD-715, and certain elements of the MD-715.
PROPERTIES:		
Location:		*Scope:*
Frequency:		Board OD&I activities from January 2011-January 2013.
Category 4:		
User Category:		*Details:*
Category 5		
Category 6		(b) (5)
SCORECARD:		
Rating:		
Sample Size:		

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
	Notes:
	Results 4:
E.5.PRG - OD&I	*Purpose:*
Procedure Step: (b) (5)	(b) (5)
Type:	

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
Assigned To:	SMN	*Source:*
Prepared By:	SMN, 3/17/2015	
Reviewed By:	KLP, 3/25/2015	*Scope:* Board employee satisfaction survey results for FY11-FY13.
PROPERTIES:		
Location:		*Details:*
Frequency:		
Category 4:		(b) (5)
User Category:		
Category 5		
Category 6		
SCORECARD:		
Rating:		
Sample Size:		

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted] *Notes:* *Results 4:*
E.5.PRG - OD&I ***Procedure Step:*** (b) (5) [redacted] ***Type:*** ***Assigned To:*** SMN ***Prepared By:*** SPK, 3/23/2015 ***Reviewed By:*** KLP, 3/26/2015 **PROPERTIES:** ***Location:*** ***Frequency:***	*Purpose:* (b) (5) [redacted] *Criteria:* OWMI's efforts *Source:* Shelia Clark, OD&I, OIG Analysis *Scope:* OMWI activities/efforts in 2011-2013

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
Category 4: *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	*Details:* (b) (5) *Conclusion:* See record of work done. No exceptions noted. *Notes:* *Results 4:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
E.5.PRG - OD&I		*Purpose:* Assess the OMWI's efforts to increase diversity within the agency overall and in senior management .
Procedure Step:	Efforts to Increase Diversity - OMWI	
Type:		*Criteria:* Board policies and procedures, GAO's Expert-Identified Leading practices, and benchmarking with NCUA. In addition, relevant laws and regulations such as MD-715, the No FEAR Act and section 342 of the Dodd-Frank Act.
Assigned To:	SMN	
Prepared By:	SPK, 3/19/2015	
Reviewed By:	KLP, 3/26/2015	
PROPERTIES:		*Source:* Board documents, GAO, and National Credit Union Association reports.
Location:		
Frequency:		
Category 4:		
User Category:		*Scope:* OMWI and EEO function under OD&I's diversity programs and activities for 2011-2013.
Category 5		
Category 6		*Details:* (b) (5)
SCORECARD:		
Rating:		
Sample Size:		

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted] *Notes:* *Results 4:*
E.5.PRG - OD&I ***Procedure Step:*** EEO and Diversity Training ***Type:*** ***Assigned To:*** SMN ***Prepared By:*** BPM, 3/17/2015 ***Reviewed By:*** KLP, 3/27/2015 **PROPERTIES:** ***Location:*** ***Frequency:***	*Purpose:* Assess the OMWI's diversity training. *Criteria:* The Board's No FEAR Act Written Training Plan, wp E.5.4 5 CFR Part 724.203, Training Obligations, B.1.110 Instructions to Federal Agencies for EEO MD-715 B.1.33 *Source:* No FEAR Act Training plan provided by Sheila Clark, Office of

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
Category 4: *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	Diversity and Inclusion Director. Guidance documents MD-715 and 5 CFR 724 were both publically available. *Scope:* OMWI's diversity training for FY11-FY13. *Details:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
	Notes:

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Results 4:
E.5.PRG - OD&I *Procedure Step:* (b) (5) *Type:* *Assigned To:* SPK *Prepared By:* BPM, 2/28/2015 *Reviewed By:* KLP, 3/30/2015 PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	*Purpose:* (b) (5) *Criteria:* (b) (5) *Source:* Board Divisions *Scope:* OMWI's programs and activities for FY11-FY13 *Details:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted] *Notes:* *Results 4:*
E.5.PRG - OD&I *Procedure Step:* (b) (5) [redacted] *Type:* *Assigned To:* SMN *Prepared By:* SMN, 3/17/2015 *Reviewed By:* KLP, 3/17/2015 **PROPERTIES:** *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6*	*Purpose:* (b) (5) [redacted] *Criteria:* (b) (5) [redacted] *Source:* Shelia Clark, Director, OD&I *Scope:* 2014 OMWI Annual Report *Details:* *Record of Work Done:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
SCORECARD: *Rating:* *Sample Size:*	(b) (5) *Notes:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Results 4:
E.5.PRG - OD&I *Procedure Step:* (b) (5) *Type:* *Assigned To:* SPK *Prepared By:* SPK, 3/17/2015 *Reviewed By:* KLP, 3/17/2015 PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	*Purpose:* *Criteria:* Section 342 of Dodd Frank Act requirements for the establishment of an agency's OMWI. *Source:* Board policies and procedures, Dodd-Frank Act, and interviews with OD&I officials. *Scope:* OD&I, specifically OMWI's programs and activities from 2011-2013. *Details:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
	Notes: *Results 4:*
E.5.PRG - OD&I ***Procedure Step:*** Benchmarking	*Purpose:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
Type:		(b) (5)
Assigned To:	KLP	
Prepared By:	SPK, 2/26/2015	
Reviewed By:	KLP, 3/17/2015	*Criteria:* (b) (5)
PROPERTIES:		
Location:		*Source:* Allison D. Washington, Senior Auditor, NCUA OIG, OIG, Shelia Clark, ODI Director
Frequency:		
Category 4:		
User Category:		
Category 5		
Category 6		*Scope:* NCUA's Strategic Plan
SCORECARD:		
Rating:		*Details:*
Sample Size:		(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
	Notes: *Results 4:*

The Board Can Enhance Its Diversity and Inclusion Efforts

The Board Can Enhance Its Diversity and Inclusion Efforts

Profile

General

Code: 2015-MO-B-006

Name: The Board Can Enhance Its Diversity and Inclusion Efforts

Audit Plan: 2014

Entities:

Name	*Breadcrumb*
Federal Reserve Board (FRB)	Organizations > Federal Reserve Board (FRB)

Unit:

Group: Audits & Evaluations

Type: Management & Operations

Location: FRB

Scope: Other

Origin:

Team

Lead: Kimberly Perteet

Manager:

Staff Type:

The Board Can Enhance Its Diversity and Inclusion Efforts

Schedule

(b) (5)

(b) (5)

Actual Start Date: 4/4/2014

Actual End Date:

(b) (5)

Actual Hours: 0

(b) (5)

Actual Resource Costs:

(b) (5)

Actual External Costs: $0.00

(b) (5)

Actual Expenses:

The Board Can Enhance Its Diversity and Inclusion Efforts

Risk

Risk:

Total Risk Score: 0

Inherent Risk: 0

Residual Risk: 0

Objective(s)

2014 Congressional Request on the Board’s Personnel Practices in Team Mate

Background

Planning

Scope

General

The Board Can Enhance Its Diversity and Inclusion Efforts

Contact

Primary

Other

Summary

Final Risk:	
Opinion:	
Cost Savings:	$0.00
Cost Avoidance:	$0.00
Rating:	
Summary:	

Tracking

(b) (5)	
Actual Draft Date:	3/19/2015
(b) (5)	
Actual Response Date:	3/19/2015

The Board Can Enhance Its Diversity and Inclusion Efforts

(b) (5)

Actual Issue Date: 3/31/2015

Milestones

Category	(b) (5)	Act. Date	Comments
Blank			
Entrance Meeting		5/12/2014	
Midpoint Meeting		9/3/2014	
Project Design Meeting		5/12/2014	
Message Development Meeting		10/2/2014	
AIG-Approved Draft Report		3/4/2015	
Discussion Draft Report		3/4/2015	
Exit Meeting		3/13/2015	
Formal Draft Report		3/19/2015	
Final Report		3/31/2015	

Custom Properties

Custom Property Name	Value

Procedures

Summary		Detail
E.2.PRG - Personnel Operations, Policies, and Procedures		*Purpose:* Documents the OIG's approval of the Audit of the Board's Diversity and Inclusion's Processes Audit Program
Procedure Step:	OIG Approval of Audit Program	
Type:		*Criteria:* OIG policies and procedures
Assigned To:	KLP	
Prepared By:	KLP, 1/20/2015	*Source:* Klmnberly Perteet, Project Lead
Reviewed By:	(None)	
PROPERTIES:		*Scope:* Board's Audit Program CY 2011- CY 2014
Location:		
Frequency:		*Details:*
Category 4:		
User Category:		*Record of Work Done:* See the following procedure steps oulined in E.2.78
Category 5		
Category 6		*Conclusion:* This audit program is in compliance with OIG policies and procedures.
SCORECARD:		
Rating:		*Notes:*
Sample Size:		*Results 4:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
E.2.PRG - Personnel Operations, Policies, and Procedures *Procedure Step:* (b) (5) *Type:* *Assigned To:* SMN *Prepared By:* SMN, 3/12/2015 *Reviewed By:* KLP, 3/23/2015 PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	*Purpose:* (b) (5) *Criteria:* Vacant Posting Policy *Source:* Board and OIG *Scope:* Board hiring operations, policies, and procedures from FY11-FY13 *Details:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted] *Conclusion:* Based on the record of work completed, *Notes:* *Results 4:*
E.2.PRG - Personnel Operations, Policies, and Procedures ***Procedure Step:*** (b) (5) [redacted] (b) (5) [redacted] ***Type:*** ***Assigned To:*** SPK ***Prepared By:*** SMN, 3/12/2015 ***Reviewed By:*** KLP, 3/23/2015	*Purpose:* (b) (5) [redacted] *Criteria:* The Board's Human Capital Practices *Source:* Human Capital Officals *Scope:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
PROPERTIES:	CY 2011- CY 2013
Location:	
Frequency:	*Details:*
Category 4:	
User Category:	(b) (5)
Category 5	
Category 6	
SCORECARD:	
Rating:	
Sample Size:	

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted] *Notes:* *Results 4:*
E.2.PRG - Personnel Operations, Policies, and Procedures ***Procedure Step:*** (b) (5) [redacted] ***Type:*** ***Assigned To:*** SPK ***Prepared By:*** SPK, 3/25/2015 ***Reviewed By:*** KLP, 3/25/2015 **PROPERTIES:**	*Purpose:* (b) (5) [redacted] *Criteria:* Federal Reserve Act Section 10 *Source:* Board of Governors Legal Staff

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
Location: *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	*Scope:* Board hiring operations, policies, and procedures from FY11-FY13 *Details:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted] *Notes:* *Results 4:*
E.2.PRG - Personnel Operations, Policies, and Procedures *Procedure Step:* (b) (5) [redacted] *Type:* *Assigned To:* SPK *Prepared By:* SPK, 1/21/2015 *Reviewed By:* (None) PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6*	*Purpose:* (b) (5) [redacted] *Criteria:* *Source:* *Scope:* Board hiring operations, policies, and procedures from FY11-FY13 *Details:* (b) (5) [redacted]

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
SCORECARD: *Rating:* *Sample Size:*	(b) (5) *Notes:* *Results 4:*
E.2.PRG - Personnel Operations, Policies, and Procedures *Procedure Step:* (b) (5) *Type:* *Assigned To:* SMN *Prepared By:* SPK, 3/24/2015 *Reviewed By:* KLP, 3/25/2015	*Purpose:* (b) (5) *Criteria:* Board policies and procedures. *Source:* Board interviews and documents. *Scope:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	(b) (5) *Conclusion:* See record of work done. No exception noted. *Notes:* *Results 4:*
E.2.PRG - Personnel Operations, Policies, and Procedures *Procedure Step:* (b) (5) *Type:*	*Purpose:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
Assigned To:	SPK	Board policies and procedures.
Prepared By:	SPK, 3/18/2015	
Reviewed By:	KLP, 3/18/2015	*Source:* Board
PROPERTIES:		
Location:		*Scope:* Board performance management operations, policies, and procedures from 2011 to 2013.
Frequency:		
Category 4:		
User Category:		*Details:*
Category 5		(b) (5)
Category 6		
SCORECARD:		
Rating:		
Sample Size:		

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted]
	Conclusion: See record of work done. *Notes:* *Results 4:*
E.2.PRG - Personnel Operations, Policies, and Procedures	*Purpose:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
Procedure Step:	(b) (5)	(b) (5)
Type:		*Criteria:*
Assigned To:	SPK	The Board's Perfomance Management Policy
Prepared By:	SPK, 3/25/2015	*Source:*
Reviewed By:	KLP, 3/25/2015	Board officials and the OIG
PROPERTIES:		*Scope:*
Location:		Board performance management operations, policies, and procedures from FY11-FY13
Frequency:		
Category 4:		*Details:*
User Category:		(b) (5)
Category 5		
Category 6		
SCORECARD:		
Rating:		
Sample Size:		

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted] *Conclusion:* See record of work done. *Notes:* *Results 4:*
E.2.PRG - Personnel Operations, Policies, and Procedures *Procedure Step:* (b) (5) [redacted] *Type:* *Assigned To:* SPK *Prepared By:* SPK, 11/10/2014	*Purpose:* (b) (5) [redacted] *Criteria:* *Source:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
Reviewed By:	KLP, 3/25/2015	
PROPERTIES:		*Scope:* Board performance management operations, policies, and procedures from FY11-FY13
Location:		
Frequency:		*Details:*
Category 4:		
User Category:		(b) (5)
Category 5		
Category 6		
SCORECARD:		
Rating:		
Sample Size:		

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Notes: *Results 4:*
E.2.PRG - Personnel Operations, Policies, and Procedures *Procedure Step:* (b) (5) *Type:* *Assigned To:* SPK *Prepared By:* SPK, 3/25/2015 *Reviewed By:* KLP, 3/25/2015 PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:*	*Purpose:* (b) (5) *Criteria:* The Board's Performance Management policy *Source:* Board officials and the OIG *Scope:* Board performance management operations, policies, and procedures from FY11-FY13 *Details:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
Sample Size:	(b) (5)
	Notes: *Results 4:*
E.2.PRG - Personnel Operations, Policies, and Procedures *Procedure Step:* (b) (5) *Type:*	*Purpose:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
Assigned To:	SMN	*Criteria:*
Prepared By:	SMN, 3/10/2015	GAGAS Appendix A, Section 6.04 - Types of Evidence
Reviewed By:	KLP, 3/10/2015	A6.04 In terms of its form and how it is collected, evidence may be categorized as physical, documentary, or testimonial. Physical evidence is obtained by auditors' direct inspection or observation of people, property, or events. Such evidence may be documented in summary memos, photographs, videos, drawings, charts, maps, or physical samples. Documentary evidence is obtained in the form of already existing information such as letters, contracts, accounting records, invoices, spreadsheets, database extracts, electronically stored information, and management information on performance. Testimonial evidence is obtained through inquiries, interviews, focus groups, public forums, or questionnaires. Auditors frequently use analytical processes including computations, comparisons, separation of information into components, and rational arguments to analyze any evidence gathered to determine whether it is sufficient and appropriate. The strength and weakness of each form of evidence depends on the facts and circumstances associated with the evidence and professional judgment in the context of the audit objectives.
PROPERTIES:		
Location:		
Frequency:		
Category 4:		
User Category:		
Category 5		
Category 6		
SCORECARD:		
Rating:		
Sample Size:		
		Source:
		Policies and procedures, interviews, and review of other documentation.
		Scope:
		Board promotion practices/operations, policies, and procedures from CY11-CY13

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Details: (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted]
	Conclusion: This review is in complaince with GAGAS and OIG policies and procedures based on the work conducted. *Notes:* *Results 4:*
E.2.PRG - Personnel Operations, Policies, and Procedures	*Purpose:* (b) (5) [redacted]

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
Procedure Step:	(b) (5)	(b) (5)
Type:		*Criteria:* Federal Reserve Act Section 10
Assigned To:	SPK	
Prepared By:	SPK, 3/25/2015	*Source:* Board Legal and the OIG
Reviewed By:	KLP, 3/26/2015	
PROPERTIES:		*Scope:* Board promotion operations, policies, and procedures from FY11-FY13
Location:		
Frequency:		*Details:*
Category 4:		
User Category:		(b) (5)
Category 5		
Category 6		
SCORECARD:		
Rating:		
Sample Size:		

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted] *Notes:* *Results 4:*
E.2.PRG - Personnel Operations, Policies, and Procedures *Procedure Step:* (b) (5) [redacted] *Type:* *Assigned To:* SPK *Prepared By:* SPK, 3/25/2015 *Reviewed By:* KLP, 3/26/2015	*Purpose:* (b) (5) [redacted] *Criteria:* Board promotion policies and procedures

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	*Source:* Bioard and OIG Analysis *Scope:* Board promotion operations, policies, and procedures from FY11-FY13 *Details:* (b) (5) *Conclusion:* See record of work done. No exception noted.

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Notes: *Results 4:*
E.2.PRG - Personnel Operations, Policies, and Procedures *Procedure Step:* (b) (5) *Type:* *Assigned To:* SPK *Prepared By:* SPK, 3/25/2015 *Reviewed By:* KLP, 3/26/2015 PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:*	*Purpose:* (b) (5) *Criteria:* Board policies and procedures related to promotions. *Source:* Board officials and the OIG *Scope:* Board promotion operations, policies, and procedures from FY11-FY13 *Details:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
Sample Size:	(b) (5)
	Notes: *Results 4:*
E.2.PRG - Personnel Operations, Policies, and Procedures *Procedure Step:* (b) (5)	*Purpose:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
Type:		
Assigned To:	SPK	*Criteria:*
Prepared By:	SPK, 3/25/2015	(b) (5)
Reviewed By:	KLP, 3/26/2015	
PROPERTIES:		*Source:*
Location:		Board officials and the OIG
Frequency:		
Category 4:		*Scope:*
User Category:		(b) (5)
Category 5		
Category 6		*Details:*
SCORECARD:		(b) (5)
Rating:		
Sample Size:		

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
	Notes:
	Results 4:
E.2.PRG - Personnel Operations, Policies, and Procedures	*Purpose:* (b) (5)
Procedure Step: (b) (5)	
Type:	

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
Assigned To:	BPM	(b) (5)
Prepared By:	BPM, 3/26/2015	
Reviewed By:	KLP, 3/26/2015	*Source:*
		OIG interviews with Office of Diversity and Inclusion
PROPERTIES:		Board Policies and Procedures
Location:		Flowcharts created by the OIG
Frequency:		
Category 4:		*Scope:*
User Category:		Board EEO complaint operations, policies, and procedures from FY11-FY13
Category 5		*Details:*
Category 6		
		(b) (5)
SCORECARD:		
Rating:		
Sample Size:		

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) *Notes:* *Results 4:*
E.2.PRG - Personnel Operations, Policies, and Procedures *Procedure Step:* (b) (5) *Type:* *Assigned To:* SMN *Prepared By:* BPM, 3/25/2015 *Reviewed By:* KLP, 3/25/2015	*Purpose:* (b) (5) *Criteria:* The Board of Governors of the Federal Reserve System (the Board) has adopted a final rule that amends its "Rules Regarding Equal Opportunity," which establishes programs and procedures to promote equal opportunity for Board employees. This rule was published in the Federal Register as 12 CFR 268 B.1.25

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* **SCORECARD:** *Rating:* *Sample Size:*	268.104 outlines Pre-complaint processing 268.105 outlines Individual complaints 268.106 outlines Dismissals of complaints 268.107 outlines investigation of complaints 268.108 outlines Hearings 268.109 outlines Final action by the Board Also we identified the Board's EEO Policy which mirrors the above guidance in 12 CFR 268 B.1.1 *Source:* For guidance information, see PSSC's in wp links B.1.1 and B.1.25 Board EEO complaint data obtained from E.3.PRG and the OD&I Office points of contact listed below: Andre Smith, Senior Diversity and Inclusion Specialist, andre.m.smith@frb.gov , 202-728-5876 Johanna Bruce, Diversity and Inclusion Specialist Supervisor, johanna.c.bruce@frb.gov , 202-452-2787 *Scope:* Board EEO complaint operations, policies, and procedures from FY11-FY13 *Details:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
	Notes: *Results 4:*
E.2.PRG - Personnel Operations, Policies, and Procedures *Procedure Step:* (b) (5) *Type:*	*Purpose:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
Assigned To:	SPK	*Criteria:*
Prepared By:	SPK, 3/25/2015	Board EEO Complaint policy
Reviewed By:	KLP, 3/25/2015	
		Source:
PROPERTIES:		Board and OIG analysis
Location:		
Frequency:		*Scope:*
Category 4:		Board EEO complaint operations, policies, and procedures from FY11-FY13
User Category:		
Category 5		*Details:*
Category 6		(b) (5)
SCORECARD:		
Rating:		
Sample Size:		
		Conclusion:
		See record of work done. No exception noted.

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Notes: *Results 4:*
E.2.PRG - Personnel Operations, Policies, and Procedures *Procedure Step:* (b) (5) [redacted] *Type:* *Assigned To:* BPM *Prepared By:* BPM, 3/25/2015 *Reviewed By:* KLP, 3/26/2015 PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD:	*Purpose:* (b) (5) [redacted] *Criteria:* (b) (5) [redacted] *Source:* Board EEO complaint data obtained from the OD&I Office points of contact listed below: Andre Smith, Senior Diversity and Inclusion Specialist, andre.m.smith@frb.gov , 202-728-5876 Johanna Bruce, Diversity and Inclusion Specialist Supervisor, johanna.c.bruce@frb.gov , 202-452-2787 *Scope:* Board EEO complaint operations, policies, and procedures from FY11-FY13 *Details:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
Rating: *Sample Size:*	(b) (5)
	Notes: *Results 4:*
E.2.PRG - Personnel Operations, Policies, and Procedures	*Purpose:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
Procedure Step:	(b) (5)	(b) (5)
Type:		*Criteria:*
Assigned To:	BPM	GAGAS Standards 6.56 Auditors must obtain sufficient, appropriate evidence to provide a reasonable basis for their findings and conclusions. 6.57 The concept of sufficient, appropriate evidence is integral to an audit. Appropriateness is the measure of the quality of evidence that encompasses its relevance, validity, and reliability in providing support for findings and conclusions related to the audit objectives. In assessing the overall appropriateness of evidence, auditors should assess whether the evidence is relevant, valid, and reliable. Sufficiency is a measure of the quantity of evidence used to support the findings and conclusions related to the audit objectives. In assessing the sufficiency of evidence, auditors should determine whether enough evidence has been obtained to persuade a knowledgeable person that the findings are reasonable.
Prepared By:	BPM, 3/19/2015	
Reviewed By:	KLP, 3/25/2015	
PROPERTIES:		
Location:		
Frequency:		
Category 4:		
User Category:		
Category 5		
Category 6		
		Source: Allison Dichoso, ER Supervisor Kevin May, Sr Employee Relations Specialist Keisha Hargo, Sr Employee Relations Specialist
SCORECARD:		
Rating:		
Sample Size:		
		Scope: Board non-EEO complaint operations, policies, and procedures from FY11-FY13

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Notes: *Results 4:*
E.2.PRG - Personnel Operations, Policies, and Procedures *Procedure Step:* (b) (5) [redacted] *Type:* *Assigned To:* SPK *Prepared By:* BPM, 3/25/2015 *Reviewed By:* KLP, 3/26/2015 **PROPERTIES:** *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* **SCORECARD:**	*Purpose:* (b) (5) [redacted] *Criteria:* (b) (5) [redacted] *Source:* We obtained data from the Employee Relations group in the Management Division: E.3.79, E.3.80, E.3.81 (b) (5) [redacted] *Scope:* Board non-EEO complaint operations, policies, and procedures from FY11-FY13 *Details:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
Rating: *Sample Size:*	(b) (5)
	Notes: *Results 4:*
E.2.PRG - Personnel Operations, Policies, and Procedures *Procedure Step:* (b) (5)	*Purpose:* *Criteria:* Board policies related to non-EEO complaints or matters.

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
Type:		
Assigned To:	SPK	*Source:*
Prepared By:	SPK, 3/25/2015	Board policies and OIG auditor analysis.
Reviewed By:	KLP, 3/25/2015	
		Scope:
PROPERTIES:		Board non-EEO complaint operations, policies, and procedures from FY11-FY13
Location:		
Frequency:		*Details:*
Category 4:		
User Category:		(b) (5)
Category 5		
Category 6		
SCORECARD:		
Rating:		
Sample Size:		

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	See record of work done. No exception noted. *Notes:* *Results 4:*
E.2.PRG - Personnel Operations, Policies, and Procedures *Procedure Step:* (b) (5) [redacted] *Type:* *Assigned To:* BPM *Prepared By:* BPM, 3/25/2015 *Reviewed By:* KLP, 3/26/2015 PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6*	*Purpose:* (b) (5) [redacted] *Criteria:* (b) (5) [redacted] *Source:* We obtained data from the Employee Relations group in the Management Division:E.3.79, E.3.80, and E.3.81 (b) (5) [redacted] *Scope:* Board non-EEO complaint operations, policies, and procedures from FY11-FY13

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
SCORECARD: *Rating:* *Sample Size:*	(b) (5) *Notes:* *Results 4:*

The Board Can Enhance Its Diversity and Inclusion Efforts

The Board Can Enhance Its Diversity and Inclusion Efforts

Profile

General

Code: 2015-MO-B-006

Name: The Board Can Enhance Its Diversity and Inclusion Efforts

Audit Plan: 2014

Entities:

Name	*Breadcrumb*
Federal Reserve Board (FRB)	Organizations > Federal Reserve Board (FRB)

Unit:

Group: Audits & Evaluations

Type: Management & Operations

Location: FRB

Scope: Other

Origin:

Team

Lead: Kimberly Perteet

Manager:

Staff Type:

The Board Can Enhance Its Diversity and Inclusion Efforts

Schedule

(b) (5)

(b) (5)

Actual Start Date: 4/4/2014

Actual End Date:

(b) (5)

Actual Hours: 0

(b) (5)

Actual Resource Costs:

(b) (5)

Actual External Costs: $0.00

(b) (5)

Actual Expenses:

The Board Can Enhance Its Diversity and Inclusion Efforts

Risk

Risk:

Total Risk Score:	0
Inherent Risk:	0
Residual Risk:	0

Objective(s)

2014 Congressional Request on the Board’s Personnel Practices in Team Mate

Background

Planning

Scope

General

The Board Can Enhance Its Diversity and Inclusion Efforts

Contact

Primary

Other

Summary

Final Risk:	
Opinion:	
Cost Savings:	$0.00
Cost Avoidance:	$0.00
Rating:	
Summary:	

Tracking

(b) (5)	
Actual Draft Date:	3/19/2015

(b) (5)	
Actual Response Date:	3/19/2015

The Board Can Enhance Its Diversity and Inclusion Efforts

(b) (5)

Actual Issue Date: 3/31/2015

Milestones

Category	(b) (5)	Act. Date	Comments
Blank			
Entrance Meeting		5/12/2014	
Midpoint Meeting		9/3/2014	
Project Design Meeting		5/12/2014	
Message Development Meeting		10/2/2014	
AIG-Approved Draft Report		3/4/2015	
Discussion Draft Report		3/4/2015	
Exit Meeting		3/13/2015	
Formal Draft Report		3/19/2015	
Final Report		3/31/2015	

Custom Properties

Custom Property Name	Value

Procedures

Summary		Detail
D.1.PRG - Reporting		*Purpose:* Document the preliminary observations and findings related to the Board's diversity and inclusion processes.
Procedure Step:	Preliminary Observations and Findings	
Type:		*Criteria:* OIG policies and procedures
Assigned To:	SMN	
Prepared By:	SMN, 4/1/2015	*Source:* See record of work done.
Reviewed By:	KLP, 4/7/2015	
PROPERTIES:		*Scope:* Audit of the Board's diversity and inclusion processes.
Location:		
Frequency:		*Details:*
Category 4:		
User Category:		*Record of Work Done:* Refer to D.1.1
Category 5		
Category 6		*Conclusion:* See record of work done.
SCORECARD:		
Rating:		*Notes:*
Sample Size:		

Summary	Detail
	Results 4:
D.1.PRG - Reporting *Procedure Step:* Prepare Draft Reports *Type:* Reporting *Assigned To:* SMN *Prepared By:* SMN, 4/1/2015 *Reviewed By:* KLP, 4/1/2015 PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	*Purpose:* (b) (5) *Criteria:* GAGAS 7.03, 7.08-7.31 7.03 Auditors must issue audit reports communicating the results of each completed performance audit. 7.08 Auditors should prepare audit reports that contain (1) the objectives, scope, and methodology of the audit; (2) the audit results, including findings, conclusions, and recommendations, as appropriate; (3) a statement about the auditors' compliance with GAGAS; (4) a summary of the views of responsible officials; and (5) if applicable, the nature of any confidential or sensitive information omitted. 7.09 Auditors should include in the report a description of the audit objectives and the scope and methodology used for addressing the audit objectives. Report users need this information to understand the purpose of the audit, the nature and extent of the audit work performed, the context and perspective regarding what is reported, and any significant limitations in audit objectives, scope, or methodology. 7.10 Audit objectives for performance audits may vary widely. Auditors should communicate audit objectives in the audit report in a clear, specific, neutral, and unbiased manner that includes relevant assumptions. When audit objectives are limited but broader objectives could be inferred by users, auditors should state in the audit report that certain issues were outside the scope of the audit in order to avoid potential misunderstanding.

Summary	Detail
	7.11 Auditors should describe the scope of the work performed and any limitations, including issues that would be relevant to likely users, so that they could reasonably interpret the findings, conclusions, and recommendations in the report without being misled. Auditors should also report any significant constraints imposed on the audit approach by information limitations or scope impairments, including denials or excessive delays of access to certain records or individuals. 7.12 In describing the work conducted to address the audit objectives and support the reported findings and conclusions, auditors should, as applicable, explain the relationship between the population and the items tested; identify organizations, geographic locations, and the period covered; report the kinds and sources of evidence; and explain any significant limitations or uncertainties based on the auditors' overall assessment of the sufficiency and appropriateness of the evidence in the aggregate. 7.13 In reporting audit methodology, auditors should explain how the completed audit work supports the audit objectives, including the evidence gathering and analysis techniques, in sufficient detail to allow knowledgeable users of their reports to understand how the auditors addressed the audit objectives. Auditors may include a description of the procedures performed as part of their assessment of the sufficiency and appropriateness of information used as audit evidence. Auditors should identify significant assumptions made in conducting the audit; describe comparative techniques applied; describe the criteria used; and, when sampling significantly supports the auditors' findings, conclusions, or recommendations, describe the sample design and state why the design was chosen, including whether the results can be projected to the intended population. 7.14 In the audit report, auditors should present sufficient, appropriate evidence to support the findings and conclusions in relation to the audit objectives. Clearly developed findings[164] assist management and oversight officials of the audited entity in understanding the need for taking corrective action. If auditors are able to sufficiently develop the elements of a finding, they should provide recommendations for corrective action if they are significant within the context of the audit objectives. However, the extent to which the elements for a finding are developed depends on the audit

Summary	Detail
	objectives. Thus, a finding or set of findings is complete to the extent that the auditors address the audit objectives. 7.15 Auditors should describe in their report limitations or uncertainties with the reliability or validity of evidence if (1) the evidence is significant to the findings and conclusions within the context of the audit objectives and (2) such disclosure is necessary to avoid misleading the report users about the findings and conclusions. As discussed in paragraphs 6.69 through 6.72, even though the auditors may have some uncertainty about the sufficiency or appropriateness of some of the evidence, they may nonetheless determine that in total there is sufficient, appropriate evidence given the findings and conclusions. Auditors should describe the limitations or uncertainties regarding evidence in conjunction with the findings and conclusions, in addition to describing those limitations or uncertainties as part of the objectives, scope, and methodology. Additionally, this description provides report users with a clear understanding regarding how much responsibility the auditors are taking for the information. 7.16 Auditors should place their findings in perspective by describing the nature and extent of the issues being reported and the extent of the work performed that resulted in the finding. To give the reader a basis for judging the prevalence and consequences of these findings, auditors should, as appropriate, relate the instances identified to the population or the number of cases examined and quantify the results in terms of dollar value, or other measures. If the results cannot be projected, auditors should limit their conclusions appropriately. 7.17 Auditors may provide background information to establish the context for the overall message and to help the reader understand the findings and significance of the issues discussed. Appropriate background information may include information on how programs and operations work; the significance of programs and operations (e.g., dollars, impact, purposes, and past audit work, if relevant); a description of the audited entity's responsibilities; and explanation of terms, organizational structure, and the statutory basis for the program and operations. When reporting on the results of their work, auditors should disclose significant facts relevant to the objectives of their work and known to them which, if not disclosed, could mislead knowledgeable users, misrepresent the results, or conceal significant improper or illegal practices.

Summary	Detail
	7.18 Auditors should also report deficiencies in internal control, instances of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that have occurred or are likely to have occurred and are significant within the context of the audit objectives. 7.19 Auditors should include in the audit report (1) the scope of their work on internal control and (2) any deficiencies in internal control that are significant within the context of the audit objectives and based upon the audit work performed.165 When auditors detect deficiencies in internal control that are not significant to the objectives of the audit but warrant the attention of those charged with governance, they should include those deficiencies either in the report or communicate those deficiencies in writing to audited entity officials. Auditors should refer to that written communication in the audit report if the written communication is separate from the audit report. When auditors detect deficiencies that do warrant the attention of those charged with governance, the determination of whether and how to communicate such deficiencies to audited entity officials is a matter of professional judgment. 7.20 In a performance audit, auditors may conclude that identified deficiencies in internal control that are significant within the context of the audit objectives are the cause of deficient performance of the program or operations being audited. In reporting this type of finding, the internal control deficiency would be described as the cause. **7.21 When auditors conclude, based on sufficient, appropriate evidence, that fraud,166 noncompliance with provisions of laws, regulations, contracts or grant agreements, or abuse167 either has occurred or is likely to have occurred which is significant within the context of the audit objectives, they should report the matter as a finding. Whether a particular act is, in fact, fraud or noncompliance with provisions of laws, regulations, contracts or grant agreements may have to await final determination by a court of law or other adjudicative body.** 7.22 When auditors detect instances of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that are not significant within the context of the audit objectives but warrant

Summary	Detail
	the attention of those charged with governance, they should communicate those findings in writing to audited entity officials. When auditors detect any instances of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that do not warrant the attention of those charged with governance, the auditors' determination of whether and how to communicate such instances to audited entity officials is a matter of professional judgment. 7.23 When fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse either have occurred or are likely to have occurred, auditors may consult with authorities or legal counsel about whether publicly reporting such information would compromise investigative or legal proceedings. Auditors may limit their public reporting to matters that would not compromise those proceedings and, for example, report only on information that is already a part of the public record. 7.24 Auditors should report known or likely fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse directly to parties outside the audited entity in the following two circumstances. a. When entity management fails to satisfy legal or regulatory requirements to report such information to external parties specified in law or regulation, auditors should first communicate the failure to report such information to those charged with governance. If the audited entity still does not report this information to the specified external parties as soon as practicable after the auditors' communication with those charged with governance, then the auditors should report the information directly to the specified external parties. b. When entity management fails to take timely and appropriate steps to respond to known or likely fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that (1) is significant to the findings and conclusions and (2) involves funding received directly or indirectly from a government agency, auditors should first report management's failure to take timely and appropriate steps to those charged with governance. If the audited entity still does not take timely and appropriate steps as soon as practicable after the auditors' communication

Summary	Detail
	with those charged with governance, then the auditors should report the entity's failure to take timely and appropriate steps directly to the funding agency. 7.25 The reporting in paragraph 7.24 is in addition to any legal requirements for the auditor to report such information directly to parties outside the audited entity. Auditors should comply with these requirements even if they have resigned or been dismissed from the audit prior to its completion. Internal audit organizations do not have a duty to report outside the audited entity unless required by law, rule, regulation, or policy.168 7.26 Auditors should obtain sufficient, appropriate evidence, such as confirmation from outside parties, to corroborate assertions by management of the audited entity that it has reported such findings in accordance with laws, regulations, or funding agreements. When auditors are unable to do so, they should report such information directly as discussed in paragraphs 7.24 and 7.25. 7.27 Auditors should report conclusions based on the audit objectives and the audit findings. Report conclusions are logical inferences about the program based on the auditors' findings, not merely a summary of the findings. The strength of the auditors' conclusions depends on the sufficiency and appropriateness of the evidence supporting the findings and the soundness of the logic used to formulate the conclusions. Conclusions are more compelling if they lead to the auditors' recommendations and convince the knowledgeable user of the report that action is necessary. 7.28 Auditors should recommend actions to correct deficiencies and other findings identified during the audit and to improve programs and operations when the potential for improvement in programs, operations, and performance is substantiated by the reported findings and conclusions. Auditors should make recommendations that flow logically from the findings and conclusions, are directed at resolving the cause of identified deficiencies and findings, and clearly state the actions recommended. 7.29 Effective recommendations encourage improvements in the conduct of government programs and operations. Recommendations are effective when they are addressed to parties that have the authority to act and when the recommended actions are specific, practical, cost effective, and

Summary	Detail
	measurable. 7.30 When auditors comply with all applicable GAGAS requirements, they should use the following language, which represents an unmodified GAGAS compliance statement, in the audit report to indicate that they performed the audit in accordance with GAGAS. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. 7.31 When auditors do not comply with all applicable GAGAS requirements, they should include a modified GAGAS compliance statement in the audit report. For performance audits, auditors should use a statement that includes either (1) the language in 7.30, modified to indicate the requirements that were not followed or (2) language that the auditor did not follow GAGAS.170 *Source:* See record of work done. *Scope:* Audit of the Board's diversity and inclusion processes. *Details:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
	Conclusion: See record of work done. No exceptions noted. *Notes:* *Results 4:*
D.1.PRG - Reporting *Procedure Step:* Index and Reference the Draft Report *Type:* Reporting *Assigned To:* *Prepared By:* SMN, 3/31/2015 *Reviewed By:* (None)	*Purpose:* Index and reference all sections of the report. *Criteria:* GAGAS 3.91 3.91 Audit organizations should establish policies and procedures for audit performance, documentation, and reporting that are designed to provide the audit organization with reasonable assurance that audits are performed and reports are issued in accordance with professional standards and legal and regulatory requirements.

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	*Source:* See record of work done *Scope:* Audit of the Board's diversity and inclusion processes. *Details:* *Record of Work Done:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

Summary	Detail
	Conclusion: See record of work done. No exceptions noted. *Notes:* *Results 4:*
D.1.PRG - Reporting *Procedure Step:* Issue the Discussion Draft Report *Type:* Reporting *Assigned To:* KLP *Prepared By:* KLP, 3/9/2015 *Reviewed By:* (None) PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6*	*Purpose:* Document an electronic copy of the draft report as well as the transmittal letter or email. *Criteria:* GAGAS 7.32-7.38 **7.32** Auditors should obtain and report the views of responsible officials of the audited entity concerning the findings, conclusions, and recommendations included in the audit report, as well as any planned corrective actions. 7.33 Providing a draft report with findings for review and comment by responsible officials of the audited entity and others helps the auditors develop a report that is fair, complete, and objective. Including the views of responsible officials results in a report that presents not only the auditors' findings, conclusions, and recommendations, but also the perspectives of the responsible officials of the audited entity and the corrective actions they plan to take. Obtaining the comments in writing is preferred, but oral comments are acceptable. 7.34 When auditors receive written comments from the responsible officials, they should include in their report a copy of the officials' written comments,

Summary	Detail
SCORECARD: *Rating:* *Sample Size:*	or a summary of the comments received. When the responsible officials provide oral comments only, auditors should prepare a summary of the oral comments and provide a copy of the summary to the responsible officials to verify that the comments are accurately stated. 7.35 Auditors should also include in the report an evaluation of the comments, as appropriate. In cases in which the audited entity provides technical comments in addition to its written or oral comments on the report, auditors may disclose in the report that such comments were received. 7.36 Obtaining oral comments may be appropriate when, for example, there is a reporting date critical to meeting a user's needs; auditors have worked closely with the responsible officials throughout the work and the parties are familiar with the findings and issues addressed in the draft report; or the auditors do not expect major disagreements with the findings, conclusions, and recommendations in the draft, or major controversies with regard to the issues discussed in the draft report. 7.37 When the audited entity's comments are inconsistent or in conflict with the findings, conclusions, or recommendations in the draft report, or when planned corrective actions do not adequately address the auditors' recommendations, the auditors should evaluate the validity of the audited entity's comments. If the auditors disagree with the comments, they should explain in the report their reasons for disagreement. Conversely, the auditors should modify their report as necessary if they find the comments valid and supported with sufficient, appropriate evidence. 7.38 If the audited entity refuses to provide comments or is unable to provide comments within a reasonable period of time, the auditors may issue the report without receiving comments from the audited entity. In such cases, the auditors should indicate in the report that the audited entity did not provide comments. *Source:* OIG Audit Team the Board's Diversity a

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Scope: The Board's Diversity and Inclusion Processes CY 2011- CY 2013 an d any changes made during FY 2014. *Details:* (b) (5) *Conclusion:* This work is in compliance with GAGAS standards and the OIG policies and procedures. *Notes:* *Results 4:*
D.1.PRG - Reporting ***Procedure Step:*** Issue the Draft Report for Comment	*Purpose:* Document an electronic copy of the draft report as well as the transmittal letter or email.

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
Type:	Reporting	
Assigned To:		*Criteria:*
Prepared By:	SMN, 3/31/2015	GAGAS 7.32-7.38
Reviewed By:	(None)	**7.32 Auditors should obtain and report the views of responsible officials of the audited entity concerning the findings, conclusions, and recommendations included in the audit report, as well as any planned corrective actions.**
PROPERTIES:		
Location:		7.33 Providing a draft report with findings for review and comment by responsible officials of the audited entity and others helps the auditors develop a report that is fair, complete, and objective. Including the views of responsible officials results in a report that presents not only the auditors' findings, conclusions, and recommendations, but also the perspectives of the responsible officials of the audited entity and the corrective actions they plan to take. Obtaining the comments in writing is preferred, but oral comments are acceptable.
Frequency:		7.34 When auditors receive written comments from the responsible officials, they should include in their report a copy of the officials' written comments, or a summary of the comments received. When the responsible officials provide oral comments only, auditors should prepare a summary of the oral comments and provide a copy of the summary to the responsible officials to verify that the comments are accurately stated.
Category 4:		7.35 Auditors should also include in the report an evaluation of the comments, as appropriate. In cases in which the audited entity provides technical comments in addition to its written or oral comments on the report, auditors may disclose in the report that such comments were received.
User Category:		7.36 Obtaining oral comments may be appropriate when, for example, there is a reporting date critical to meeting a user's needs; auditors have worked closely with the responsible officials throughout the work and the parties are familiar with the findings and issues addressed in the draft report; or the auditors do not expect major disagreements with the findings, conclusions, and recommendations in the draft, or major controversies with regard to the issues discussed in the draft report.
Category 5		
Category 6		
SCORECARD:		
Rating:		
Sample Size:		

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	7.37 When the audited entity's comments are inconsistent or in conflict with the findings, conclusions, or recommendations in the draft report, or when planned corrective actions do not adequately address the auditors' recommendations, the auditors should evaluate the validity of the audited entity's comments. If the auditors disagree with the comments, they should explain in the report their reasons for disagreement. Conversely, the auditors should modify their report as necessary if they find the comments valid and supported with sufficient, appropriate evidence. 7.38 If the audited entity refuses to provide comments or is unable to provide comments within a reasonable period of time, the auditors may issue the report without receiving comments from the audited entity. In such cases, the auditors should indicate in the report that the audited entity did not provide comments. *Source:* OIG Management *Scope:* Audit of the Board's Diversity and Inclusion Processes *Details:* *Record of Work Done:* (b) (5)

Summary	Detail
	Conclusion: This workstep complies with GAGAS and the OIG policies and procedures. See record of work done. No exceptions noted. *Notes:* *Results 4:*
D.1.PRG - Reporting *Procedure Step:* Obtain and Evaluate Management's Response *Type:* Reporting *Assigned To:* *Prepared By:* SMN, 3/31/2015 *Reviewed By:* (None) PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:*	*Purpose:* Document a copy of the signed response from Board/CFPB management as well as the OIG "Analysis of Comments." Index and reference the analysis and any changes to the report based on management's comments, as appropriate. *Criteria:* GAGAS 7.32-7.38 **7.32 Auditors should obtain and report the views of responsible officials of the audited entity concerning the findings, conclusions, and recommendations included in the audit report, as well as any planned corrective actions.** 7.33 Providing a draft report with findings for review and comment by responsible officials of the audited entity and others helps the auditors develop a report that is fair, complete, and objective. Including the views of responsible officials results in a report that presents not only the auditors' findings, conclusions, and recommendations, but also the perspectives of the responsible officials of the audited entity and the corrective actions they plan to take. Obtaining the comments in writing is preferred, but oral

Summary	Detail
Category 5 *Category 6* SCORECARD: *Rating:* *Sample Size:*	comments are acceptable. 7.34 When auditors receive written comments from the responsible officials, they should include in their report a copy of the officials' written comments, or a summary of the comments received. When the responsible officials provide oral comments only, auditors should prepare a summary of the oral comments and provide a copy of the summary to the responsible officials to verify that the comments are accurately stated. 7.35 Auditors should also include in the report an evaluation of the comments, as appropriate. In cases in which the audited entity provides technical comments in addition to its written or oral comments on the report, auditors may disclose in the report that such comments were received. 7.36 Obtaining oral comments may be appropriate when, for example, there is a reporting date critical to meeting a user's needs; auditors have worked closely with the responsible officials throughout the work and the parties are familiar with the findings and issues addressed in the draft report; or the auditors do not expect major disagreements with the findings, conclusions, and recommendations in the draft, or major controversies with regard to the issues discussed in the draft report. 7.37 When the audited entity's comments are inconsistent or in conflict with the findings, conclusions, or recommendations in the draft report, or when planned corrective actions do not adequately address the auditors' recommendations, the auditors should evaluate the validity of the audited entity's comments. If the auditors disagree with the comments, they should explain in the report their reasons for disagreement. Conversely, the auditors should modify their report as necessary if they find the comments valid and supported with sufficient, appropriate evidence. 7.38 If the audited entity refuses to provide comments or is unable to provide comments within a reasonable period of time, the auditors may issue the report without receiving comments from the audited entity. In such cases, the auditors should indicate in the report that the audited entity did not provide comments. *Source:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Board response signed by Don Hammondm, COO. *Scope:* OIG analysis of Board response to official draft. *Details:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
	Notes: *Results 4:*

Summary		Detail
D.1.PRG - Reporting		*Purpose:* Document an electronic copy of the final, signed report.
Procedure Step:	Issue the Final Report	
Type:	Reporting	*Criteria:* GAGAS 7.03, 7.08-7.31 7.03 Auditors must issue audit reports communicating the results of each completed performance audit.
Assigned To:		
Prepared By:	SMN, 3/31/2015	
Reviewed By:	(None)	7.08 Auditors should prepare audit reports that contain (1) the objectives, scope, and methodology of the audit; (2) the audit results, including findings, conclusions, and recommendations, as appropriate; (3) a statement about the auditors' compliance with GAGAS; (4) a summary of the views of responsible officials; and (5) if applicable, the nature of any confidential or sensitive information omitted. 7.09 Auditors should include in the report a description of the audit objectives and the scope and methodology used for addressing the audit objectives. Report users need this information to understand the purpose of the audit, the nature and extent of the audit work performed, the context and perspective regarding what is reported, and any significant limitations in audit objectives, scope, or methodology. 7.10 Audit objectives for performance audits may vary widely. Auditors should communicate audit objectives in the audit report in a clear, specific, neutral, and unbiased manner that includes relevant assumptions. When audit objectives are limited but broader objectives could be inferred by users, auditors should state in the audit report that certain issues were outside the scope of the audit in order to avoid potential misunderstanding. 7.11 Auditors should describe the scope of the work performed and any limitations, including issues that would be relevant to likely users, so that they could reasonably interpret the findings, conclusions, and recommendations in the report without being misled. Auditors should also report any significant constraints imposed on the audit approach by information limitations or scope impairments, including denials or excessive delays of access to certain records or individuals.
PROPERTIES:		
Location:		
Frequency:		
Category 4:		
User Category:		
Category 5		
Category 6		
SCORECARD:		
Rating:		
Sample Size:		

Summary	Detail
	7.12 In describing the work conducted to address the audit objectives and support the reported findings and conclusions, auditors should, as applicable, explain the relationship between the population and the items tested; identify organizations, geographic locations, and the period covered; report the kinds and sources of evidence; and explain any significant limitations or uncertainties based on the auditors' overall assessment of the sufficiency and appropriateness of the evidence in the aggregate. 7.13 In reporting audit methodology, auditors should explain how the completed audit work supports the audit objectives, including the evidence gathering and analysis techniques, in sufficient detail to allow knowledgeable users of their reports to understand how the auditors addressed the audit objectives. Auditors may include a description of the procedures performed as part of their assessment of the sufficiency and appropriateness of information used as audit evidence. Auditors should identify significant assumptions made in conducting the audit; describe comparative techniques applied; describe the criteria used; and, when sampling significantly supports the auditors' findings, conclusions, or recommendations, describe the sample design and state why the design was chosen, including whether the results can be projected to the intended population. 7.14 In the audit report, auditors should present sufficient, appropriate evidence to support the findings and conclusions in relation to the audit objectives. Clearly developed findings[164] assist management and oversight officials of the audited entity in understanding the need for taking corrective action. If auditors are able to sufficiently develop the elements of a finding, they should provide recommendations for corrective action if they are significant within the context of the audit objectives. However, the extent to which the elements for a finding are developed depends on the audit objectives. Thus, a finding or set of findings is complete to the extent that the auditors address the audit objectives. 7.15 Auditors should describe in their report limitations or uncertainties with the reliability or validity of evidence if (1) the evidence is significant to the findings and conclusions within the context of the audit objectives and (2) such disclosure is necessary to avoid misleading the report users about the findings and conclusions. As discussed in paragraphs 6.69 through 6.72, even though the auditors may have

Summary	Detail
	some uncertainty about the sufficiency or appropriateness of some of the evidence, they may nonetheless determine that in total there is sufficient, appropriate evidence given the findings and conclusions. Auditors should describe the limitations or uncertainties regarding evidence in conjunction with the findings and conclusions, in addition to describing those limitations or uncertainties as part of the objectives, scope, and methodology. Additionally, this description provides report users with a clear understanding regarding how much responsibility the auditors are taking for the information. 7.16 Auditors should place their findings in perspective by describing the nature and extent of the issues being reported and the extent of the work performed that resulted in the finding. To give the reader a basis for judging the prevalence and consequences of these findings, auditors should, as appropriate, relate the instances identified to the population or the number of cases examined and quantify the results in terms of dollar value, or other measures. If the results cannot be projected, auditors should limit their conclusions appropriately. 7.17 Auditors may provide background information to establish the context for the overall message and to help the reader understand the findings and significance of the issues discussed. Appropriate background information may include information on how programs and operations work; the significance of programs and operations (e.g., dollars, impact, purposes, and past audit work, if relevant); a description of the audited entity's responsibilities; and explanation of terms, organizational structure, and the statutory basis for the program and operations. When reporting on the results of their work, auditors should disclose significant facts relevant to the objectives of their work and known to them which, if not disclosed, could mislead knowledgeable users, misrepresent the results, or conceal significant improper or illegal practices. 7.18 Auditors should also report deficiencies in internal control, instances of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that have occurred or are likely to have occurred and are significant within the context of the audit objectives. 7.19 Auditors should include in the audit report (1) the scope of their work on internal control and (2) any deficiencies in internal control that are significant within the context of the audit objectives and based upon the audit work performed.165 When auditors detect deficiencies in internal control that are not significant to the objectives of the audit but warrant the

Summary	Detail
	attention of those charged with governance, they should include those deficiencies either in the report or communicate those deficiencies in writing to audited entity officials. Auditors should refer to that written communication in the audit report if the written communication is separate from the audit report. When auditors detect deficiencies that do warrant the attention of those charged with governance, the determination of whether and how to communicate such deficiencies to audited entity officials is a matter of professional judgment. 7.20 In a performance audit, auditors may conclude that identified deficiencies in internal control that are significant within the context of the audit objectives are the cause of deficient performance of the program or operations being audited. In reporting this type of finding, the internal control deficiency would be described as the cause. **7.21 When auditors conclude, based on sufficient, appropriate evidence, that fraud,166 noncompliance with provisions of laws, regulations, contracts or grant agreements, or abuse167 either has occurred or is likely to have occurred which is significant within the context of the audit objectives, they should report the matter as a finding. Whether a particular act is, in fact, fraud or noncompliance with provisions of laws, regulations, contracts or grant agreements may have to await final determination by a court of law or other adjudicative body.** 7.22 When auditors detect instances of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that are not significant within the context of the audit objectives but warrant the attention of those charged with governance, they should communicate those findings in writing to audited entity officials. When auditors detect any instances of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that do not warrant the attention of those charged with governance, the auditors' determination of whether and how to communicate such instances to audited entity officials is a matter of professional judgment. 7.23 When fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse either have occurred or are likely to have occurred, auditors may consult with authorities or legal counsel about whether publicly

Summary	Detail
	reporting such information would compromise investigative or legal proceedings. Auditors may limit their public reporting to matters that would not compromise those proceedings and, for example, report only on information that is already a part of the public record. 7.24 Auditors should report known or likely fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse directly to parties outside the audited entity in the following two circumstances. a. When entity management fails to satisfy legal or regulatory requirements to report such information to external parties specified in law or regulation, auditors should first communicate the failure to report such information to those charged with governance. If the audited entity still does not report this information to the specified external parties as soon as practicable after the auditors' communication with those charged with governance, then the auditors should report the information directly to the specified external parties. b. When entity management fails to take timely and appropriate steps to respond to known or likely fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that (1) is significant to the findings and conclusions and (2) involves funding received directly or indirectly from a government agency, auditors should first report management's failure to take timely and appropriate steps to those charged with governance. If the audited entity still does not take timely and appropriate steps as soon as practicable after the auditors' communication with those charged with governance, then the auditors should report the entity's failure to take timely and appropriate steps directly to the funding agency. 7.25 The reporting in paragraph 7.24 is in addition to any legal requirements for the auditor to report such information directly to parties outside the audited entity. Auditors should comply with these requirements even if they have resigned or been dismissed from the audit prior to its completion. Internal audit organizations do not have a duty to report outside the audited entity unless required by law, rule, regulation, or policy.168 7.26 Auditors should obtain sufficient, appropriate evidence, such as confirmation

Summary	Detail
	from outside parties, to corroborate assertions by management of the audited entity that it has reported such findings in accordance with laws, regulations, or funding agreements. When auditors are unable to do so, they should report such information directly as discussed in paragraphs 7.24 and 7.25. 7.27 Auditors should report conclusions based on the audit objectives and the audit findings. Report conclusions are logical inferences about the program based on the auditors' findings, not merely a summary of the findings. The strength of the auditors' conclusions depends on the sufficiency and appropriateness of the evidence supporting the findings and the soundness of the logic used to formulate the conclusions. Conclusions are more compelling if they lead to the auditors' recommendations and convince the knowledgeable user of the report that action is necessary. 7.28 Auditors should recommend actions to correct deficiencies and other findings identified during the audit and to improve programs and operations when the potential for improvement in programs, operations, and performance is substantiated by the reported findings and conclusions. Auditors should make recommendations that flow logically from the findings and conclusions, are directed at resolving the cause of identified deficiencies and findings, and clearly state the actions recommended. 7.29 Effective recommendations encourage improvements in the conduct of government programs and operations. Recommendations are effective when they are addressed to parties that have the authority to act and when the recommended actions are specific, practical, cost effective, and measurable. 7.30 When auditors comply with all applicable GAGAS requirements, they should use the following language, which represents an unmodified GAGAS compliance statement, in the audit report to indicate that they performed the audit in accordance with GAGAS. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our

Summary	Detail
	audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. 7.31 When auditors do not comply with all applicable GAGAS requirements, they should include a modified GAGAS compliance statement in the audit report. For performance audits, auditors should use a statement that includes either (1) the language in 7.30, modified to indicate the requirements that were not followed or (2) language that the auditor did not follow GAGAS.170 *Source:* Melissa Heist, Associate Inspector General for Audits and Evaluations *Scope:* Audit of the Board's diversity and inclusion processes. *Details:* *Record of Work Done:* Melissa Heist, Associate Inspector General for Audits and Evaluations issued the final report on 03/31/15. See D.1.42 and D.1.43. *Conclusion:* See record of work done. No exceptions noted. *Notes:*

Summary	Detail
	Results 4:
D.1.PRG - Reporting *Procedure Step:* Prepare Semi-Annual Report Narrative *Type:* Reporting *Assigned To:* KLP *Prepared By:* KLP, 4/1/2015 *Reviewed By:* (None) PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	*Purpose:* Document the text for the semi-annual report. *Criteria:* FRB/CFPB OIG Policy *Source:* Kimberly Perteet, Senior Auditor *Scope:* Audit of the Board's diversity and inclusion processes. *Details:* *Record of Work Done:* (b) (5) [redacted] *Conclusion:* Not applicable for team. See record of work done. *Notes:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Results 4:
D.1.PRG - Reporting *Procedure Step:* Send the Final Report to OIG IT Staff *Type:* Reporting *Assigned To:* SMN *Prepared By:* SMN, 4/1/2015 *Reviewed By:* KLP, 4/7/2015 PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	*Purpose:* Send the final report to OIG IT Staff for inclusion on the OIG webpage. *Criteria:* FRB/CFPB OIG Policy *Source:* Laura Polly, Supervisory Writer-Editor *Scope:* Audit of the Board's diversity and inclusion processes. *Details:* *Record of Work Done:* (b) (5) *Conclusion:* See record of work done. No exceptions noted.

Summary	Detail
	Notes: *Results 4:*
D.1.PRG - Reporting *Procedure Step:* Hard Copy Working Papers *Type:* Reporting *Assigned To:* *Prepared By:* SMN, 3/23/2015 *Reviewed By:* (None) PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	*Purpose:* Collect and provide all hardcopy workpapers to the OIG administrative assistant for filing. *Criteria:* GAGAS 6.79-6.85 6.79 Auditors must prepare audit documentation related to planning, conducting, and reporting for each audit. Auditors should prepare audit documentation in sufficient detail to enable an experienced auditor, having no previous connection to the audit, to understand from the audit documentation the nature, timing, extent, and results of audit procedures performed, the audit evidence obtained and its source and the conclusions reached, including evidence that supports the auditors' significant judgments and conclusions. An experienced auditor means an individual (whether internal or external to the audit organization) who possesses the competencies and skills that would have enabled him or her to conduct the performance audit. These competencies and skills include an understanding of (1) the performance audit processes, (2) GAGAS and applicable legal and regulatory requirements, (3) the subject matter associated with achieving the audit objectives, and (4) issues related to the audited entity's environment. 6.80 Auditors should prepare audit documentation that contains evidence that supports the findings, conclusions, and recommendations before they issue their report. 6.81 Auditors should design the form and content of audit documentation to meet the circumstances of the particular audit. The audit documentation constitutes the principal record of the work that the auditors have performed in accordance with

Summary	Detail
	standards and the conclusions that the auditors have reached. The quantity, type, and content of audit documentation are a matter of the auditors' professional judgment. 6.82 Audit documentation is an essential element of audit quality. The process of preparing and reviewing audit documentation contributes to the quality of an audit. Audit documentation serves to (1) provide the principal support for the auditors' report, (2) aid auditors in conducting and supervising the audit, and (3) allow for the review of audit quality. 6.83 Auditors should document159 the following: a. the objectives, scope, and methodology of the audit; b. the work performed and evidence obtained to support significant judgments and conclusions, including descriptions of transactions and records examined (for example, by listing file numbers, case numbers, or other means of identifying specific documents examined, but copies of documents examined or detailed listings of information from those documents are not required); and c. supervisory review, before the audit report is issued, of the evidence that supports the findings, conclusions, and recommendations contained in the audit report. 6.84 When auditors do not comply with applicable GAGAS requirements due to law, regulation, scope limitations, restrictions on access to records, or other issues impacting the audit, the auditors should document the departure from the GAGAS requirements and the impact on the audit and on the auditors' conclusions. This applies to departures from unconditional requirements and from presumptively mandatory requirements when alternative procedures performed in the circumstances were not sufficient to achieve the objectives of the standard.160 6.85 Underlying GAGAS audits is the premise that audit organizations in federal, state, and local governments and public accounting firms engaged to perform audits in accordance with GAGAS cooperate in auditing programs of common interest so that auditors may use others' work and avoid duplication of efforts. Subject to applicable laws and regulations, auditors should make appropriate individuals, as well as audit documentation, available upon request and in a timely manner to other

Summary	Detail
	auditors or reviewers to satisfy these objectives. The use of auditors' work by other auditors may be facilitated by contractual arrangements for GAGAS audits that provide for full and timely access to appropriate individuals, as well as audit documentation. *Source:* Hardcopy workpapers related to the audit. *Scope:* Audit of the Board's diversity and inclusion processes. *Details:* *Record of Work Done:* No hardcopy workpapers were retained for this audit. *Conclusion:* See record of work done. No exceptions noted. *Notes:* *Results 4:*
D.1.PRG - Reporting	*Purpose:* Complete the referencing checklist.

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
Procedure Step:	Complete Referencing Checklist	
Type:	Reporting	*Criteria:* FRB/CFPB OIG Policy
Assigned To:		
Prepared By:	KLP, 4/7/2015	
Reviewed By:	(None)	*Source:* See referencing checklist procedure steps and related workpapers.
PROPERTIES:		*Scope:* Audit of the Board's diversity and inclusion processes.
Location:		
Frequency:		
Category 4:		*Details:*
User Category:		
Category 5		*Record of Work Done:* See completed referencing checklists: 1. Project Leader - C.4.PRG 2. Project Manager - C.5.PRG 3. Referencer - C.6.PRG
Category 6		
SCORECARD:		
Rating:		*Conclusion:* Referencing checklists are complete. Links in record of work done.
Sample Size:		
		Notes:
		Results 4:

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
D.1.PRG - Reporting *Procedure Step:* Follow-up *Type:* *Assigned To:* KLP *Prepared By:* KLP, 4/1/2015 *Reviewed By:* (None) **PROPERTIES:** *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* **SCORECARD:** *Rating:* *Sample Size:*	*Purpose:* (b) (5) *Criteria:* FRB/CFPB OIG Policy *Source:* The Board's report (#2015-MO-B-006) titled *The Board Can Enhance Its Diversity and Inclusion Efforts* *Scope:* Audit of the Board's diversity and inclusion processes. *Details:* (b) (5) *Conclusion:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
	Results 4:

The Board Can Enhance Its Diversity and Inclusion Efforts

Profile

General

Code: 2015-MO-B-006

Name: The Board Can Enhance Its Diversity and Inclusion Efforts

Audit Plan: 2014

Entities:

Name	*Breadcrumb*
Federal Reserve Board (FRB)	Organizations > Federal Reserve Board (FRB)

Unit:

Group: Audits & Evaluations

Type: Management & Operations

Location: FRB

Scope: Other

Origin:

Team

Lead: Kimberly Perteet

Manager:

Staff Type:

The Board Can Enhance Its Diversity and Inclusion Efforts

Schedule

(b) (5)

(b) (5)

Actual Start Date: 4/4/2014

Actual End Date:

(b) (5)

Actual Hours: 0

(b) (5)

Actual Resource Costs:

(b) (5)

Actual External Costs: $0.00

(b) (5)

Actual Expenses:

The Board Can Enhance Its Diversity and Inclusion Efforts

Risk

Risk:

Total Risk Score:	0
Inherent Risk:	0
Residual Risk:	0

Objective(s)

2014 Congressional Request on the Board’s Personnel Practices in Team Mate

Background

Planning

Scope

General

The Board Can Enhance Its Diversity and Inclusion Efforts

Contact

Primary

Other

Summary

Final Risk:

Opinion:

Cost Savings: $0.00

Cost Avoidance: $0.00

Rating:

Summary:

Tracking

(b) (5)

Actual Draft Date: 3/19/2015

(b) (5)

Actual Response Date: 3/19/2015

The Board Can Enhance Its Diversity and Inclusion Efforts

(b) (5)

Actual Issue Date: 3/31/2015

Milestones

Category	(b) (5)	Act. Date	Comments
Blank			
Entrance Meeting		5/12/2014	
Midpoint Meeting		9/3/2014	
Project Design Meeting		5/12/2014	
Message Development Meeting		10/2/2014	
AIG-Approved Draft Report		3/4/2015	
Discussion Draft Report		3/4/2015	
Exit Meeting		3/13/2015	
Formal Draft Report		3/19/2015	
Final Report		3/31/2015	

Custom Properties

Custom Property Name	Value

Procedures

Summary		Detail
B.2.PRG - Scoping		*Purpose:*
Procedure Step:	Phone Conference with Dave Harmon	The purpose of the meeting was to conduct an initial meeting with the Board's Human Capital Officer and the Human Capital Function to gather information regarding their main roles and responsibilities.
5/20/2014		
Type:		*Criteria:*
Assigned To:	BPM	GAGAS 6.47-6.49
Prepared By:	BPM, 7/11/2014	6.47 Auditors should communicate an overview of the objectives, scope, and methodology and the timing of the performance audit and planned reporting (including any potential restrictions on the report), unless doing so could significantly impair the auditors' ability to obtain sufficient, appropriate evidence to address the audit objectives, such as when the auditors plan to conduct unannounced cash counts or perform procedures related to indications of fraud. Auditors should communicate with the following parties, as applicable:
Reviewed By:	(None)	a. management of the audited entity, including those with sufficient authority and responsibility to implement corrective action in the program or activity being audited;
PROPERTIES:		b. those charged with governance;146
Location:		c. the individuals contracting for or requesting audit services, such as contracting officials or grantees; and
Frequency:		d. the cognizant legislative committee, when auditors perform the audit pursuant to a law or regulation or they conduct the work for the legislative committee that has oversight of the audited entity.
Category 4:		6.48 In those situations where there is not a single individual or group that both oversees the strategic direction of the audited entity and the fulfillment of its accountability obligations or in other situations where the identity of those charged with governance is not clearly evident, auditors should document the process followed and conclusions reached for identifying the appropriate individuals to receive the required auditor communications.
User Category:		6.49 Determining the form, content, and frequency of the communication is
Category 5		
Category 6		
SCORECARD:		
Rating:		
Sample Size:		

Summary	Detail
	a matter of professional judgment, although written communication is preferred. Auditors may use an engagement letter to communicate the information. Auditors should document this communication. *Source:* Board: • Dave Harmon, Deputy Director & CHO • Lewis Andrews, Manager, HR Analytics OIG: • Anna Saez, Manager, OIG • Kim Perteet, Senior Auditor, OIG • Brian Murphy, Auditor, OIG • Brandon Lee, Auditor, OIG *Scope:* The scope of the meeting was general conversation where the OIG asked questions in order to gain clarity around what kind of high level responsibilities the Board's Human Resources function plays with regard to diversity in the workforce. The meeting was held on 5/20/2014. *Details:* *Record of Work Done:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted] *Notes:* *Results 4:*
B.2.PRG - Scoping ***Procedure Step:*** Meeting with Board OMWI 5/22/2014 ***Type:*** ***Assigned To:*** BPM ***Prepared By:*** BPM, 7/11/2014 ***Reviewed By:*** (None)	*Purpose:* The purpose of the meeting was to conduct an initial meeting with the Board's Office of Diversity and Inclusion/Minority and Women Inclusion to gather information regarding their main roles and responsibilities. *Criteria:* GAGAS 6.47-6.49 6.47 Auditors should communicate an overview of the objectives, scope, and methodology and the timing of the performance audit and planned reporting (including any potential restrictions on the report), unless doing so could significantly impair the auditors' ability to obtain sufficient, appropriate evidence to address the audit objectives, such as when the auditors plan to conduct unannounced cash counts or perform procedures related to indications of fraud.

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	Auditors should communicate with the following parties, as applicable: a. management of the audited entity, including those with sufficient authority and responsibility to implement corrective action in the program or activity being audited; b. those charged with governance;146 c. the individuals contracting for or requesting audit services, such as contracting officials or grantees; and d. the cognizant legislative committee, when auditors perform the audit pursuant to a law or regulation or they conduct the work for the legislative committee that has oversight of the audited entity. 6.48 In those situations where there is not a single individual or group that both oversees the strategic direction of the audited entity and the fulfillment of its accountability obligations or in other situations where the identity of those charged with governance is not clearly evident, auditors should document the process followed and conclusions reached for identifying the appropriate individuals to receive the required auditor communications. 6.49 Determining the form, content, and frequency of the communication is a matter of professional judgment, although written communication is preferred. Auditors may use an engagement letter to communicate the information. Auditors should document this communication. *Source:* Attendees: OD&I: Sheila Clark, Program Director, Office of Diversity and Inclusion Johanna Bruce, Diversity/EEO Specialist OIG: Anna Saez, Senior OIG Manager Kim Perteet, Project Lead Twyla Tatum, Auditor Note: Ms. Tatum's attendance was to reduce project overlap with another OIG engagement. Brandon Lee, Auditor Brian Murphy, Auditor *Scope:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted]
	Details:
	(b) (5) [redacted]

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted] *Notes:* *Results 4:*
B.2.PRG - Scoping *Procedure Step:* Meeting with BS&R 6/10/2014 *Type:* *Assigned To:* BML *Prepared By:* SMN, 10/8/2014	*Purpose:* The purpose of the meeting was to gain an understanding of the employee survey completed by BS&R. *Criteria:* GAGAS 6.47-6.49 6.47 Auditors should communicate an overview of the objectives, scope,

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
Reviewed By: (None) PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	and methodology and the timing of the performance audit and planned reporting (including any potential restrictions on the report), unless doing so could significantly impair the auditors' ability to obtain sufficient, appropriate evidence to address the audit objectives, such as when the auditors plan to conduct unannounced cash counts or perform procedures related to indications of fraud. Auditors should communicate with the following parties, as applicable: a. management of the audited entity, including those with sufficient authority and responsibility to implement corrective action in the program or activity being audited; b. those charged with governance;146 c. the individuals contracting for or requesting audit services, such as contracting officials or grantees; and d. the cognizant legislative committee, when auditors perform the audit pursuant to a law or regulation or they conduct the work for the legislative committee that has oversight of the audited entity. 6.48 In those situations where there is not a single individual or group that both oversees the strategic direction of the audited entity and the fulfillment of its accountability obligations or in other situations where the identity of those charged with governance is not clearly evident, auditors should document the process followed and conclusions reached for identifying the appropriate individuals to receive the required auditor communications. 6.49 Determining the form, content, and frequency of the communication is a matter of professional judgment, although written communication is preferred. Auditors may use an engagement letter to communicate the information. Auditors should document this communication. *Source:* BS&R: Tameika Pope, Assistant Director OIG Participants: Kimberly Perteet, Sr. Auditor and Project Leader Brandon Lee, Auditor

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Scope: The scope of the meeting was general conversation where the OIG asked questions in order to gain an understanding of the survey conducted by BS&R. The meeting was held on 6/10/2014. *Details:* *Record of Work Done:* Interview with BSR *Conclusion:* (b) (5)

Summary	Detail
	(b) (5) *Notes:* *Results 4:*
B.2.PRG - Scoping *Procedure Step:* Meeting with RBOPS 6/11/2014 *Type:* *Assigned To:* SMN *Prepared By:* SMN, 7/10/2014 *Reviewed By:* (None) PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD:	*Purpose:* The purpose of the meeting was to gain an understanding of the employee survey completed by RBOPS. *Criteria:* GAGAS 6.47-6.49 6.47 Auditors should communicate an overview of the objectives, scope, and methodology and the timing of the performance audit and planned reporting (including any potential restrictions on the report), unless doing so could significantly impair the auditors' ability to obtain sufficient, appropriate evidence to address the audit objectives, such as when the auditors plan to conduct unannounced cash counts or perform procedures related to indications of fraud. Auditors should communicate with the following parties, as applicable: a. management of the audited entity, including those with sufficient authority and responsibility to implement corrective action in the program or activity being audited; b. those charged with governance;146 c. the individuals contracting for or requesting audit services, such as contracting officials or grantees; and d. the cognizant legislative committee, when auditors perform the audit pursuant to a law or regulation or they conduct the work for the legislative committee that has oversight of the audited entity. 6.48 In those situations where there is not a single individual or group that

Summary	Detail
Rating: *Sample Size:*	both oversees the strategic direction of the audited entity and the fulfillment of its accountability obligations or in other situations where the identity of those charged with governance is not clearly evident, auditors should document the process followed and conclusions reached for identifying the appropriate individuals to receive the required auditor communications. 6.49 Determining the form, content, and frequency of the communication is a matter of professional judgment, although written communication is preferred. Auditors may use an engagement letter to communicate the information. Auditors should document this communication. *Source:* RBOPS Participants: Lisa Hoskins, Deputy Associate Director of RBOPS Jennifer Chang, Manager of Admin. & Special Projects OIG Participants: Kimberly Perteet, Sr. Auditor and Project Leader Sean Newman, Auditor Brandon Lee, Auditor *Scope:* The scope of the meeting was general conversation where the OIG asked questions in order to gain an understanding of the survey conducted by RBOPS. The meeting was held on 6/11/2014. *Details:* *Record of Work Done:* 06_11_14 Write-Up for Meeting with RBOPS

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Conclusion: (b) (5) [redacted]
	Notes: *Results 4:*
B.2.PRG - Scoping ***Procedure Step:*** Meeting with Employee Relations	*Purpose:* The purpose of the meeting was to gain an understanding of the roles and responsibilties completed by Employee Relations.

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
6/12/2014		*Criteria:*
Type:		<P style="MARGIN-TOP: 0px; DIRECTION: ltr; MARGIN-BOTTOM: 0px"></P>
Assigned To:	SMN	<P>GAGAS 6.47-6.49
Prepared By:	SMN, 10/8/2014	<P>6.47 Auditors should communicate an overview of the objectives, scope, and methodology and the timing of the performance audit and planned reporting (including any potential restrictions on the report), unless doing so could significantly impair the auditors' ability to obtain sufficient, appropriate evidence to address the audit objectives, such as when the auditors plan to conduct unannounced cash counts or perform procedures related to indications of fraud. Auditors should communicate with the following parties, as applicable:
Reviewed By:	(None)	<P>a. management of the audited entity, including those with sufficient authority and responsibility to implement corrective action in the program or activity being audited;
PROPERTIES:		<P>b. those charged with governance;146
Location:		<P>c. the individuals contracting for or requesting audit services, such as contracting officials or grantees; and
Frequency:		<P>d. the cognizant legislative committee, when auditors perform the audit pursuant to a law or regulation or they conduct the work for the legislative committee that has oversight of the audited entity.
Category 4:		<P>6.48 In those situations where there is not a single individual or group that both oversees the strategic direction of the audited entity and the fulfillment of its accountability obligations or in other situations where the identity of those charged with governance is not clearly evident, auditors should document the process followed and conclusions reached for identifying the appropriate individuals to receive the required auditor communications.
User Category:		
Category 5		
Category 6		
SCORECARD:		
Rating:		
Sample Size:		

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	<P>6.49 Determining the form, content, and frequency of the communication is a matter of professional judgment, although written communication is preferred. Auditors may use an engagement letter to communicate the information. Auditors should document this communication. <P> </P></SPAN> *Source:* ER Participants: Allison Dichoso, Employee Relations Supervisor Kevin May, Sr. Employee Relations Specialist Keisha Hargo, Sr. Employee Relations Specialist OIG Participants: Kimberly Perteet, Sr. Auditor and Project Leader Sean Newman, Auditor Brandon Lee, Auditor (b) (5) *Details:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
	Conclusion: (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Notes: *Results 4:*
B.2.PRG - Scoping *Procedure Step:* Meeting with HR Analytics 6/24/2014 *Type:* *Assigned To:* SMN *Prepared By:* SMN, 2/10/2015 *Reviewed By:* (None) **PROPERTIES:** *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* **SCORECARD:** *Rating:*	*Purpose:* (b) (5) *Criteria:* <P style="MARGIN-TOP: 0px; DIRECTION: ltr; MARGIN-BOTTOM: 0px"></P> <P>GAGAS 6.47-6.49 <P>6.47 Auditors should communicate an overview of the objectives, scope, and methodology and the timing of the performance audit and planned reporting (including any potential restrictions on the report), unless doing so could significantly impair the auditors' ability to obtain sufficient, appropriate evidence to address the audit objectives, such as when the auditors plan to conduct unannounced cash counts or perform procedures related to indications of fraud. Auditors should communicate with the following parties, as applicable: <P>a. management of the audited entity, including those with sufficient authority and responsibility to implement corrective action in the program or activity being audited; <P>b. those charged with governance;146 <P>c. the individuals contracting for or requesting audit services, such as contracting officials or grantees; and

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
Sample Size:	<P>d. the cognizant legislative committee, when auditors perform the audit pursuant to a law or regulation or they conduct the work for the legislative committee that has oversight of the audited entity. <P>6.48 In those situations where there is not a single individual or group that both oversees the strategic direction of the audited entity and the fulfillment of its accountability obligations or in other situations where the identity of those charged with governance is not clearly evident, auditors should document the process followed and conclusions reached for identifying the appropriate individuals to receive the required auditor communications. <P>6.49 Determining the form, content, and frequency of the communication is a matter of professional judgment, although written communication is preferred. Auditors may use an engagement letter to communicate the information. Auditors should document this communication. <P> </P></P></SPAN> *Source:* HR Analytics Participants: Lewis Andrews, Manager of HR Analytics Jack Martin, Sr. Information Systems Specialist, HR Analytics OIG Participants: Anna Saez, OIG Manager Kimberly Perteet, Sr. Auditor and Project Leader Sean Newman, Auditor Brian Murphy, Auditor *Scope:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) *Details:* *Record of Work Done:* (b) (5) *Conclusion:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) *Notes:* *Results 4:*
B.2.PRG - Scoping *Procedure Step:* Meeting with the Office of Development & Learning 6/30/2014 *Type:* *Assigned To:* SMN *Prepared By:* SMN, 7/10/2014 *Reviewed By:* (None) **PROPERTIES:** *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6*	*Purpose:* The purpose of the meeting was to gain an understanding of the roles and responsibilties completed by the Office of Development & Learning (OD&L). *Criteria:* <P style="MARGIN-TOP: 0px; DIRECTION: ltr; MARGIN-BOTTOM: 0px"></P> <P>GAGAS 6.47-6.49 <P>6.47 Auditors should communicate an overview of the objectives, scope, and methodology and the timing of the performance audit and planned reporting (including any potential restrictions on the report), unless doing so could significantly impair the auditors' ability to obtain sufficient, appropriate evidence to address the audit objectives, such as when the auditors plan to conduct unannounced cash counts or perform procedures related to indications of fraud. Auditors should communicate with the following parties, as applicable: <P>a. management of the audited entity, including those with sufficient authority and responsibility to implement corrective action in the program or activity being audited; <P>b. those charged with governance;146

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
SCORECARD: *Rating:* *Sample Size:*	<P>c. the individuals contracting for or requesting audit services, such as contracting officials or grantees; and <P>d. the cognizant legislative committee, when auditors perform the audit pursuant to a law or regulation or they conduct the work for the legislative committee that has oversight of the audited entity. <P>6.48 In those situations where there is not a single individual or group that both oversees the strategic direction of the audited entity and the fulfillment of its accountability obligations or in other situations where the identity of those charged with governance is not clearly evident, auditors should document the process followed and conclusions reached for identifying the appropriate individuals to receive the required auditor communications. <P>6.49 Determining the form, content, and frequency of the communication is a matter of professional judgment, although written communication is preferred. Auditors may use an engagement letter to communicate the information. Auditors should document this communication. <P> </P></SPAN> *Source:* OD&L Participants: Sioux Thompson, Manager, Org. Development & Learning OIG Participants: Kimberly Perteet, Sr. Auditor and Project Leader Sean Newman, Auditor Brian Murphy, Auditor *Scope:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	The scope of the meeting was general conversation where the OIG asked questions in order to gain an understanding of the role the OD&L group serves on a daily basis. The meeting was held on 6/30/2014. *Details:* *Record of Work Done:* 6_30_14 Write-Up for Meeting with OD&L *Conclusion:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted] *Notes:* *Results 4:*
B.2.PRG - Scoping ***Procedure Step:*** Follow-Up Meeting with Board OMWI 7/1/2014 ***Type:*** ***Assigned To:*** BPM ***Prepared By:*** BPM, 7/11/2014 ***Reviewed By:*** (None)	*Purpose:* The purpose of the meeting was to conduct a follow-up meeting with the Board's Office of Diversity and Inclusion/Minority and Women Inclusion to gather information regarding their main roles and responsibilities, documentation of activities, interactions with other divisions, etc. *Criteria:* GAGAS 6.47-6.49 6.47 Auditors should communicate an overview of the objectives, scope, and methodology and the timing of the performance audit and planned reporting (including any potential restrictions on the report), unless doing so

Summary	Detail
PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	could significantly impair the auditors' ability to obtain sufficient, appropriate evidence to address the audit objectives, such as when the auditors plan to conduct unannounced cash counts or perform procedures related to indications of fraud. Auditors should communicate with the following parties, as applicable: a. management of the audited entity, including those with sufficient authority and responsibility to implement corrective action in the program or activity being audited; b. those charged with governance;146 c. the individuals contracting for or requesting audit services, such as contracting officials or grantees; and d. the cognizant legislative committee, when auditors perform the audit pursuant to a law or regulation or they conduct the work for the legislative committee that has oversight of the audited entity. 6.48 In those situations where there is not a single individual or group that both oversees the strategic direction of the audited entity and the fulfillment of its accountability obligations or in other situations where the identity of those charged with governance is not clearly evident, auditors should document the process followed and conclusions reached for identifying the appropriate individuals to receive the required auditor communications. 6.49 Determining the form, content, and frequency of the communication is a matter of professional judgment, although written communication is preferred. Auditors may use an engagement letter to communicate the information. Auditors should document this communication. *Source:* Attendees: OD&I: Sheila Clark, Program Director, Office of Diversity and Inclusion Johanna Bruce, Diversity/EEO Specialist OIG: Anna Saez, Senior OIG Manager

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Kim Perteet, Project Lead Brian Murphy, Auditor *Scope:* The scope of the meeting was general conversation where the OIG asked questions in order to gain an understanding of the roles and responsibilities of the Office of Diversity and Inclusion/Minority and Women Inclusion. The meeting was held on 7/1/2014. *Details:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
	Notes: *Results 4:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
B.2.PRG - Scoping		*Purpose:* The purpose of the meeting was to gain an understanding of the roles and responsibilties completed by Human Resources and Talent Acquisition.
Procedure Step:	Meeting with Human Resources 7/2/2014	
Type:		*Criteria:*
Assigned To:	SMN	<P style="MARGIN-TOP: 0px; DIRECTION: ltr; MARGIN-BOTTOM: 0px"></P>
Prepared By:	SMN, 7/10/2014	<P>GAGAS 6.47-6.49
Reviewed By:	(None)	<P>6.47 Auditors should communicate an overview of the objectives, scope, and methodology and the timing of the performance audit and planned reporting (including any potential restrictions on the report), unless doing so could significantly impair the auditors' ability to obtain sufficient, appropriate evidence to address the audit objectives, such as when the auditors plan to conduct unannounced cash counts or perform procedures related to indications of fraud. Auditors should communicate with the following parties, as applicable:
PROPERTIES:		<P>a. management of the audited entity, including those with sufficient authority and responsibility to implement corrective action in the program or activity being audited;
Location:		<P>b. those charged with governance;146
Frequency:		<P>c. the individuals contracting for or requesting audit services, such as contracting officials or grantees; and
Category 4:		<P>d. the cognizant legislative committee, when auditors perform the audit pursuant to a law or regulation or they conduct the work for the legislative committee that has oversight of the audited entity.
User Category:		<P>6.48 In those situations where there is not a single individual or group that both oversees the strategic direction of the audited entity and the fulfillment of its accountability obligations or in other situations
Category 5		
Category 6		
SCORECARD:		
Rating:		
Sample Size:		

Summary	Detail
	where the identity of those charged with governance is not clearly evident, auditors should document the process followed and conclusions reached for identifying the appropriate individuals to receive the required auditor communications. <P>6.49 Determining the form, content, and frequency of the communication is a matter of professional judgment, although written communication is preferred. Auditors may use an engagement letter to communicate the information. Auditors should document this communication. <P> </P></SPAN> *Source:* HR Participants: Debra York, Talent Acquisition Supervisor Gioia Wallace, Sr. Recruiting Specialist OIG Participants: Kimberly Perteet, Sr. Auditor and Project Leader Sean Newman, Auditor Brian Murphy, Auditor *Scope:* The scope of the meeting was general conversation where the OIG asked questions in order to gain an understanding of the role the HR group serves on a daily basis. The meeting was held on 7/2/2014. *Details:* *Record of Work Done:* 7_2_14 Write-Up for Meeting with HR

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Conclusion: (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) *Notes:* *Results 4:*
B.2.PRG - Scoping *Procedure Step:* Audit Objective, Scope, and Methodology *Type:* *Assigned To:* BPM *Prepared By:* SMN, 3/24/2015 *Reviewed By:* KLP, 3/26/2015 PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6*	*Purpose:* To finalize objective, scope and methodology to be used to complete the 2014 Congressional Request on the Board's Personnel Practices. *Criteria:* *Source:* OIG Audit Team *Scope:* Audit of the Board's Diversity and Inclusion Processes. *Details:* *Record of Work Done:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
SCORECARD: *Rating:* *Sample Size:*	Objective (b) (5) *Conclusion:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Notes: *Results 4:*
B.2.PRG - Scoping *Procedure Step:* End of Scoping *Type:* *Assigned To:* BPM *Prepared By:* BPM, 3/26/2015 *Reviewed By:* KLP, 3/26/2015 PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:*	*Purpose:* (b) (5) *Criteria:* The audit team will discuss with the AIG for Audits and Evaluations or the AIG for Information Technology, as applicable, whether a scoping effort is needed, with the final determination made by the applicable AIG. *Source:* OIG Audit Team *Scope:* Audit of the Board's Diversity and Inclusion Processes. *Details:* *Record of Work Done:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
Sample Size:	*Conclusion:* This decision complies with the OIG's policies and procedures for scoping an audit. *Notes:* *Results 4:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Profile

General

Code: 2015-MO-B-006

Name: The Board Can Enhance Its Diversity and Inclusion Efforts

Audit Plan: 2014

Entities:

Name	*Breadcrumb*
Federal Reserve Board (FRB)	Organizations > Federal Reserve Board (FRB)

Unit:

Group: Audits & Evaluations

Type: Management & Operations

Location: FRB

Scope: Other

Origin:

Team

Lead: Kimberly Perteet

Manager:

Staff Type:

The Board Can Enhance Its Diversity and Inclusion Efforts

Schedule

(b) (5)

(b) (5)

Actual Start Date: 4/4/2014

Actual End Date:

(b) (5)

Actual Hours: 0

(b) (5)

Actual Resource Costs:

(b) (5)

Actual External Costs: $0.00

(b) (5)

Actual Expenses:

The Board Can Enhance Its Diversity and Inclusion Efforts

Risk

Risk:

Total Risk Score: 0

Inherent Risk: 0

Residual Risk: 0

Objective(s)

2014 Congressional Request on the Board’s Personnel Practices in Team Mate

Background

Planning

Scope

General

The Board Can Enhance Its Diversity and Inclusion Efforts

Contact

Primary

Other

Summary

Final Risk:	
Opinion:	
Cost Savings:	$0.00
Cost Avoidance:	$0.00
Rating:	
Summary:	

Tracking

(b) (5)	
Actual Draft Date:	3/19/2015
(b) (5)	
Actual Response Date:	3/19/2015

The Board Can Enhance Its Diversity and Inclusion Efforts

(b) (5)

Actual Issue Date: 3/31/2015

Milestones

Category	(b) (5)	Act. Date	Comments
Blank			
Entrance Meeting		5/12/2014	
Midpoint Meeting		9/3/2014	
Project Design Meeting		5/12/2014	
Message Development Meeting		10/2/2014	
AIG-Approved Draft Report		3/4/2015	
Discussion Draft Report		3/4/2015	
Exit Meeting		3/13/2015	
Formal Draft Report		3/19/2015	
Final Report		3/31/2015	

Custom Properties

Custom Property Name	Value

Procedures

Summary	Detail
A.2.PRG - Admin Steps *Procedure Step:* Professional Competence *Type:* Preliminary *Assigned To:* SMN *Prepared By:* SMN, 3/27/2015 *Reviewed By:* KLP, 4/1/2015 PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	*Purpose:* Ensure staff assigned to the audit collectively possess adequate professional competence for the tasks required. *Criteria:* GAGAS 3.69-3.81, 6.12d, 6.45, and 6.51 **Competence** 3.69 The staff assigned to perform the audit must collectively possess adequate professional competence needed to address the audit objectives and perform the work in accordance with GAGAS. 3.70 The audit organization's management should assess skill needs to consider whether its workforce has the essential skills that match those necessary to perform the particular audit. Accordingly, audit organizations should have a process for recruitment, hiring, continuous development, assignment, and evaluation of staff to maintain a competent workforce. The nature, extent, and formality of the process will depend on various factors such as the size of the audit organization, its structure, and its work. 3.71 Competence is derived from a blending of education and experience. Competencies are not necessarily measured by years of auditing experience because such a quantitative measurement may not accurately reflect the kinds of experiences gained by an auditor in any given time period. Maintaining competence through a commitment to learning and development throughout an auditor's professional life is an important element for auditors. Competence enables an auditor to make sound professional judgments. **Technical Knowledge** 3.72 The staff assigned to conduct an audit in accordance with GAGAS should collectively possess the technical knowledge, skills, and experience necessary to be competent for the type of work being performed before

Summary	Detail
	beginning work on that audit. The staff assigned to a GAGAS audit should collectively possess a. knowledge of GAGAS applicable to the type of work they are assigned and the education, skills, and experience to apply this knowledge to the work being performed; b. general knowledge of the environment in which the audited entity operates and the subject matter; c. skills to communicate clearly and effectively, both orally and in writing; and d. skills appropriate for the work being performed; for example, skills in (1) statistical or nonstatistical sampling if the work involves use of sampling; (2) information technology if the work involves review of information systems; (3) engineering if the work involves review of complex engineering data; (4) specialized audit methodologies or analytical techniques, such as the use of complex survey instruments, actuarial-based estimates, or statistical analysis tests, as applicable; or (5) specialized knowledge in subject matters, such as scientific, medical, environmental, educational, or any other specialized subject matter, if the work calls for such expertise. **Additional Qualifications** 3.73 Auditors performing financial audits should be knowledgeable in U.S. generally accepted accounting principles (GAAP), or with the applicable financial reporting framework being used, and the American Institute of Certified Public Accountants' (AICPA) Statements on Auditing Standards (SAS)37and they should be competent in applying these SASs to the audit work. 3.74 Similarly, auditors performing attestation engagements should be knowledgeable in the AICPA general attestation standard related to criteria, the AICPA attestation standards for field work and reporting, and the related Statements on Standards for Attestation Engagements (SSAE),38 and they should be competent in applying these standards and SSAE to the

Summary	Detail
	attestation work.39 3.75 Auditors engaged to perform financial audits or attestation engagements should be licensed certified public accountants, persons working for a licensed certified public accounting firm or for a government auditing organization, or licensed accountants in states that have multi-class licensing systems that recognize licensed accountants other than certified public accountants. **Continuing Professional Education** 3.76 Auditors performing work in accordance with GAGAS, including planning, directing, performing audit procedures, or reporting on an audit conducted in accordance with GAGAS, should maintain their professional competence through continuing professional education (CPE). Therefore, each auditor performing work in accordance with GAGAS should complete, every 2 years, at least 24 hours of CPE that directly relates to government auditing, the government environment, or the specific or unique environment in which the audited entity operates. Auditors who are involved in any amount of planning, directing, or reporting on GAGAS audits and auditors who are not involved in those activities but charge 20 percent or more of their time annually to GAGAS audits should also obtain at least an additional 56 hours of CPE (for a total of 80 hours of CPE in every 2-year period) that enhances the auditor's professional proficiency to perform audits. Auditors required to take the total 80 hours of CPE should complete at least 20 hours of CPE in each year of the 2-year periods. Auditors hired or initially assigned to GAGAS audits after the beginning of an audit organization's 2-year CPE period should complete a prorated number of CPE hours. 3.77 CPE programs are structured educational activities with learning objectives designed to maintain or enhance participants' knowledge, skills, and abilities in areas applicable to performing audits. Determining what subjects are appropriate for individual auditors to satisfy both the 80-hour and the 24-hour requirements is a matter of professional judgment to be exercised by auditors in consultation with appropriate officials in their audit

Summary	Detail
	organizations. Among the considerations in exercising that judgment are the auditors' experience, the responsibilities they assume in performing GAGAS audits, and the operating environment of the audited entity. 3.78 Meeting CPE requirements is primarily the responsibility of individual auditors. The audit organization should have quality control procedures to help ensure that auditors meet the continuing education requirements, including documentation of the CPE completed. The Government Accountability Office (GAO) has developed guidance pertaining to CPE requirements to assist auditors and audit organizations in exercising professional judgment in complying with the CPE requirements. **CPE For Specialists** 3.79 The audit team should determine that external specialists assisting in performing a GAGAS audit are qualified and competent in their areas of specialization; however, external specialists are not required to meet the GAGAS CPE requirements. 3.80 The audit team should determine that internal specialists consulting on a GAGAS audit who are not involved in directing, performing audit procedures, or reporting on a GAGAS audit, are qualified and competent in their areas of specialization; however, these internal specialists are not required to meet the GAGAS CPE requirements. 3.81 The audit team should determine that internal specialists, who are performing work in accordance with GAGAS as part of the audit team, including directing, performing audit procedures, or reporting on a GAGAS audit, comply with GAGAS, including the CPE requirements.41 The GAGAS CPE requirements become effective for internal specialists when an audit organization first assigns an internal specialist to an audit. Because internal specialists apply specialized knowledge in government audits, training in their areas of specialization qualify under the requirement for 24 hours of CPE that directly relates to government auditing, the government environment, or the specific or unique environment in which the audited entity operates. **Planning** 6.12 During planning, auditors should also **(d)** assign sufficient staff and

Summary	Detail
	specialists with adequate collective professional competence and identify other resources needed to perform the audit; **Assigning Staff & Other Resources** 6.45 Audit management should assign sufficient staff and specialists with adequate collective professional competence to perform the audit. Staffing an audit includes, among other things: a. assigning staff and specialists with the collective knowledge, skills, and experience appropriate for the job, b. assigning a sufficient number of staff and supervisors to the audit, c. providing for on-the-job training of staff, and d. engaging specialists when necessary. **Written Audit Plan** 6.51 Auditors must prepare a written audit plan for each audit. The form and content of the written audit plan may vary among audits and may include an audit strategy, audit program, project plan, audit planning paper, or other appropriate documentation of key decisions about the audit objectives, scope, and methodology and the auditors' basis for those decisions. Auditors should update the plan, as necessary, to reflect any significant changes to the plan made during the audit. *Source:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Details: (b) (5) (b) (6)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (6) [redacted] *Conclusion:* Audit organization's management has deemed the staff qualfied to excute the assigned audit in accordance with GAGAS. *Notes:* *Results 4:*
A.2.PRG - Admin Steps *Procedure Step:* Notify Stakeholders *Type:* Preliminary *Assigned To:* KLP	*Purpose:* Prepare and issue announcement letter. When appropriate, prepare a separate letter at the end of the scoping stage. *Criteria:* GAGAS 6.47-6.49

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
Prepared By:	KLP, 4/29/2014	6.47 Auditors should communicate an overview of the objectives, scope, and methodology and the timing of the performance audit and planned reporting (including any potential restrictions on the report), unless doing so could significantly impair the auditors' ability to obtain sufficient, appropriate evidence to address the audit objectives, such as when the auditors plan to conduct unannounced cash counts or perform procedures related to indications of fraud. Auditors should communicate with the following parties, as applicable: a. management of the audited entity, including those with sufficient authority and responsibility to implement corrective action in the program or activity being audited; b. those charged with governance;146 c. the individuals contracting for or requesting audit services, such as contracting officials or grantees; and d. the cognizant legislative committee, when auditors perform the audit pursuant to a law or regulation or they conduct the work for the legislative committee that has oversight of the audited entity. 6.48 In those situations where there is not a single individual or group that both oversees the strategic direction of the audited entity and the fulfillment of its accountability obligations or in other situations where the identity of those charged with governance is not clearly evident, auditors should document the process followed and conclusions reached for identifying the appropriate individuals to receive the required auditor communications. 6.49 Determining the form, content, and frequency of the communication is a matter of professional judgment, although written communication is preferred. Auditors may use an engagement letter to communicate the information. Auditors should document this communication. *Source:* *Scope:*
Reviewed By:	(None)	
PROPERTIES:		
Location:		
Frequency:		
Category 4:		
User Category:		
Category 5		
Category 6		
SCORECARD:		
Rating:		
Sample Size:		

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) [redacted] *Details:* *Record of Work Done:* The OIG audit team issued its announcement letter and document request list to the appropriate officials at the Board of Governors of the Federal Reserve System's (Board) in regards to the Audit of the Board's Diversity and Inclusion Processes. The letter was issued on Friday, April 25, 2014. References Board Announcement CR Diversity April 2014 Board Announcement CR Diversity April 2014 Email Confirmation *Conclusion:* The OIG audit team issued its announcement letter and document request list to the appropriate officials at the Board of Governors of the Federal Reserve System's (Board) on Friday, April 25, 2014. *Notes:* *Results 4:*
A.2.PRG - Admin Steps	*Purpose:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
Procedure Step:	Conduct Entrance Conference	Plan for and conduct entrance conference.
Type:		*Criteria:*
Assigned To:	BML	GAGAS 6.47-6.49 6.47 Auditors should communicate an overview of the objectives, scope, and methodology and the timing of the performance audit and planned reporting (including any potential restrictions on the report), unless doing so could significantly impair the auditors' ability to obtain sufficient, appropriate evidence to address the audit objectives, such as when the auditors plan to conduct unannounced cash counts or perform procedures related to indications of fraud. Auditors should communicate with the following parties, as applicable: a. management of the audited entity, including those with sufficient authority and responsibility to implement corrective action in the program or activity being audited; b. those charged with governance;146 c. the individuals contracting for or requesting audit services, such as contracting officials or grantees; and d. the cognizant legislative committee, when auditors perform the audit pursuant to a law or regulation or they conduct the work for the legislative committee that has oversight of the audited entity. 6.48 In those situations where there is not a single individual or group that both oversees the strategic direction of the audited entity and the fulfillment of its accountability obligations or in other situations where the identity of those charged with governance is not clearly evident, auditors should document the process followed and conclusions reached for identifying the appropriate individuals to receive the required auditor communications. 6.49 Determining the form, content, and frequency of the communication is a matter of professional judgment, although written communication is preferred. Auditors may use an engagement letter to communicate the information. Auditors should document this communication.
Prepared By:	BML, 6/4/2014	
Reviewed By:	KLP, 8/4/2014	
PROPERTIES:		
Location:		
Frequency:		
Category 4:		
User Category:		
Category 5		
Category 6		
SCORECARD:		
Rating:		
Sample Size:		

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Source: FRB OIG Management Division Human Capital Office Diversity and Inclusion (b) (5) *Details:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
A.2.PRG - Admin Steps *Procedure Step:* Conduct Exit Conference *Type:* Preliminary *Assigned To:* SMN *Prepared By:* SMN, 3/31/2015	*Purpose:* Plan for and conduct exit conference. *Criteria:* GAGAS 6.47-6.49 Auditors should communicate an overview of the objectives, scope, and methodology and the timing of the performance audit and planned

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
Reviewed By: KLP, 4/1/2015 PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	reporting (including any potential restrictions on the report), unless doing so could significantly impair the auditors' ability to obtain sufficient, appropriate evidence to address the audit objectives, such as when the auditors plan to conduct unannounced cash counts or perform procedures related to indications of fraud. Auditors should communicate with the following parties, as applicable: a. management of the audited entity, including those with sufficient authority and responsibility to implement corrective action in the program or activity being audited; b. those charged with governance;146 c. the individuals contracting for or requesting audit services, such as contracting officials or grantees; and d. the cognizant legislative committee, when auditors perform the audit pursuant to a law or regulation or they conduct the work for the legislative committee that has oversight of the audited entity. 6.48 In those situations where there is not a single individual or group that both oversees the strategic direction of the audited entity and the fulfillment of its accountability obligations or in other situations where the identity of those charged with governance is not clearly evident, auditors should document the process followed and conclusions reached for identifying the appropriate individuals to receive the required auditor communications. 6.49 Determining the form, content, and frequency of the communication is a matter of professional judgment, although written communication is preferred. Auditors may use an engagement letter to communicate the information. Auditors should document this communication. *Source:* Auditor's notes taken during meetings. *Scope:* 2014 Audit of the Board's Diversity and Inclusion Processes

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Details: (b) (5) [redacted] *Notes:* *Results 4:*
A.2.PRG - Admin Steps	*Purpose:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
Procedure Step:	Document Deviations from GAGAS	Ensure that if a decision was made by the OIG that a standard was not applicable, this decision has been documented in the report and supporting workpapers.
Type:	Fieldwork	
Assigned To:		*Criteria:*
Prepared By:	SMN, 3/24/2015	GAGAS 6.84
Reviewed By:	KLP, 3/26/2015	6.84 When auditors do not comply with applicable GAGAS requirements due to law, regulation, scope limitations, restrictions on access to records, or other issues impacting the audit, the auditors should document the departure from the GAGAS requirements and the impact on the audit and on the auditors' conclusions. This applies to departures from unconditional requirements and from presumptively mandatory requirements when alternative procedures performed in the circumstances were not sufficient to achieve the objectives of the standard.
PROPERTIES:		
Location:		
Frequency:		
Category 4:		
User Category:		*Source:*
Category 5		Audit Team
Category 6		
SCORECARD:		*Scope:*
Rating:		To document deviations from GAGAS for the audit on the Board's diversity and inclusion processes during the planning, field work, and reporting phases. This audit was conducted from March 2014 through March 2015.
Sample Size:		
		Details:
		Record of Work Done:

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	We confirmed that all GAGAS requirements were met by completing the audit checklists found in Teammate's program group C, as well as by completing applicable Teammate steps for planning, fieldwork, and reporting. No deviations from GAGAS have been documented. *Conclusion:* No deviations from GAGAS have been documented. *Notes:* *Results 4:*

Entrance Conference for the Audit of the Board's Diversity and Inclusion Processes

Date: 5/12/2014

Participants:

- Donald Hammond, Chief Operating Officer, COO
- Michell Clark, Director, Management Division
- David Harmon, Deputy Director, Human Capital
- Shelia Clark, Program Director, Diversity and Inclusion
- Melissa Heist, Associate Inspector General, OIG
- Timothy Rogers, Senior Manager, OIG
- Kimberly Perteet, Senior Auditor, OIG
- Jina Hwang, Counsel, OIG
- Brian Murphy, Auditor, OIG
- Brandon Lee, Auditor, OIG

Meeting objective/Purpose:

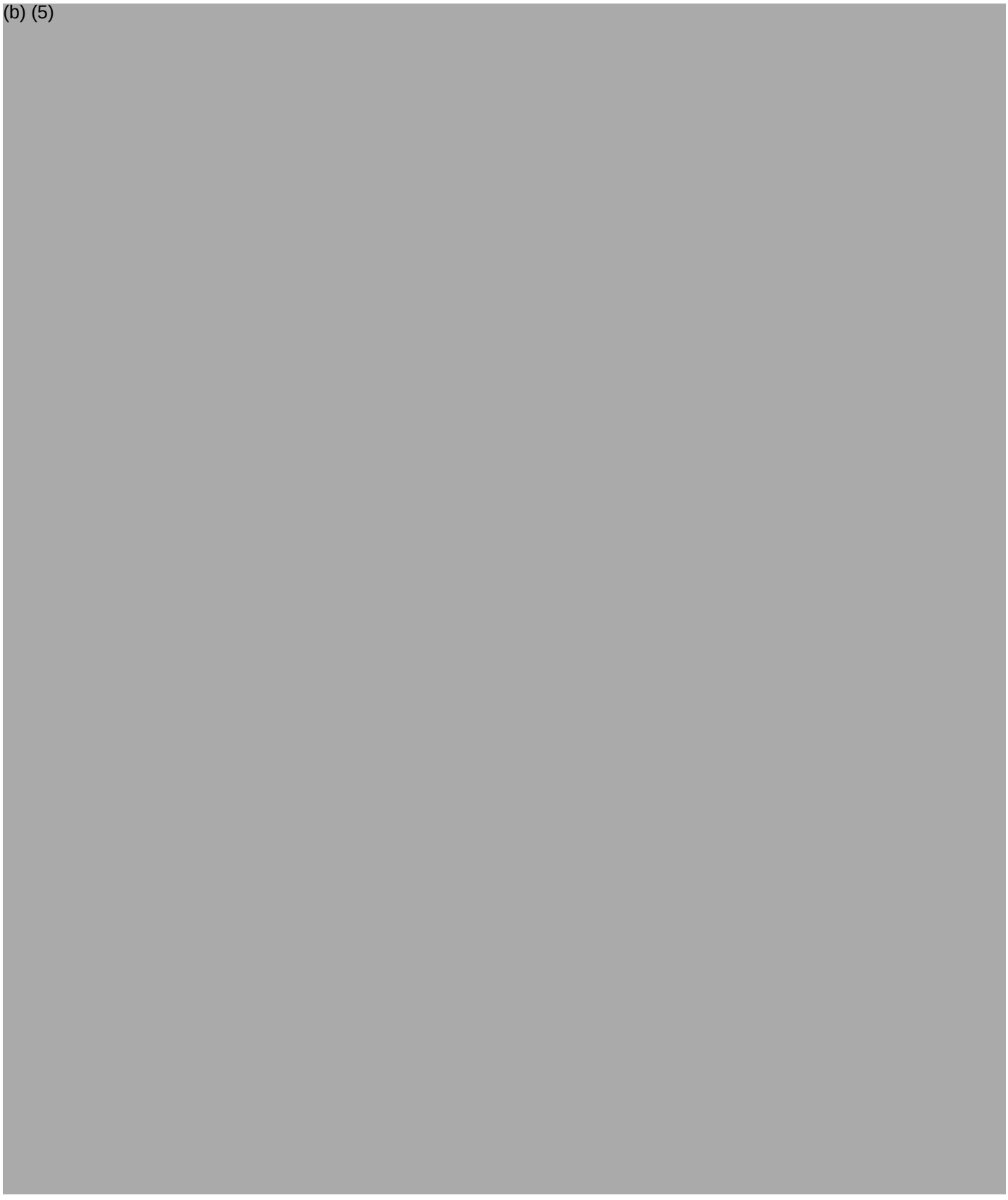
The purpose of this meeting was to provide senior Management Division staff of objective, scope, methodology, and key dates related to the audit.

Minutes:

- The audit team presented an agenda and audit process documents.
- The team informed the auditees of the objective, scope and methodology.
    - (b) (5)

(b) (5)

(b) (5)



Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Exit Conference 3/13/2015

Purpose: To obtain the Board's thoughts on the discussion draft.

Source: Auditor's notes taken during meeting.

Scope: 2014 Audit of the Board's Diversity and Inclusion Processes

Conclusion: See "Next Steps"

Prepared by: S. Newman, Auditor, Sopeany Keo, and B. Murphy, Auditor
Reviewed by: K. Perteet, Senior Auditor/Project Lead

PSSC: See A.2.PRG, workstep.
A.2.PRG

Meeting minutes written up by project team members Sean Newman, Sopeany Keo, and Brian Murphy.

Attendees:

Board

Donald Hammond, Chief Operating Officer
David Harmon, Deputy Director & Chief HCO
Michell Clark, Director of the Management Division
Sheila Clark, ODI Program Director
Lil Shewmaker, Chief Admin & Special Projects for R/S
Janice Shack-Marquez, Deputy Director of R&S
Kit Wheatley, Associate General Counsel Lit/Legal Services
Jean Anderson, Assistant General Counsel for HR&SP
Daniel Covitz, Deputy Director of R&S
Egon Zakrajsek, Associate Director of Monetary Affairs
Thomas Connors, Deputy Director of International Finance

OIG

Melissa Heist, Associate Inspector General for Audits and Evaluations
Jackie Becker, Associate Inspector General & Counsel
Tim Rogers, Senior OIG Manager
Anna Saez, OIG Manager
Kimberly Perteet, Senior Auditor/Project Lead
Sean Newman, Auditor
Brian Murphy, Auditor
Sopeany Keo, Auditor

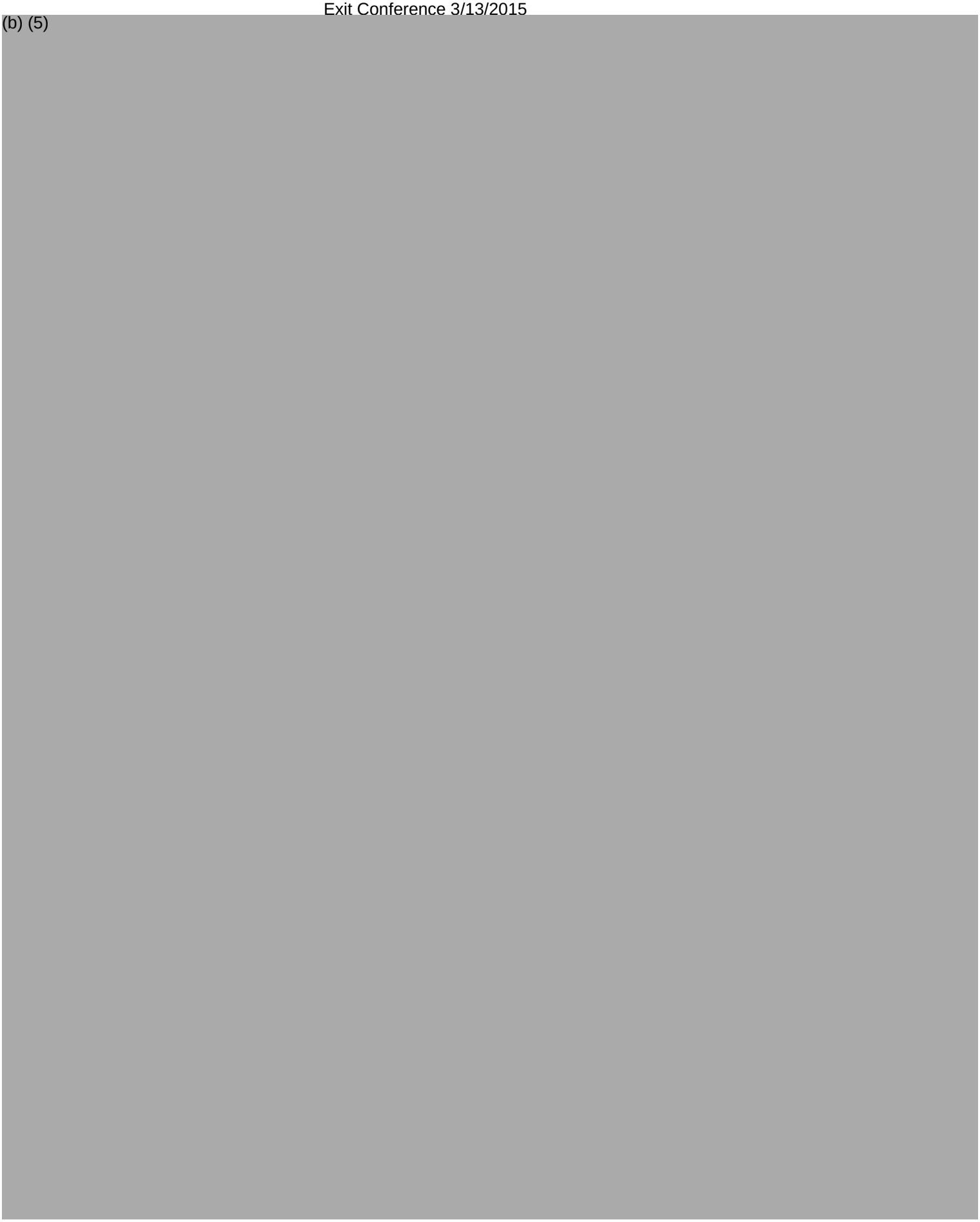
Time, Date, and Location:
Meeting held at 10:00 AM on 3/13/2015 in Room KI-3810 at 1801 K St. Washington, DC

Summary of Discussions:

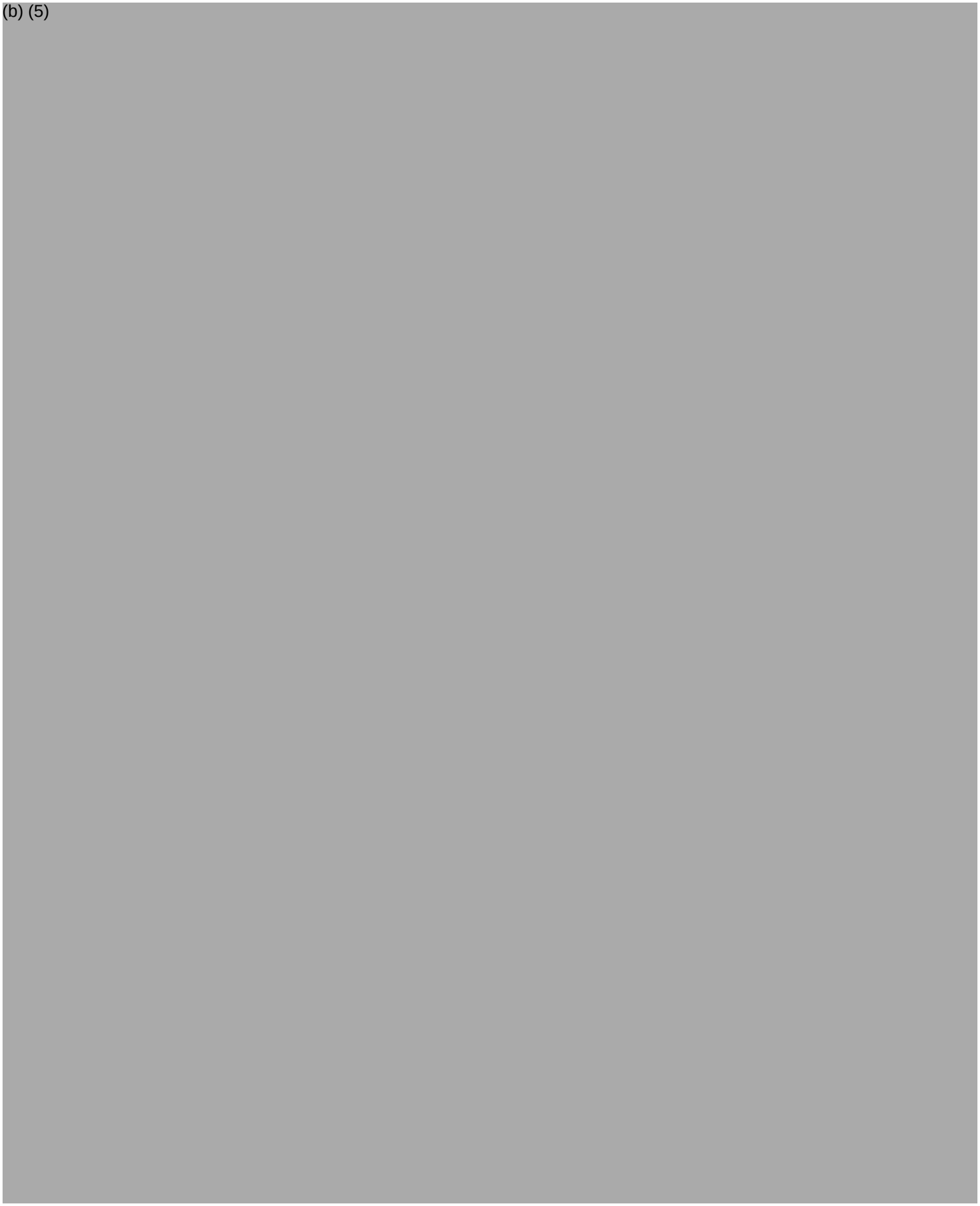
(b) (5)

[redacted]

(b) (5)



(b) (5)



(b) (5)

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

Restricted-FR

September 30, 2014

MEMORANDUM

TO: Audit of the Board's Diversity and Inclusion Processes Audit File

FROM: Sean Newman

CC: Anna Saez

SUBJECT: (b) (5)

Purpose: (b) (5)

(b) (5)

(b) (5)

Source: Memo prepared by OIG Auditor Sean Newman.

The Board Can Enhance Its Diversity and Inclusion Efforts

Profile

General

Code: 2015-MO-B-006

Name: The Board Can Enhance Its Diversity and Inclusion Efforts

Audit Plan: 2014

Entities:

Name	*Breadcrumb*
Federal Reserve Board (FRB)	Organizations > Federal Reserve Board (FRB)

Unit:

Group: Audits & Evaluations

Type: Management & Operations

Location: FRB

Scope: Other

Origin:

Team

Lead: Kimberly Perteet

Manager:

Staff Type:

The Board Can Enhance Its Diversity and Inclusion Efforts

Schedule

(b) (5)

(b) (5)

Actual Start Date: 4/4/2014

Actual End Date:

(b) (5)

Actual Hours: 0

(b) (5)

Actual Resource Costs:

(b) (5)

Actual External Costs: $0.00

(b) (5)

Actual Expenses:

The Board Can Enhance Its Diversity and Inclusion Efforts

Risk

Risk:

Total Risk Score: 0

Inherent Risk: 0

Residual Risk: 0

Objective(s)

2014 Congressional Request on the Board’s Personnel Practices in Team Mate

Background

Planning

Scope

General

The Board Can Enhance Its Diversity and Inclusion Efforts

Contact

Primary

Other

Summary

Final Risk:	
Opinion:	
Cost Savings:	$0.00
Cost Avoidance:	$0.00
Rating:	
Summary:	

Tracking

(b) (5)	
Actual Draft Date:	3/19/2015
(b) (5)	
Actual Response Date:	3/19/2015

The Board Can Enhance Its Diversity and Inclusion Efforts

(b) (5)

Actual Issue Date: 3/31/2015

Milestones

Category	(b) (5)	Act. Date	Comments
Blank			
Entrance Meeting		5/12/2014	
Midpoint Meeting		9/3/2014	
Project Design Meeting		5/12/2014	
Message Development Meeting		10/2/2014	
AIG-Approved Draft Report		3/4/2015	
Discussion Draft Report		3/4/2015	
Exit Meeting		3/13/2015	
Formal Draft Report		3/19/2015	
Final Report		3/31/2015	

Custom Properties

Custom Property Name	Value

Procedures

Summary	Detail
B.1.PRG - Background\Planning *Procedure Step:* 1. (b) (5) *Type:* Planning *Assigned To:* KLP *Prepared By:* SPK, 3/26/2015 *Reviewed By:* KLP, 3/26/2015 PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	*Purpose:* (b) (5) *Criteria:* GAGAS 3.40 - 3.49, 7.04, 7.13 - 7.14 3.40 Routine activities performed by auditors that relate directly to the performance of an audit, such as providing advice and responding to questions as part of an audit, are not considered nonaudit services under GAGAS. Such routine activities generally involve providing advice or assistance to the entity on an informal basis as part of an audit. Routine activities typically are insignificant in terms of time incurred or resources expended and generally do not result in a specific project or engagement or in the auditors producing a formal report or other formal work product. However, activities such as financial statement preparation, cash to accrual conversions, and reconciliations are considered nonaudit services under GAGAS, not routine activities related to the performance of an audit, and are evaluated using the conceptual framework as discussed in paragraph 3.46. 3.41 Routine activities directly related to an audit include the following: a. providing advice to the audited entity on an accounting matter as an ancillary part of the overall financial audit; b. researching and responding to the audited entity's technical questions on relevant tax laws as an ancillary part of providing tax services; c. providing advice to the audited entity on routine business matters; d. educating the audited entity on matters within the technical expertise of the auditors; and readily available to the auditors, such as best practices and

Summary	Detail
	benchmarking studies. 3.42 An auditor who previously performed nonaudit services for an entity that is a prospective subject of an audit should evaluate the impact of those nonaudit services on independence before accepting an audit. If the nonaudit services were performed in the period to be covered by the audit, the auditor should (1) determine if the nonaudit service is expressly prohibited by GAGAS and, if not, (2) determine whether a threat to independence exists and address any threats noted in accordance with the conceptual framework. 3.43 Nonaudit services provided by auditors can impact independence of mind and in appearance in periods subsequent to the period in which the nonaudit service was provided. For example, if auditors have designed and implemented an accounting and financial reporting system that is expected to be in place for many years, a threat to independence in appearance for future financial audits or attestation engagements performed by those auditors may exist in subsequent periods. For recurring audits, having another independent audit organization perform an audit of the areas affected by the nonaudit service may provide a safeguard that allows the audit organization that provided the nonaudit service to mitigate the threat to its independence. Auditors use professional judgment to determine whether the safeguards adequately mitigate the threats. 3.44 An auditor in a government entity may be required to perform a nonaudit service that could impair the auditor's independence with respect to a required audit. If the auditor cannot, as a consequence of constitutional or statutory requirements over which the auditor has no control, implement safeguards to reduce the resulting threat to an acceptable level, or decline to perform or terminate a nonaudit service that is incompatible with audit responsibilities, the auditor should disclose the nature of the threat that could not be eliminated or reduced to an acceptable level and modify the GAGAS compliance statement accordingly. 3.45 By their nature, certain nonaudit services directly support the entity's operations and impair auditors' ability to maintain independence in mind and appearance. The nonaudit services discussed below are among those

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	frequently requested of auditors working in a government environment. Some aspects of these services will impair an auditor's ability to perform audits for the entities for which the services are provided. The specific services indicated are not the only nonaudit services that would impair an auditor's independence. 3.46 Auditors may be able to provide nonaudit services in the broad areas indicated in paragraphs 3.49 through 3.58 without impairing independence if (1) the nonaudit services are not expressly prohibited, (2) the auditor has determined that the requirements for performing nonaudit services in paragraphs 3.34 through 3.44 have been met, and (3) any significant threats to independence have been eliminated or reduced to an acceptable level through the application of safeguards. Auditors should use the conceptual framework to evaluate independence given the facts and circumstances of individual services not specifically prohibited in this section. 3.47 For performance audits and agreed-upon procedures engagements, nonaudit services that are otherwise prohibited by GAGAS may be provided when such services do not relate to the specific subject matter of the engagement. 3.48 For financial statement audits and examination or review engagements, a nonaudit service performed during the period covered by the financial statements may not impair an auditor's independence with respect to those financial statements provided that the following conditions exist: a. the nonaudit service was provided prior to the period of professional engagement; b. the nonaudit service related only to periods prior to the period covered by the financial statements; and c. the financial statements for the period to which the nonaudit service did relate were audited by another auditor (or in the case of an examination or review engagement, examined, reviewed, or audited by another auditor as appropriate). **Management Responsibilities** **3.49** If performed on behalf of an audited entity by the entity's auditor, management responsibilities such as those listed in paragraph 3.36 would

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	create management participation threats so significant that no safeguards could reduce them to an acceptable level. Consequently the auditor's independence would be impaired with respect to that entity. *Source:* FRB OIG House of Representatives Committee on Financial Services *Scope:* (b) (5) 2014 Board's Congressional Request -- Personnel activities from January 2011 to December 2013, and Changes to policies and procedures since December 2013. (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
B.1.PRG - Background\Planning *Procedure Step:* 2. Understand the Program to be Audited *Type:* Planning *Assigned To:* BML *Prepared By:* BML, 5/20/2014 *Reviewed By:* KLP, 3/11/2015	*Purpose:* Review, as applicable, information explaining the program's applicable laws and regulations, goals and objectives, size (resource efforts), operations, outputs, and outcomes. *Criteria:* GAGAS 6.15 6.15 Obtaining an understanding of the program under audit helps auditors to assess the relevant risks associated with the program and the impact of the risks on the audit objectives, scope, and methodology. The auditors'

Summary	Detail
PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	understanding may come from knowledge they already have about the program or knowledge they gain from inquiries, observations, and reviewing documents while planning the audit. The extent and breadth of those inquiries and observations will vary among audits based on the audit objectives, as will the need to understand individual aspects of the program, such as the following: a. Provisions of laws, regulations, contracts and grant agreements: Government programs are usually created by law and are subject to specific laws and regulations. Laws and regulations usually set forth what is to be done, who is to do it, the purpose to be achieved, the population to be served, and related funding guidelines or restrictions. Government programs may also be subject to contracts or grant agreements. Thus, understanding the laws and legislative history establishing a program and the provisions of any contracts or grant agreements is essential to understanding the program itself. Obtaining that understanding is also a necessary step in identifying the provisions of laws, regulations, contracts, or grant agreements that are significant within the context of the audit objectives. b. Purpose and goals: Purpose is the result or effect that is intended or desired from a program's operation. Legislatures usually establish the program's purpose when they provide authority for the program. Entity officials may provide more detailed information on the program's purpose to supplement the authorizing legislation. Entity officials are sometimes asked to set goals for program performance and operations, including both output and outcome goals. Auditors may use the stated program purpose and goals as criteria for assessing program performance or may develop additional criteria to use when assessing performance. c. Internal control: Internal control, sometimes referred to as management control, in the broadest sense includes the plan, policies, methods, and procedures adopted by management to meet its missions, goals, and objectives. Internal control includes the processes for planning, organizing, directing, and controlling program operations. It includes the systems for measuring, reporting, and monitoring program performance. Internal

Summary	Detail
	control serves as a defense in safeguarding assets and in preventing and detecting errors; fraud; noncompliance with provisions of laws, regulations, contracts or grant agreements; or abuse. d. Inputs: Inputs are the amount of resources (in terms of money, material, personnel, etc.) that are put into a program. These resources may come from within or outside the entity operating the program. Measures of inputs can have a number of dimensions, such as cost, timing, and quality. Examples of measures of inputs are dollars spent, employee-hours expended, and square feet of building space. e. Program operations: Program operations are the strategies, processes, and activities management uses to convert inputs into outputs. Program operations may be subject to internal control. f. Outputs: Outputs represent the quantity of goods or services produced by a program. For example, an output measure for a job training program could be the number of persons completing training, and an output measure for an aviation safety inspection program could be the number of safety inspections completed. g. Outcomes: Outcomes are accomplishments or results of a program. For example, an outcome measure for a job training program could be the percentage of trained persons obtaining a job and still in the work place after a specified period of time. An example of an outcome measure for an aviation safety inspection program could be the percentage reduction in safety problems found in subsequent inspections or the percentage of problems deemed corrected in follow-up inspections. Such outcome measures show the progress made in achieving the stated program purpose of helping unemployable citizens obtain and retain jobs, and improving the safety of aviation operations. Outcomes may be influenced by cultural, economic, physical, or technological factors outside the program. Auditors may use approaches drawn from other disciplines, such as program evaluation, to isolate the effects of the program from these other influences. Outcomes also include unexpected and/or unintentional effects of a program, both positive and negative.

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Source: • Board internal website • FRB OIG *Scope:* (b) (5) *Details:* *Record of Work Done:* Background *Organization* **The Board of Governors of the Federal Reserve System (Board)** is a federal government agency. The Board is composed of seven members, who are appointed by the President of the United States and confirmed by the U.S. Senate. *Mission & Objectives* The Federal Reserve System is the central bank of the United States. It was founded by Congress in 1913 to provide the nation with a safer, more flexible, and more stable monetary and financial system. Over the years, its role in banking and the economy has expanded. FRB Mission ; B.1.86 *Organization*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	The Office of Diversity and Inclusion (OD&I) is comprised of the Equal Employment Opportunity office, Diversity and Inclusion, and The Office of Minority, Women, and Inclusion. Shelia Clark is the program Director and has 9 employees. Office of Diversity and Inclusion - Organizational ChartOffice of Diversity and Inclusion staff *Mission & Objectives* The mission of OD&I to provide equal opportunity for all qualified persons; to prohibit discrimination in employment and because of race, color, notational origin, disability, age, or sex; and to promote the full realization of equal employment opportunity. Additionally, the office provides oversight to the reserve banks. Some of the objectives of OD&I are (1) meet the spirit and intent of relevant laws and regulations, (2) develop standards for EEO and diversity in the workforce, (3) Monitor the Reserve Banks progress related to EEO and diversity, (4) advise the Board about the impact of policies related to minority and women businesses, (5) provide guidance to help resolve EEO matters, (6) assist procurement in developing standards for good-faith estimates related to minorities and women, (7) work with staff from BSR, Legal, and Consumer Affairs to assess diversity policies and practices, (8) provide oversight related to training on EEO and diversity, (9) support HR and procurement related to diversity and EEO objectives, (10) review legal precedents that could affect EEO and diversity, (11) provide leadership to employee advisory committees, (12) sponsor programs/awareness about inter-group relations, (13) evaluate the EEO information system, (14) implement outreach programs to high schools and colleges, (15) maintain relationships with organizations who are responsible for EEO, (16) establish a board evaluation process that will withstand external review, (17) work with reserve banks, and various entities to balance the autonomy of the reserve banks with the Board's oversight role. OD&I Mission and Objectives Laws, Regulations, and Policies *PMP*

Summary	Detail
	The purpose of the PMP process is to (1) continuously improve individual and organizational performance, (2) develop and motivate employees to become top performers and help the Board achieve its mission and purpose, and (3) inform various employment decisions. The performance ratings are extraordinary, outstanding, commendable, marginal, and unsatisfactory. To meet the goals of the PMP process, supervisors are responsible for creating performance standards, monitoring performance, and providing an employee with feedback on his or her performance. Board PMP Policy (Including Appeals Process) *EEO* The EEO policy is to provide equal opportunity in employment for all persons. The policy prohibits discrimination in employment on the basis of race, color, religion, sex, national origin, age, disability, or genetic information, and promotes the full realization of equal employment opportunity. Additionally, the Board complies with the following statues and any amendments: • Civil Rights Act of 1964 (title VII), • section 501 of the Rehabilitation Act of 1973, • the Age Discrimination in Employment Act of 1967 (ADEA), • the Equal Pay Act of 1963, the Genetic Information Nondiscrimination Act of 2008, and • the Uniformed Services Employment and Reemployment Rights Act of 1994 (USERRA) If an employee feels they have been discriminated against on the basis of race, color, religion, sex, national origin, disability, age, or genetic information, or subject to retaliation the employee may raise a complaint with the ODI office. The aggrieved person must contact an EEO counselor

Summary	Detail
	within 45 days of the date of the action. An employee or applicant for employment, who believes that he or she has been discriminated against on the basis of any application, membership, or service in the uniformed services, or subject to retaliation for engaging in protected activity, may raise any such complaint with the Department of Labor. Because the process for USERRA-related complaints differs from the process for complaints of other forms of discrimination, ODI does not counsel or provide any complaint processing for USERRA-related complaints. The Board has assigned managers and supervisors direct reasonability for implementation of EEO policies. The ODI director coordinates agency wide EEO procedures, advise the Board related to EEO laws, implementing other related Board policies, coordinating EEO complaint resolutions, and recommending corrective actions. Board EEO Policy *Dodd Frank Wall Street Reform* Section 342 of Dodd Frank established the Office of Minority and Women Inclusion (OMWI). Each agency was required to establish an OMWI, within 6 months of the Act date, related to matters of diversity in management, employment, and business activities. The Act outlines duties of the director to coordinate with the agency to design and implement related policies (such as increased minority owned and women owned business participation, EEO, and assessing diversity polices). The agencies are required to submit an annual report to congress related to amounts paid by contractors, percentage totals of those amounts, challenges faced, and any findings/recommendations. Lastly, the agency will is required to take affirmative action steps to promote diversity. Dodd_Frank_Act_Section_342 *OMWI Reprot April 2014* The Board's ODI office regularly releases a report to Congress related about the activities of the Office of Diversity and Inclusion. ODI strives to meet the "Essential Elements of a Model EEO Program" found in the Equal Employment Opportunity Commission's (EEOC) Management Directive 715. The Board reviews quarterly employment data to determine any adverse impact based on race or gender as well as complaint trends. The

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Board annually submits the EEOC, EEO-1 Report, and EEO status report. The Board's total workforce is 44 percent female and 44 percent minority. The Board reported an increase of 69 (3 percent) employees in the total workforce for 2013, of which 32 were minorities and 20 were women. The percentage of minorities in the Executive Senior Level category increased from 21 percent in 2012 to 23 percent in 2013. In the 1st/Mid. Level Manager category, the percentage of minorities increased from 42 percent in 2012 to 53 percent in 2013. Representation of women decreased from 65% in 2012 to 55% in 2013. The representation of women remained at 40 percent in the Executive Senior Level category. In 2013, the Board filled 409 positions, of which 113 were summer interns. Board utilized a variety of sources to fill the positions. Thirty-nine percent of the positions were filled internally. In filling the remaining 61 percent of positions, the Board used a variety of methods. The Board still struggles to hire Hispanics in the overall workforce and in the hiring of minorities in economic and regulatory roles. A comprehensive program strategy was implemented by setting forth specific actions to assist the Board in fostering relationships with minority-owned and women-owned businesses. omwi-report-20140401 omwi-report-20120402omwi-report-20130329 *Conclusion:* The OIG has identified relevant information and data to gain an understanding of the entities to be audited. The information sources were policies/procedures, laws, and organizational charts. *Notes:* *Results 4:*

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
B.1.PRG - Background\Planning *Procedure Step:* 3. (b) (5) *Type:* Planning *Assigned To:* *Prepared By:* KLP, 5/18/2014 *Reviewed By:* (None) PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	*Purpose:* (b) (5) *Criteria:* GAGAS 7.04, 7.08-7.43 7.04 Auditors should use a form of the audit report that is appropriate for its intended use and is in writing or in some other retrievable form.162 For example, auditors may present audit reports using electronic media that are retrievable by report users and the audit organization. The users' needs will influence the form of the audit report. Different forms of audit reports include written reports, letters, briefing slides, or other presentation materials. **REPORT CONTENTS** 7.08 Auditors should prepare audit reports that contain (1) the objectives, scope, and methodology of the audit; (2) the audit results, including findings, conclusions, and recommendations, as appropriate; (3) a statement about the auditors' compliance with GAGAS; (4) a summary of the views of responsible officials; and (5) if applicable, the nature of any confidential or sensitive information omitted. **Objective, Scope, Methodology** 7.09 Auditors should include in the report a description of the audit objectives and the scope and methodology used for addressing the audit objectives. Report users need this information to understand the purpose of the audit, the nature and extent of the audit work performed, the context and perspective regarding what is reported, and any significant limitations in audit objectives, scope, or methodology. 7.10 Audit objectives for performance audits may vary widely. Auditors should communicate audit objectives in the audit report in a clear, specific, neutral, and unbiased manner that includes relevant assumptions. When audit objectives are limited but broader objectives could be inferred by users, auditors should state in the audit report that certain issues were outside the scope of the audit in order to avoid potential misunderstanding. 7.11 Auditors should describe the scope of the work performed and any

Summary	Detail
	limitations, including issues that would be relevant to likely users, so that they could reasonably interpret the findings, conclusions, and recommendations in the report without being misled. Auditors should also report any significant constraints imposed on the audit approach by information limitations or scope impairments, including denials or excessive delays of access to certain records or individuals. 7.12 In describing the work conducted to address the audit objectives and support the reported findings and conclusions, auditors should, as applicable, explain the relationship between the population and the items tested; identify organizations, geographic locations, and the period covered; report the kinds and sources of evidence; and explain any significant limitations or uncertainties based on the auditors' overall assessment of the sufficiency and appropriateness of the evidence in the aggregate. 7.13 In reporting audit methodology, auditors should explain how the completed audit work supports the audit objectives, including the evidence gathering and analysis techniques, in sufficient detail to allow knowledgeable users of their reports to understand how the auditors addressed the audit objectives. Auditors may include a description of the procedures performed as part of their assessment of the sufficiency and appropriateness of information used as audit evidence. Auditors should identify significant assumptions made in conducting the audit; describe comparative techniques applied; describe the criteria used; and, when sampling significantly supports the auditors' findings, conclusions, or recommendations, describe the sample design and state why the design was chosen, including whether the results can be projected to the intended population. **Report Findings** 7.14 In the audit report, auditors should present sufficient, appropriate evidence to support the findings and conclusions in relation to the audit objectives. Clearly developed findings[164] assist management and oversight officials of the audited entity in understanding the need for taking corrective action. If auditors are able to sufficiently develop the elements of a finding, they should provide recommendations for corrective action if they are significant within the context of the audit objectives. However, the extent to which the elements for a finding are developed depends on the audit

Summary	Detail
	objectives. Thus, a finding or set of findings is complete to the extent that the auditors address the audit objectives. 7.15 Auditors should describe in their report limitations or uncertainties with the reliability or validity of evidence if (1) the evidence is significant to the findings and conclusions within the context of the audit objectives and (2) such disclosure is necessary to avoid misleading the report users about the findings and conclusions. As discussed in paragraphs 6.69 through 6.72, even though the auditors may have some uncertainty about the sufficiency or appropriateness of some of the evidence, they may nonetheless determine that in total there is sufficient, appropriate evidence given the findings and conclusions. Auditors should describe the limitations or uncertainties regarding evidence in conjunction with the findings and conclusions, in addition to describing those limitations or uncertainties as part of the objectives, scope, and methodology. Additionally, this description provides report users with a clear understanding regarding how much responsibility the auditors are taking for the information. 7.16 Auditors should place their findings in perspective by describing the nature and extent of the issues being reported and the extent of the work performed that resulted in the finding. To give the reader a basis for judging the prevalence and consequences of these findings, auditors should, as appropriate, relate the instances identified to the population or the number of cases examined and quantify the results in terms of dollar value, or other measures. If the results cannot be projected, auditors should limit their conclusions appropriately. 7.17 Auditors may provide background information to establish the context for the overall message and to help the reader understand the findings and significance of the issues discussed. Appropriate background information may include information on how programs and operations work; the significance of programs and operations (e.g., dollars, impact, purposes, and past audit work, if relevant); a description of the audited entity's responsibilities; and explanation of terms, organizational structure, and the statutory basis for the program and operations. When reporting on the results of their work, auditors should disclose significant facts relevant to the objectives of their work and known to them which, if not disclosed, could mislead knowledgeable users, misrepresent the results, or conceal significant improper or illegal practices. 7.18 Auditors should also report deficiencies in internal control, instances of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements,

Summary	Detail
	or abuse that have occurred or are likely to have occurred and are significant within the context of the audit objectives. **Deficiencies in Internal Control** 7.19 Auditors should include in the audit report (1) the scope of their work on internal control and (2) any deficiencies in internal control that are significant within the context of the audit objectives and based upon the audit work performed.165 When auditors detect deficiencies in internal control that are not significant to the objectives of the audit but warrant the attention of those charged with governance, they should include those deficiencies in writing to audited entity officials. Auditors should refer to that written communication in the audit report if the written communication is separate from the audit report. When auditors detect deficiencies that do warrant the attention of those charged with governance, the determination of whether and how to communicate such deficiencies to audited entity officials is a matter of professional judgment. 7.20 In a performance audit, auditors may conclude that identified deficiencies in internal control that are significant within the context of the audit objectives are the cause of deficient performance of the program or operations being audited. In reporting this type of finding, the internal control deficiency would be described as the cause. **Fraud, Noncompliance with Provisions of Laws, Regulations, Contracts, and Grant Agreements, and Abuse** 7.21 When auditors conclude, based on sufficient, appropriate evidence, that fraud,166 noncompliance with provisions of laws, regulations, contracts or grant agreements, or abuse167 either has occurred or is likely to have occurred which is significant within the context of the audit objectives, they should report the matter as a finding. Whether a particular act is, in fact, fraud or noncompliance with provisions of laws, regulations, contracts or grant agreements may have to await final determination by a court of law or other adjudicative body. 7.22 When auditors detect instances of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that are not significant within the context of the audit objectives but warrant the attention of those charged with governance, they should communicate those findings in writing to audited entity officials. When auditors detect any

Summary	Detail
	instances of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that do not warrant the attention of those charged with governance, the auditors' determination of whether and how to communicate such instances to audited entity officials is a matter of professional judgment. 7.23 When fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse either have occurred or are likely to have occurred, auditors may consult with authorities or legal counsel about whether publicly reporting such information would compromise investigative or legal proceedings. Auditors may limit their public reporting to matters that would not compromise those proceedings and, for example, report only on information that is already a part of the public record. **Reporting Findings Directly to Parties Outside the Audited Entity** 7.24 Auditors should report known or likely fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse directly to parties outside the audited entity in the following two circumstances. a. When entity management fails to satisfy legal or regulatory requirements to report such information to external parties specified in law or regulation, auditors should first communicate the failure to report such information to those charged with governance. If the audited entity still does not report this information to the specified external parties as soon as practicable after the auditors' communication with those charged with governance, then the auditors should report the information directly to the specified external parties. b. When entity management fails to take timely and appropriate steps to respond to known or likely fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that (1) is significant to the findings and conclusions and (2) involves funding received directly or indirectly from a government agency, auditors should first report management's failure to take timely and appropriate steps to those charged with governance. If the audited entity still does not take timely and appropriate steps as soon as practicable after the auditors' communication with those charged with governance, then the auditors should report the entity's failure to take timely and appropriate steps directly to the funding

Summary	Detail
	agency. 7.25 The reporting in paragraph 7.24 is in addition to any legal requirements for the auditor to report such information directly to parties outside the audited entity. Auditors should comply with these requirements even if they have resigned or been dismissed from the audit prior to its completion. Internal audit organizations do not have a duty to report outside the audited entity unless required by law, rule, regulation, or policy. 7.26 Auditors should obtain sufficient, appropriate evidence, such as confirmation from outside parties, to corroborate assertions by management of the audited entity that it has reported such findings in accordance with laws, regulations, or funding agreements. When auditors are unable to do so, they should report such information directly as discussed in paragraphs 7.24 and 7.25. **Conclusions** 7.27 Auditors should report conclusions based on the audit objectives and the audit findings. Report conclusions are logical inferences about the program based on the auditors' findings, not merely a summary of the findings. The strength of the auditors' conclusions depends on the sufficiency and appropriateness of the evidence supporting the findings and the soundness of the logic used to formulate the conclusions. Conclusions are more compelling if they lead to the auditors' recommendations and convince the knowledgeable user of the report that action is necessary. **Recommendations** 7.28 Auditors should recommend actions to correct deficiencies and other findings identified during the audit and to improve programs and operations when the potential for improvement in programs, operations, and performance is substantiated by the reported findings and conclusions. Auditors should make recommendations that flow logically from the findings and conclusions, are directed at resolving the cause of identified deficiencies and findings, and clearly state the actions recommended. 7.29 Effective recommendations encourage improvements in the conduct of government programs and operations. Recommendations are effective when they are addressed to parties that have the authority to act and when the recommended actions are specific, practical, cost effective, and measurable. **Reporting Auditors' Compliance with GAGAS**

Summary	Detail
	7.30 When auditors comply with all applicable GAGAS requirements, they should use the following language, which represents an unmodified GAGAS compliance statement, in the audit report to indicate that they performed the audit in accordance with GAGAS. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. 7.31 When auditors do not comply with all applicable GAGAS requirements, they should include a modified GAGAS compliance statement in the audit report. For performance audits, auditors should use a statement that includes either (1) the language in 7.30, modified to indicate the requirements that were not followed or (2) language that the auditor did not follow GAGAS **Reporting Views of Responsible Officials** 7.32 Auditors should obtain and report the views of responsible officials of the audited entity concerning the findings, conclusions, and recommendations included in the audit report, as well as any planned corrective actions. 7.33 Providing a draft report with findings for review and comment by responsible officials of the audited entity and others helps the auditors develop a report that is fair, complete, and objective. Including the views of responsible officials results in a report that presents not only the auditors' findings, conclusions, and recommendations, but also the perspectives of the responsible officials of the audited entity and the corrective actions they plan to take. Obtaining the comments in writing is preferred, but oral comments are acceptable. 7.34 When auditors receive written comments from the responsible officials, they should include in their report a copy of the officials' written comments, or a summary of the comments received. When the responsible officials provide oral comments only, auditors should prepare a summary of the oral comments and provide a copy of the summary to the responsible officials to verify that the comments are accurately stated. 7.35 Auditors should also include in the report an evaluation of the

Summary	Detail
	comments, as appropriate. In cases in which the audited entity provides technical comments in addition to its written or oral comments on the report, auditors may disclose in the report that such comments were received. 7.36 Obtaining oral comments may be appropriate when, for example, there is a reporting date critical to meeting a user's needs; auditors have worked closely with the responsible officials throughout the work and the parties are familiar with the findings and issues addressed in the draft report; or the auditors do not expect major disagreements with the findings, conclusions, and recommendations in the draft, or major controversies with regard to the issues discussed in the draft report. 7.37 When the audited entity's comments are inconsistent or in conflict with the findings, conclusions, or recommendations in the draft report, or when planned corrective actions do not adequately address the auditors' recommendations, the auditors should evaluate the validity of the audited entity's comments. If the auditors disagree with the comments, they should explain in the report their reasons for disagreement. Conversely, the auditors should modify their report as necessary if they find the comments valid and supported with sufficient, appropriate evidence. 7.38 If the audited entity refuses to provide comments or is unable to provide comments within a reasonable period of time, the auditors may issue the report without receiving comments from the audited entity. In such cases, the auditors should indicate in the report that the audited entity did not provide comments. **Reporting Confidential and Sensitive Information** 7.39 If certain pertinent information is prohibited from public disclosure or is excluded from a report due to the confidential or sensitive nature of the information, auditors should disclose in the report that certain information has been omitted and the reason or other circumstances that make the omission necessary. 7.40 Certain information may be classified or may be otherwise prohibited from general disclosure by federal, state, or local laws or regulations. In such circumstances, auditors may issue a separate, classified or limited use report containing such information and distribute the report only to persons authorized by law or regulation to receive it. 7.41 Additional circumstances associated with public safety, privacy, or

Summary	Detail
	security concerns could also justify the exclusion of certain information from a publicly available or widely distributed report. For example, detailed information related to computer security for a particular program may be excluded from publicly available reports because of the potential damage that could be caused by the misuse of this information. In such circumstances, auditors may issue a limited use report containing such information and distribute the report only to those parties responsible for acting on the auditors' recommendations. In some instances, it may be appropriate to issue both a publicly available report with the sensitive information excluded and a limited use report. The auditors may consult with legal counsel regarding any requirements or other circumstances that may necessitate the omission of certain information. 7.42 Considering the broad public interest in the program or activity under audit assists auditors when deciding whether to exclude certain information from publicly available reports. When circumstances call for omission of certain information, auditors should evaluate whether this omission could distort the audit results or conceal improper or illegal practices. 7.43 When audit organizations are subject to public records laws, auditors should determine whether public records laws could impact the availability of classified or limited use reports and determine whether other means of communicating with management and those charged with governance would be more appropriate. For example, the auditors may communicate general information in a written report and communicate detailed information orally. The auditor may consult with legal counsel regarding applicable public records laws. *Source:* FRB OIG *Scope:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) *Details:* *Record of Work Done:* (b) (5) (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5) *Notes:* *Results 4:*
B.1.PRG - Background\Planning *Procedure Step:* 4. Define Objectives, Scope, and Methodology *Type:* Planning *Assigned To:* BPM *Prepared By:* SMN, 3/23/2015 *Reviewed By:* (None) PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6*	*Purpose:* Define the objectives, scope, and methodology of the audit. *Criteria:* GAGAS 6.07 - 6.10, 6.39 - 6.40, 6.83a 6.07 Auditors must plan the audit to reduce audit risk to an appropriate level for the auditors to obtain reasonable assurance that the evidence is sufficient and appropriate128 to support the auditors' findings and conclusions. This determination is a matter of professional judgment. In planning the audit, auditors should assess significance and audit risk and apply these assessments in defining the audit objectives and the scope and methodology to address those objectives. Planning is a continuous process throughout the audit. Therefore, auditors may need to adjust the audit objectives, scope, and methodology as work is being completed. In situations where the audit objectives are established by statute or legislative oversight, auditors may not have latitude to define or adjust the audit objectives or scope. 6.08 The objectives are what the audit is intended to accomplish. They identify the audit subject matter and performance aspects to be included, and may also include the potential findings and reporting elements that the auditors expect to develop. Audit objectives can be thought of as questions about the program that the auditors seek to answer based on evidence obtained and assessed against criteria. The term "program" is used in GAGAS to include government entities, organizations, programs, activities, and functions.

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
SCORECARD: *Rating:* *Sample Size:*	6.09 Scope is the boundary of the audit and is directly tied to the audit objectives. The scope defines the subject matter that the auditors will assess and report on, such as a particular program or aspect of a program, the necessary documents or records, the period of time reviewed, and the locations that will be included. 6.10 The methodology describes the nature and extent of audit procedures for gathering and analyzing evidence to address the audit objectives. Audit procedures are the specific steps and tests auditors perform to address the audit objectives. Auditors should design the methodology to obtain reasonable assurance that the evidence is sufficient and appropriate to support the auditors' findings and conclusions in relation to the audit objectives and to reduce audit risk to an acceptable level. 6.39 If auditors believe that it is likely that sufficient, appropriate evidence will not be available, they may revise the audit objectives or modify the scope and methodology and determine alternative procedures to obtain additional evidence or other forms of evidence to address the current audit objectives. Auditors should also evaluate whether the lack of sufficient, appropriate evidence is due to internal control deficiencies or other program weaknesses, and whether the lack of sufficient, appropriate evidence could be the basis for audit findings. 6.40 Auditors should determine whether other auditors have conducted, or are conducting, audits of the program that could be relevant to the current audit objectives. The results of other auditors' work may be useful sources of information for planning and performing the audit. If other auditors have identified areas that warrant further audit work or follow-up, their work may influence the auditors' selection of objectives, scope, and methodology. 6.83 Auditors should document159 the following: **a.** the objectives, scope, and methodology of the audit; *Source:* FRB OIG

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
	Details:
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Source: Board- Entrance Conference Agenda Final (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
	Notes:
	Results 4:
B.1.PRG - Background\Planning	*Purpose:* (b) (5)
Procedure Step: (b) (5) *Type:* Planning *Assigned To:* BPM *Prepared By:* BPM, 7/25/2014 *Reviewed By:* KLP, 8/1/2014	
PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6*	*Criteria:* GAGAS Appendix A, Section 6.04 - Types of Evidence A6.04 In terms of its form and how it is collected, evidence may be categorized as physical, documentary, or testimonial. Physical evidence is obtained by auditors' direct inspection or observation of people, property, or events. Such evidence may be documented in summary memos, photographs, videos, drawings, charts, maps, or physical samples. Documentary evidence is obtained in the form of already existing information such as letters, contracts, accounting records, invoices, spreadsheets, database extracts, electronically stored information, and management information on performance. Testimonial evidence is obtained through inquiries, interviews, focus groups, public forums, or questionnaires. Auditors frequently use analytical processes including computations, comparisons, separation of information into components, and rational arguments to analyze any evidence gathered to determine whether it is sufficient and appropriate. The strength and weakness of each form of evidence depends on the facts and circumstances associated with the evidence and professional judgment in the context of the audit objectives.
SCORECARD:	

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
Rating: *Sample Size:*	*Source:* Attendees: Jina Hwang, Senior OIG Counsel Tim Rogers, Senior OIG Manager Anna Saez, OIG Manager Ed Fernandez, Project Leader for CFPB Review Kim Perteet, Project Leader for Board Review Megan Taylor, Auditor Amanda Sundstrom, Auditor Brandon Lee, Auditor Brian Murphy, Auditor *Scope:* (b) (5) *Details:* *Record of Work Done:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
B.1.PRG - Background\Planning *Procedure Step:* 6. Understand Internal Controls Relevant to Project *Type:* Planning *Assigned To:* SPK *Prepared By:* SPK, 3/10/2015 *Reviewed By:* (None) **PROPERTIES:** *Location:* *Frequency:* *Category 4:*	*Purpose:* Describe the internal controls process for the program and the rationale for the extent that such controls will be evaluated and tested in the audit. *Criteria:* Board Policies Reviewed: - Equal Employment Opportunity - EEO Complaint Process and How It Works - Performance Management Program - Adverse Action - Vacant Position Posting - Discriminatory Workplace Harassment GAGAS 6.16 - 6.22 6.16 Auditors should obtain an understanding of internal control132 that is significant within the context of the audit objectives. For internal control that is significant within the context of the audit objectives, auditors should

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
User Category: *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	assess whether internal control has been properly designed and implemented and should perform procedures designed to obtain sufficient, appropriate evidence to support their assessment about the effectiveness of those controls. Information systems controls are often an integral part of an entity's internal control. The effectiveness of significant internal controls is frequently dependent on the effectiveness of information systems controls. Thus, when obtaining an understanding of internal control significant to the audit objectives, auditors should also determine whether it is necessary to evaluate information systems controls.133 6.17 The effectiveness of internal control that is significant within the context of the audit objectives can affect audit risk. Consequently, auditors may determine that it is necessary to modify the nature, timing, or extent of the audit procedures based on the auditors' assessment of internal control and the results of internal control testing. For example, poorly controlled aspects of a program have a higher risk of failure, so auditors may choose to focus more efforts in these areas. Conversely, effective controls at the audited entity may enable the auditors to limit the extent and type of audit testing needed. 6.18 Auditors may obtain an understanding of internal control through inquiries, observations, inspection of documents and records, review of other auditors' reports, or direct tests. The nature and extent of procedures auditors perform to obtain an understanding of internal control may vary among audits based on audit objectives, audit risk, known or potential internal control deficiencies, and the auditors' knowledge about internal control gained in prior audits. 6.19 The following discussion of the principal types of internal control objectives is intended to help auditors better understand internal controls and determine whether or to what extent they are significant to the audit objectives. a. Effectiveness and efficiency of program operations: Controls over program operations include policies and procedures that the audited entity has implemented to provide reasonable assurance that a program meets its objectives, while considering cost-effectiveness and efficiency. Understanding these controls can help auditors understand the program operations that convert inputs to outputs and outcomes. b. Relevance and reliability of information: Controls over the relevance and

Summary	Detail
	reliability of information include policies and procedures that officials of the audited entity have implemented to provide themselves reasonable assurance that operational and financial information they use for decision making and reporting externally is relevant and reliable and fairly disclosed in reports. Understanding these controls can help auditors (1) assess the risk that the information gathered by the entity may not be relevant or reliable and (2) design appropriate tests of the information considering the audit objectives. c. Compliance with applicable laws, regulations, contracts, and grant agreements: Controls over compliance include policies and procedures that the audited entity has implemented to provide reasonable assurance that program implementation is in accordance with provisions of laws, regulations, contracts, and grant agreements. Understanding the relevant controls concerning compliance with those laws, regulations, contracts or grant agreements that the auditors have determined are significant within the context of the audit objectives can help them assess the risk of noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse. 6.20 A subset of these categories of internal control objectives is the safeguarding of assets and resources. Controls over the safeguarding of assets and resources include policies and procedures that the audited entity has implemented to reasonably prevent or promptly detect unauthorized acquisition, use, or disposition of assets and resources. 6.21 In performance audits, a deficiency in internal control[134] exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct (1) impairments of effectiveness or efficiency of operations, (2) misstatements in financial or performance information, or (3) noncompliance with provisions of laws, regulations, contracts, or grant agreements on a timely basis. A deficiency in design exists when (a) a control necessary to meet the control objective is missing or (b) an existing control is not properly designed so that, even if the control operates as designed, the control objective is not met. A deficiency in operation exists when a properly designed control does not operate as designed, or when the necessary authority or qualifications to perform the control effectively. 6.22 Internal auditing is an important part of overall governance, accountability, and internal control. A key role of many internal audit organizations is to provide assurance that internal controls are in place to adequately mitigate risks and achieve

Summary	Detail
	program goals and objectives. The auditor may determine that it is appropriate to use the work of the internal auditors in the auditor's assessment of the effectiveness of design or operation of internal controls that are significant within the context of the audit objectives. *Source:* FRB OIG GAO Government Auditing Standards Board policies *Scope:* (b) (5) *Details:* *Record of Work Done:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
	Background (b) (5) (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
B.1.PRG - Background\Planning *Procedure Step:* 7. Board's Internal Controls (Policies and	*Purpose:* To summarize the audit approach to evaluating the Board's internal controls, specifically the agency's policies and procedures. These

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
Procedures)		controls may contribute to the prevention of bias or discrimination within the human resources-related activities or functions.
Type:	Planning	
Assigned To:	SPK	*Criteria:*
Prepared By:	SPK, 3/10/2015	See criteria in Record of Work Done.
Reviewed By:	(None)	
		Source:
PROPERTIES:		See sources in Record of Word Done.
Location:		
Frequency:		*Scope:*
Category 4:		Audit objective: To assess the Board's human resources–related functions and other efforts to provide for equal employment opportunities, including equal opportunity for minorities and women to obtain senior management positions, and increase racial, ethnic, and gender diversity in the workforce.
User Category:		
Category 5		
Category 6		
		Details:
SCORECARD:		
Rating:		*Record of Work Done:*
Sample Size:		(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
B.1.PRG - Background\Planning *Procedure Step:* 8. Identify Relevant Criteria *Type:* Planning *Assigned To:* *Prepared By:* SMN, 3/26/2015 *Reviewed By:* KLP, 3/26/2015 PROPERTIES: *Location:* *Frequency:* *Category 4:*	*Purpose:* Describe the laws, regulations, policies, standards, measures, expectations, best practices, and/or benchmarks against which performance is to be compared and evaluated. *Criteria:* GAGAS 6.12a, 6.15b, 6.37 6.12 During planning, auditors should also **(a)** identify the potential criteria needed to evaluate matters subject to audit; 6.15 Obtaining an understanding of the program under audit helps auditors to assess the relevant risks associated with the program and the impact of the risks on the audit objectives, scope, and methodology. The auditors' understanding may come from knowledge they already have about the program or knowledge they gain from inquiries, observations, and

Summary	Detail
User Category: *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	reviewing documents while planning the audit. The extent and breadth of those inquiries and observations will vary among audits based on the audit objectives, as will the need to understand individual aspects of the program, such as the following: (**b)** Purpose and goals: Purpose is the result or effect that is intended or desired from a program's operation. Legislatures usually establish the program's purpose when they provide authority for the program. Entity officials may provide more detailed information on the program's purpose to supplement the authorizing legislation. Entity officials are sometimes asked to set goals for program performance and operations, including both output and outcome goals. Auditors may use the stated program purpose and goals as criteria for assessing program performance or may develop additional criteria to use when assessing performance. 6.37 Auditors should identify criteria. Criteria represent the laws, regulations, contracts, grant agreements, standards, specific requirements, measures, expected performance, defined business practices, and benchmarks against which performance is compared or evaluated. Criteria identify the required or desired state or expectation with respect to the program or operation. Criteria provide a context for evaluating evidence and understanding the findings, conclusions, and recommendations included in the report. Auditors should use criteria that are relevant to the audit objectives and permit consistent assessment of the subject matter *Source:* Dodd_Frank_Act_Section_342 EEO MD 715 Guidance on establishingAffirmative programs of EEO Executive Order 13583 On Diversity 5 USC 43 Performance Appraisal Board EEO Policy

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Board PMP Policy (Including Appeals Process) Board Adverse Action Policy Instructions to Federal Agencies for EEO MD-715 Section I Title VII of the Civil Rights Act of 1964 12 CFR Part 268 Board EEO Policy Board PMP Policy (Including Appeals Process) Board Adverse Action Policy ItB Office of Diversity and Inclusion - EEO Complaint System and How It Works EEO Complaint Process *Scope:* To identify and summarize relevant laws, regulations, and applicable criteria that could prove relevant for the audit on the Board's diversity and inclusion processes. *Details:* *Record of Work Done:* **Meeting(s) with Knowledgable Stakeholders:**

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
B.1.PRG - Background\Planning *Procedure Step:* 9. Consider Results of Prior Work *Type:* Planning *Assigned To:* BPM *Prepared By:* BPM, 6/5/2014 *Reviewed By:* KLP, 2/26/2015 PROPERTIES:	*Purpose:* If applicable, describe how this audit relates to prior OIG work, including the presence of any prior OIG recommendations (open or closed). Determine whether any work steps will be performed to test actions taken as a result of prior OIG work. *Criteria:* GAGAS 6.36 6.36 Auditors should evaluate whether the audited entity has taken appropriate corrective action to address findings and recommendations from previous engagements that are significant within the context of the

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
Location: *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	audit objectives. When planning the audit, auditors should ask management of the audited entity to identify previous audits, attestation engagements, performance audits, or other studies that directly relate to the objectives of the audit, including whether related recommendations have been implemented. Auditors should use this information in assessing risk and determining the nature, timing, and extent of current audit work, including determining the extent to which testing the implementation of the corrective actions is applicable to the current audit objectives. *Source:* The OIG reviewed its public website for any reports issued related to CFPB personnel practices. See http://www.federalreserve.gov/oig/, Reports section. *Scope:* All OIG reports issued as of June 5, 2014. *Details:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Notes: *Results 4:*
B.1.PRG - Background\Planning *Procedure Step:* 10. Identify Potential Sources of Data *Type:* Planning *Assigned To:* BPM *Prepared By:* BPM, 7/31/2014 *Reviewed By:* KLP, 8/1/2014 PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	*Purpose:* Describe the decision made regarding planned data sources, how the information will be obtained, and how the information will be used and analyzed to answer the audit objective(s). *Criteria:* GAGAS 6.38 - 6.39 6.38 Auditors should identify potential sources of information that could be used as evidence. Auditors should determine the amount and type of evidence needed to obtain sufficient, appropriate evidence to address the audit objectives and adequately plan audit work. 6.39 If auditors believe that it is likely that sufficient, appropriate evidence will not be available, they may revise the audit objectives or modify the scope and methodology and determine alternative procedures to obtain additional evidence or other forms of evidence to address the current audit objectives. Auditors should also evaluate whether the lack of sufficient, appropriate evidence is due to internal control deficiencies or other program weaknesses, and whether the lack of sufficient, appropriate evidence could be the basis for audit finding. *Source:* Public Board Reports: Board EEO 1 Reports No FEAR Act Reporting HR Analytics:

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	PeopleSoft Data PeopleFluent <u>Employee Relations:</u> E-Relations Database <u>ODI/OMWI Office:</u> Data compiled from PeopleSoft and PeopleFluent *Scope:* (b) (5) *Details:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
B.1.PRG - Background\Planning *Procedure Step:* 11. Consider Information System Controls *Type:* Planning *Assigned To:* BPM *Prepared By:* BPM, 7/31/2014 *Reviewed By:* KLP, 8/1/2014 PROPERTIES: *Location:* *Frequency:*	*Purpose:* (b) (5) *Criteria:* GAGAS 6.23 - 6.27 6.23 Understanding information systems controls is important when information systems are used extensively throughout the program under audit and the fundamental business processes related to the audit objectives rely on information systems. Information systems controls consist of those internal controls that are dependent on information systems processing and include general controls, application controls, and user controls. a. Information systems general controls (entitywide, system, and application

Summary	Detail
Category 4: *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	levels) are the policies and procedures that apply to all or a large segment of an entity's information systems. General controls help ensure the proper operation of information systems by creating the environment for proper operation of application controls. General controls include security management, logical and physical access, configuration management, segregation of duties, and contingency planning. b. Application controls, sometimes referred to as business process controls, are those controls that are incorporated directly into computer applications to help ensure the validity, completeness, accuracy, and confidentiality of transactions and data during application processing. Application controls include controls over input, processing, output, master file, interface, and data management system controls. c. User controls are portions of controls that are performed by people interacting with information system controls. A user control is an information system control if its effectiveness depends on information systems processing or the reliability (accuracy, completeness, and validity) of information processed by information systems. 6.24 An organization's use of information systems controls may be extensive; however, auditors are primarily interested in those information systems controls that are significant to the audit objectives. Information systems controls are significant to the audit objectives if auditors determine that it is necessary to evaluate the effectiveness of information systems controls in order to obtain sufficient, appropriate evidence. When information systems controls are determined to be significant to the audit objectives or when the effectiveness of significant controls is dependent on the effectiveness of information systems controls, auditors should then evaluate the design and operating effectiveness of such controls. This evaluation would include other information systems controls that impact the effectiveness of the significant controls or the reliability of information used in performing the significant controls. Auditors should obtain a sufficient understanding of information systems controls necessary to assess audit risk and plan the audit within the context of the audit objectives. 6.25 Audit procedures to evaluate the effectiveness of significant information systems controls include (1) gaining an understanding of the system as it relates to the information and (2) identifying and evaluating the general, application, and user

Summary	Detail
	controls that are critical to providing assurance over the reliability of the information required for the audit. 6.26 The evaluation of information systems controls may be done in conjunction with the auditors' consideration of internal control within the context of the audit objectives[137] or as a separate audit objective or audit procedure, depending on the objectives of the audit. Depending on the significance of information systems controls to the audit objectives, the extent of audit procedures to obtain such an understanding may be limited or extensive. In addition, the nature and extent of audit risk related to information systems controls are affected by the nature of the hardware and software used, the configuration of the entity's systems and networks, and the entity's information systems strategy. 6.27 Auditors should determine which audit procedures related to information systems controls are needed to obtain sufficient, appropriate evidence to support the audit findings and conclusions. The following factors may assist auditors in making this determination: a. The extent to which internal controls that are significant to the audit depend on the reliability of information processed or generated by information systems. b. The availability of evidence outside the information system to support the findings and conclusions: It may not be possible for auditors to obtain sufficient, appropriate evidence without evaluating the effectiveness of relevant information systems controls. For example, if information supporting the findings and conclusions is generated by information systems or its reliability is dependent on information systems controls, there may not be sufficient supporting or corroborating information or documentary evidence that is available other than that produced by the information systems. c. The relationship of information systems controls to data reliability: To obtain evidence about the reliability of computer-generated information, auditors may decide to evaluate the effectiveness of information systems controls as part of obtaining evidence about the reliability of the data. If the auditor concludes that information systems controls are effective, the auditor may reduce the extent of direct testing of data. d. Evaluating the effectiveness of information systems controls as an audit objective: When evaluating the effectiveness of information systems

Summary	Detail
	controls is directly a part of an audit objective, auditors should test information systems controls necessary to address the audit objectives. For example, the audit may involve the effectiveness of information systems controls related to certain systems, facilities, or organizations. *Source:* Conversation with Board HR Analytics Manager Lewis Andrews, see RE Follow-up Question -FRSONLY- PeopleFluent Flyer Brochure, see wp peoplefluent_brochure E-mails with OIG Office of Audits Manager Khalid Hasan, see wp IT Data Reliability_PeopleSoft OIG's own internal data assessment form, see wp Data Reliability Assessment form Final - Jun 13, 2014 *Scope:* Evaluate methods that could be used to ensure data reliability assessments are completed for each source the OIG may use for the Board's Congressional Request of Personnel Practices. *Details:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

Summary	Detail
	Results 4:
B.1.PRG - Background\Planning *Procedure Step:* 12. Consider Work Performed by Others *Type:* Planning *Assigned To:* BPM *Prepared By:* SMN, 3/26/2015 *Reviewed By:* KLP, 3/26/2015 PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	*Purpose:* Describe the extent that relevant work done by GAO, other audit organizations or experts can/will be used to satisfy any work steps. *Criteria:* GAGAS 6.40 - 6.44 6.40 Auditors should determine whether other auditors have conducted, or are conducting, audits of the program that could be relevant to the current audit objectives. The results of other auditors' work may be useful sources of information for planning and performing the audit. If other auditors have identified areas that warrant further audit work or follow-up, their work may influence the auditors' selection of objectives, scope, and methodology. 6.41 If other auditors have completed audit work related to the objectives of the current audit, the current auditors may be able to use the work of the other auditors to support findings or conclusions for the current audit and, thereby, avoid duplication of efforts. If auditors use the work of other auditors, they should perform procedures that provide a sufficient basis for using that work. Auditors should obtain evidence concerning the other auditors' qualifications and independence and should determine whether the scope, quality, and timing of the audit work performed by the other auditors is adequate for reliance in the context of the current audit objectives. Procedures that auditors may perform in making this determination include reviewing the other auditors' report, audit plan, or audit documentation, and/or performing tests of the other auditors' work. The nature and extent of evidence needed will depend on the significance of the other auditors' work to the current audit objectives and the extent to which the auditors will use that work.143 6.42 Some audits may necessitate the use of specialized techniques or methods that require the skills of a specialist. Specialists to whom this

Summary	Detail
	section applies include, but are not limited to, actuaries, appraisers, attorneys, engineers, environmental consultants, medical professionals, statisticians, geologists, and information technology experts. If auditors intend to use the work of specialists, they should assess the professional qualifications and independence of the specialists. 6.43 Auditors' assessment of professional qualifications of the specialist involves the following: a. the professional certification, license, or other recognition of the competence of the specialist in his or her field, as appropriate; b. the reputation and standing of the specialist in the views of peers and others familiar with the specialist's capability or performance; c. the specialist's experience and previous work in the subject matter; and d. the auditors' prior experience in using the specialist's work. 6.44 Auditors' assessment of the independence of specialists who perform audit work includes identifying threats and applying any necessary safeguards in the same manner as they would for auditors performing work on those audits *Source:* GAO-13-328 Diversity Management GAO-09-110 Federal SES Diversity GAO-05-90 Diversity Management Expert -Ientified Leading practices and Agency Examples EPA-ocr 20110321 finalreport GPO 9.2008 OIG Diversity Management Programs Report GAO-08-116T OPM nofearact

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	GAO-13-830SP Standards for Internal Control *Scope:* (b) (5) *Details:* *Record of Work Done:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
B.1.PRG - Background\Planning *Procedure Step:* (b) (5) *Type:* Planning *Assigned To:* BPM *Prepared By:* BPM, 7/29/2014 *Reviewed By:* KLP, 8/1/2014 PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD:	*Purpose:* *Criteria:* CPE Requirements for Specialists 3.79 The audit team should determine that external specialists assisting in performing a GAGAS audit are qualified and competent in their areas of specialization; however, external specialists are not required to meet the GAGAS CPE requirements. 3.80 The audit team should determine that internal specialists consulting on a GAGAS audit who are not involved in directing, performing audit procedures, or reporting on a GAGAS audit, are qualified and competent in their areas of specialization; however, these internal specialists are not required to meet the GAGAS CPE requirements. 3.81 The audit team should determine that internal specialists, who are performing work in accordance with GAGAS as part of the audit team, including directing, performing audit procedures, or reporting on a GAGAS audit, comply with GAGAS, including the CPE requirements.41 The GAGAS CPE requirements become effective for internal specialists when an audit organization first assigns an internal specialist to an audit. Because internal specialists apply specialized knowledge in government audits, training in their areas of specialization qualify under the requirement for 24 hours of CPE that directly relates to government auditing, the government

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
Rating: *Sample Size:*	environment, or the specific or unique environment in which the audited entity operates. (b) (5) *Details:* *Record of Work Done:* (b) (6) *Conclusion:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Notes: *Results 4:*
B.1.PRG - Background\Planning *Procedure Step:* 14. Use of External Auditors/Consultants *Type:* Planning *Assigned To:* BPM *Prepared By:* KLP, 4/10/2015 *Reviewed By:* (None) PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	*Purpose:* (b) (5) [redacted] *Criteria:* GAGAS 3.28 - 3.30, 6.42 - 6.46 3.28 Audit organizations that are structurally located within government entities are often subject to constitutional or statutory safeguards that mitigate the effects of structural threats to independence. For external audit organizations, such safeguards may include governmental structures under which a government audit organization is: a. at a level of government other than the one of which the audited entity is part (federal, state, or local); for example, federal auditors auditing a state government program; or b. placed within a different branch of government from that of the audited entity; for example, legislative auditors auditing an executive branch program. **3.29 Safeguards other than those described above may mitigate threats resulting from governmental structures. For external auditors or auditors who report both externally and internally, structural threats may be mitigated if the head of an audit organization meets any of the following criteria in accordance with constitutional or statutory requirements:** a. directly elected by voters of the jurisdiction being audited; b. elected or appointed by a legislative body, subject to removal by a legislative body, and reports the results of audits to and is accountable to a legislative body; c. appointed by someone other than a legislative body, so long as the appointment is confirmed by a legislative body and removal from the position is subject to

Summary	Detail
	oversight or approval by a legislative body, and reports the results of audits to and is accountable to a legislative body; or d. appointed by, accountable to, reports to, and can only be removed by a statutorily created governing body, the majority of whose members are independently elected or appointed and are outside the organization being audited. 3.30 In addition to the criteria in paragraphs 3.28 and 3.29, GAGAS recognizes that there may be other organizational structures under which external audit organizations in government entities could be considered to be independent. If appropriately designed and implemented, these structures provide safeguards that prevent the audited entity from interfering with the audit organization's ability to perform the work and report the results impartially. For an external audit organization or one that reports both externally and internally to be considered independent under a structure different from the ones listed in paragraphs 3.28 and 3.29, the audit organization should have all of the following safeguards. In such situations, the audit organization should document how each of the following safeguards was satisfied and provide the documentation to those performing quality control monitoring and to the external peer reviewers to determine whether all the necessary safeguards are in place. The following safeguards may also be used to augment those listed in paragraphs 3.28 and 3.29: a. statutory protections that prevent the audited entity from abolishing the audit organization; b. statutory protections that require that if the head of the audit organization is removed from office, the head of the agency reports this fact and the reasons for the removal to the legislative body; c. statutory protections that prevent the audited entity from interfering with the initiation, scope, timing, and completion of any audit; d. statutory protections that prevent the audited entity from interfering with audit reporting, including the findings and conclusions or the manner, means, or timing of the audit organization's reports; e. statutory protections that require the audit organization to report to a legislative body or other independent governing body on a recurring basis; f. statutory protections that give the audit organization sole authority over the selection, retention, advancement, and dismissal of its staff; and g. statutory access to records and documents related to the agency, program, or function being audited and access to government officials or

Summary	Detail
	other individuals as needed to conduct the audit. 6.42 Some audits may necessitate the use of specialized techniques or methods that require the skills of a specialist. Specialists to whom this section applies include, but are not limited to, actuaries, appraisers, attorneys, engineers, environmental consultants, medical professionals, statisticians, geologists, and information technology experts. If auditors intend to use the work of specialists, they should assess the professional qualifications and independence of the specialists. 6.43 Auditors' assessment of professional qualifications of the specialist involves the following: a. the professional certification, license, or other recognition of the competence of the specialist in his or her field, as appropriate; b. the reputation and standing of the specialist in the views of peers and others familiar with the specialist's capability or performance; c. the specialist's experience and previous work in the subject matter; and d. the auditors' prior experience in using the specialist's work. 6.44 Auditors' assessment of the independence of specialists who perform audit work includes identifying threats and applying any necessary safeguards in the same manner as they would for auditors performing work on those audits. 6.45 Audit management should assign sufficient staff and specialists with adequate collective professional competence to perform the audit.145 Staffing an audit includes, among other things: a. assigning staff and specialists with the collective knowledge, skills, and experience appropriate for the job, b. assigning a sufficient number of staff and supervisors to the audit, c. providing for on-the-job training of staff, and d. engaging specialists when necessary. 6.46 If planning to use the work of a specialist, auditors should document the nature and scope of the work to be performed by the specialist, including a. the objectives and scope of the specialist's work, b. the intended use of the specialist's work to support the audit objectives, c. the specialist's procedures and findings so they can be evaluated and related to other planned audit procedures, and

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	d. the assumptions and methods used by the specialist. *Source:* OIG Inspector General Statement of Work Agreements with external consultants. *Scope:* OIG audit of the Board's Diversity and Incusion processes. *Details:* *Record of Work Done:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5), (b) (6)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5), (b) (6)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
B.1.PRG - Background\Planning *Procedure Step:* 15. Assess Risk *Type:* Planning *Assigned To:* BPM *Prepared By:* BPM, 8/1/2014 *Reviewed By:* (None) PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	*Purpose:* Describe how audit risk will be reduced to an appropriate level to provide reasonable assurance that the evidence is sufficient and appropriate to support the findings and conclusions. Consider the potential for: (a) violations of law or regulatory requirements, contract provisions, grant agreements and the rationale for how such areas will be addressed in work steps. (b) fraud, waste and abuse and the rationale for how such areas will be addressed in work steps. (b) (5) *Criteria:* GAGAS 6.05, 6.07, 6.10-6.11, 6.28-6.34 6.05 Audit risk is the possibility that the auditors' findings, conclusions, recommendations, or assurance may be improper or incomplete, as a result of factors such as evidence that is not sufficient and/or appropriate, an inadequate audit process, or intentional omissions or misleading information due to misrepresentation or fraud. The assessment of audit risk involves both qualitative and quantitative considerations. Factors impacting audit risk include the time frames, complexity, or sensitivity of the work; size of the program in terms of dollar amounts and number of citizens served; adequacy of the audited entity's systems and processes to detect inconsistencies, significant errors, or fraud; and auditors' access to records. Audit risk includes the risk that auditors will not detect a mistake, inconsistency, significant error, or fraud in the evidence supporting the audit. Audit risk can be reduced by taking actions such as increasing the scope of work; adding specialists, additional reviewers, and other resources to perform the audit; changing the methodology to obtain additional evidence, higher quality evidence, or alternative forms of corroborating evidence; or aligning the findings and conclusions to reflect the evidence obtained.

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	6.07 Auditors must plan the audit to reduce audit risk to an appropriate level for the auditors to obtain reasonable assurance that the evidence is sufficient and appropriate[128] to support the auditors' findings and conclusions. This determination is a matter of professional judgment. In planning the audit, auditors should assess significance and audit risk and apply these assessments in defining the audit objectives and the scope and methodology to address those objectives. Planning is a continuous process throughout the audit. Therefore, auditors may need to adjust the audit objectives, scope, and methodology as work is being completed. In situations where the audit objectives are established by statute or legislative oversight, auditors may not have latitude to define or adjust the audit objectives or scope. 6.10 The methodology describes the nature and extent of audit procedures for gathering and analyzing evidence to address the audit objectives. Audit procedures are the specific steps and tests auditors perform to address the audit objectives. Auditors should design the methodology to obtain reasonable assurance that the evidence is sufficient and appropriate to support the auditors' findings and conclusions in relation to the audit objectives and to reduce audit risk to an acceptable level. 6.11 Auditors should assess audit risk and significance within the context of the audit objectives by gaining an understanding of the following: a. the nature and profile of the programs and the needs of potential users of the audit report; b. internal control as it relates to the specific objectives and scope of the audit; c. information systems controls for purposes of assessing audit risk and planning the audit within the context of the audit objectives; d. provisions of laws, regulations, contracts, and grant agreements, and potential fraud, and abuse that are significant within the context of the audit objectives; e. ongoing investigations or legal proceedings within the context of the audit objectives; and f. the results of previous audits and attestation engagements that directly relate to the current audit objectives

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	6.28 Auditors should identify any provisions of laws, regulations, contracts or grant agreements that are significant within the context of the audit objectives and assess the risk that noncompliance with provisions of laws, regulations, contracts or grant agreements could occur.138 Based on that risk assessment, the auditors should design and perform procedures to obtain reasonable assurance of detecting instances of noncompliance with provisions of laws, regulations, contracts, or grant agreements that are significant within the context of the audit objectives. 6.29 The auditors' assessment of audit risk may be affected by such factors as the complexity or newness of the laws, regulations, contracts or grant agreements. The auditors' assessment of audit risk also may be affected by whether the entity has controls that are effective in preventing or detecting noncompliance with provisions of laws, regulations, contracts, or grant agreements. If auditors obtain sufficient, appropriate evidence of the effectiveness of these controls, they can reduce the extent of their tests of compliance. 6.31 When auditors identify factors or risks related to fraud that has occurred or is likely to have occurred that they believe are significant within the context of the audit objectives, they should design procedures to obtain reasonable assurance of detecting any such fraud. Assessing the risk of fraud is an ongoing process throughout the audit and relates not only to planning the audit but also to evaluating evidence obtained during the audit. 6.32 When information comes to the auditors' attention indicating that fraud, significant within the context of the audit objectives, may have occurred, auditors should extend the audit steps and procedures, as necessary, to (1) determine whether fraud has likely occurred and (2) if so, determine its effect on the audit findings. If the fraud that may have occurred is not significant within the context of the audit objectives, the auditors may conduct additional audit work as a separate engagement, or refer the matter to other parties with oversight responsibility or jurisdiction 6.33 Abuse involves behavior that is deficient or improper when compared with behavior that a prudent person would consider reasonable and necessary business practice given the facts and circumstances. Abuse also includes misuse of authority or position for personal financial interests or those of an immediate or close family member or business associate.140 Abuse does not necessarily involve fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements.

Summary	Detail
	6.34 Because the determination of abuse is subjective, auditors are not required to detect abuse in performance audits. However, as part of a GAGAS audit, if auditors become aware of abuse that could be quantitatively or qualitatively significant to the program under audit, auditors should apply audit procedures specifically directed to ascertain the potential effect on the program under audit within the context of the audit objectives. After performing additional work, auditors may discover that the abuse represents potential fraud or noncompliance with provisions of laws, regulations, contracts, or grant agreements. *Source:* Auditor Developed Matrix *Scope:* Any risk factors likely to be encountered during the course of the OIG's Audit of Board Personnel Practices including (data reliability, lack of sufficient evidence, complexity of the subject matter, potential for fraud, waste, and abuse). *Details:* *Record of Work Done:* GAGAS defines audit risk as "the possibility that the auditors' findings, conclusions, recommendations, or assurance may be improper or incomplete, as a result of factors such as evidence that is not sufficient and/or appropriate, an inadequate audit process, or intentional omissions or misleading information due to misrepresentation or fraud." The OIG will assess audit risk using the below risk model. The risk model states: Audit Risk = Inherent Risk x Control Risk x Detection Risk. a) Inherent Risk: The probability that an error (whether intentional or

Summary	Detail
	unintentional) exists assuming that there are no related controls. b) Control Risk: The probability that an error (whether intentional or unintentional) will not be prevented or detected on a timely basis by the entity's internal control. c) Detection Risk: The probability that an error (whether intentional or unintentional) will not be detected by the auditor. (b) (5) *Conclusion:* (b) (5) *Notes:* *Results 4:*
B.1.PRG - Background\Planning	*Purpose:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary		Detail
Procedure Step:	16. Fraud Discussion	(b) (5)
Type:	Planning	
Assigned To:	BPM	*Criteria:*
Prepared By:	BPM, 7/28/2014	GAGAS 6.30
Reviewed By:	KLP, 8/1/2014	In planning the audit, auditors should assess risks of fraud occurring that is significant within the context of the audit objectives. Fraud involves obtaining something of value through willful misrepresentation.
PROPERTIES:		Whether an act is, in fact, fraud is a determination to be made through the judicial or other adjudicative system and is beyond auditors' professional responsibility. Audit team members should discuss among the team fraud risks, including factors such as individuals' incentives or pressures to commit fraud, the opportunity for fraud to occur, and rationalizations or attitudes that could allow individuals to commit fraud. Auditors should gather and assess information to identify risks of fraud that are significant within the scope of the audit objectives or that could affect the findings and conclusions. For example, auditors may obtain information through discussion with officials of the audited entity or through other means to determine the susceptibility of the program to fraud, the status of internal controls the audited entity has established to prevent and detect fraud, or the risk that officials of the audited entity could override internal control. An attitude of professional skepticism in assessing these risks assists auditors in assessing which factors or risks could significantly affect the audit objectives.
Location:		
Frequency:		
Category 4:		
User Category:		
Category 5		
Category 6		
SCORECARD:		
Rating:		
Sample Size:		*Source:*
		Date: 6/24/2014 Time: 9:00 AM Location: K-2737 OIG Participants: Anna Saez Kimberly Perteet

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (6) Megan Taylor Geeta Mullaney Jina Hwang Brian Murphy Ed Fernandez Amanda Sundstrom (b) (6) *Scope:* (b) (5) *Details:* *Record of Work Done:* (b) (5) *Conclusion:* (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
B.1.PRG - Background\Planning *Procedure Step:* (b) (5) *Type:* *Assigned To:* BPM *Prepared By:* BPM, 7/29/2014 *Reviewed By:* KLP, 8/1/2014 PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5*	*Purpose:* (b) (5) *Criteria:* Ongoing Investigations and Legal Proceedings 6.35 Avoiding interference with investigations or legal proceedings is important in pursuing indications of fraud, noncompliance with provisions of laws, regulations, contracts or grant agreements, or abuse. Laws, regulations, and policies may require auditors to report indications of certain types of fraud, noncompliance with provisions of laws, regulations,contracts, or grant agreements, or abuse to law enforcement or investigatory authorities before performing additional audit procedures. When investigations or legal proceedings are initiated or in process, auditors should evaluate the impact on the current audit. In some cases, it may be appropriate for the auditors to work with investigators or legal authorities, or withdraw from or defer further work on the audit or a portion of the audit to avoid interfering with an ongoing investigation or legal proceeding.

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
Category 6 SCORECARD: *Rating:* *Sample Size:*	*Source:* Participants: Larry Valett, Associate IG for Investigations Kim Perteet, Project Lead (Board Audit) Brian Murphy, Auditor (Board Audit) Amanda Sundstrom, Auditor (CFPB Audit) *Scope:* (b) (5) (b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	(b) (5)
B.1.PRG - Background\Planning *Procedure Step:* 18. Coordinate with Legal on Ongoing Legal Proceedings *Type:* *Assigned To:* BPM *Prepared By:* BPM, 7/29/2014 *Reviewed By:* KLP, 8/1/2014 PROPERTIES: *Location:* *Frequency:* *Category 4:* *User Category:* *Category 5* *Category 6* SCORECARD: *Rating:* *Sample Size:*	*Purpose:* The purpose of coordinating with OIG Legal/Board Legal is to determine whether any ongoing legal proceedings related to diversity could potentially impact the work of audit team. *Criteria:* Ongoing Investigations and Legal Proceedings 6.35 Avoiding interference with investigations or legal proceedings is important in pursuing indications of fraud, noncompliance with provisions of laws, regulations, contracts or grant agreements, or abuse. Laws, regulations, and policies may require auditors to report indications of certain types of fraud, noncompliance with provisions of laws, regulations,contracts, or grant agreements, or abuse to law enforcement or investigatory authorities before performing additional audit procedures. When investigations or legal proceedings are initiated or in process, auditors should evaluate the impact on the current audit. In some cases, it may be appropriate for the auditors to work with investigators or legal authorities, or withdraw from or defer further work on the audit or a portion of the audit to avoid interfering with an ongoing investigation or legal proceeding. *Source:* Kit Wheatley, Associate General Counsel, 202-452-3779 Geeta Mullaney, OIG Attorney, 202-475-6663 *Scope:* Any ongoing legal proceedings at the Board related to the audit objective that could impact the completion of the audit program.

The Board Can Enhance Its Diversity and Inclusion Efforts

Summary	Detail
	Details: *Record of Work Done:* (b) (5)

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

To assess the Board's personnel operations and other efforts to provide for equal employment opportunities, including equal opportunity for minorities and women to obtain senior management positions, and increase racial, ethnic, and gender diversity in the workforce.

(b) (5)

Fieldwork Program: Personnel Operations, Policies, and Procedures

Procedure Title	Record of Work Done	Comments Where Applicable	Auditor-in-Charge

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

Hiring - Gain an Understanding of the Process	(b) (5)	Sean Newman
For Divisions that exclude Human Capital in Some Hiring Processes		Kim Perteet Sopeany Keo
Hiring - Test Compliance with Applicable Laws, Regulations, and Best Practices		Kim Perteet Sopeany Keo
Hiring - Test Internal Controls		Sean Newman Sopeany Keo

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

	(b) (5)	Kim Perteet (Please check to see if Sopeany has conducted any work on this to prevent duplicative work)
Hiring – Document Alleged or Proven Bias or Discrimination		Sean Newman Sopeany Keo Kim Perteet
Performance Management - Gain an Understanding of the Process		Brian Murphy

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

	(b) (5)	
Performance Management - Test Compliance with Applicable Laws, Regulations, and Best Practices		Sopeany Keo Kim Perteet
Performance Management - Test Internal Controls		Sopeany Keo Brian Murphy Kim Perteet
Performance Management - Document instances of Alleged or Proven Bias or Discrimination		Sopeany Keo Kim Perteet
Promotions - Gain an Understanding of the Process		Brian Murphy

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

	(b) (5)	
Promotions - Test Compliance with Applicable Laws, Regulations, and Best Practices		Sean Newman
Promotions - Test Internal Controls		Sean Newman
Promotions – Document Alleged or Proven Bias or Discrimination		Sean Newman
Employee Satisfaction Surveys		Sean Newman

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

	(b) (5)	
EEO Complaints - Gain an Understanding of the Process		Brian Murphy

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

EEO Complaints - Test Compliance with Applicable Laws, Regulations, and Best Practices	(b) (5)	Sean Newman
EEO Complaints - Test Internal Controls		Sopeany Keo
EEO Complaints - Identify Alleged or Proven Bias or Discrimination		Kim Perteet Brian Murphy
Non-EEO Complaints - Gain an Understanding of the Process	(b) (5)	Brian Murphy

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

	(b) (5)	
Non-EEO Complaints - Test Compliance with Applicable Laws, Regulations, and Best Practices		Sopeany Keo
Non-EEO Complaints - Test Internal Controls		Sopeany Keo
Non-EEO Complaints – Document Alleged or Proven Bias or Discrimination		Brian Murphy Kim Perteet
Employee Exit Interview		

Fieldwork Program: OMWI

Procedure Title	Error! Unknown document property name.	Comments Where Applicable	Auditor-in-Charge

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

OWMI - Gain an understanding of the Office	(b) (5)		Sean Newman
OMWI - Test Compliance with Laws, Regulations, and Best Practices			Sean Newman

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

	(b) (5)	
OMWI - Test Internal Controls		Sean Newman
Efforts to Increase Diversity - OMWI		Sean Newman

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

	(b) (5)	
Diversity Training - OMWI		Sean Newman
Communications and Awareness - OMWI		Sean Newman
Management's Response to GAO Recommendation(s) - OMWI		Sean Newman

Fieldwork Program: Data Analyses

Procedure Title	Error! Unknown document property name.	Comments Where Applicable	Auditor-in-Charge
Workforce Demographics - Data Collection	(b) (5)		Brian Murphy Victor Calderon
Workforce Demographics - Data Reliability			Brian Murphy Victor Calderon

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

	(b) (5)	
Workforce Demographics - Data Analyses		Brian Murphy Victor Calderon
Hiring - Data Collection		Brian Murphy Victor Calderon
Hiring - Data Reliability		Brian Murphy Victor Calderon
Hiring - Data Analyses		Brian Murphy Victor Calderon

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

	(b) (5)	
Performance Management - Data Collection		Brian Murphy Victor Calderon
Performance Management - Data Reliability		Brian Murphy Victor Calderon
Performance Management - Data Analyses		Brian Murphy Victor Calderon

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

	(b) (5)	
Promotions - Data Collection		Brian Murphy Victor Calderon
Promotions - Data Reliability		Brian Murphy Victor Calderon
Promotions - Data Analyses		Brian Murphy Victor Calderon

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

	(b) (5)	
EEO Complaints - Data Collection		Sopeany Keo Brian Murphy
EEO Complaints - Data Reliability		Sopeany Keo Brian Murphy
EEO Complaints - Data Analyses		Sopeany Keo Brian Murphy
Non-EEO Complaints - Data Collection		\Brian Murphy Victor Calderon
Non-EEO Complaints - Data Reliability		Brian Murphy Victor Calderon
Non-EEO Complaints - Data Analyses		Brian Murphy Victor Calderon

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

	(b) (5)	
EEO and Non-EEO complaints related to PMP		Sopeany Keo Brian Murphy
Separation - Data Collection		Brian Murphy Victor Calderon
Separation - Data Reliability		Brian Murphy Victor Calderon
Separation - Data Analyses		Brian Murphy Victor Calderon

Fieldwork Program: Management's Efforts

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

Procedure Title	Error! Unknown document property name.	Comments Where Applicable	Auditor-in-Charge
Efforts to Respond to EEO Complaints - EEO	(b) (5)		Sopeany Keo Brian Murphy
Efforts to Respond to Other Potential Indications of Bias or Discrimination - EEO			Sopeany Keo Brian Murphy
Efforts to Increase Diversity - EEO			Sopeany Keo Brian Murphy
Efforts to Respond to Non- EEO Complaints – OHC ER			Brian Murphy
Efforts to Respond to PMP Trends – OHC ER			Brian Murphy
Efforts to Respond to Other Potential Indications of Bias or Discrimination – OHC ER			Brian Murphy

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Fieldwork Audit Program
Prepared By: Kimberly Perteet June 6/2014
Reviewed By: Anna Saez 8/15/2014

Efforts to Increase Diversity – OHC (Dave Harmon)	(b) (5)	Sean Newman
Efforts to Respond to Complaints, PMP, Hiring, Promotions, and Diversity - Divisions		Kim Perteet Brian Murphy

Purpose: (b) (5)

Date: Discussions held on 6/26/2014

(b) (5)

Participants:
Larry Valett, Associate IG for Investigations
Kim Perteet, Project Lead (Board Audit)
Brian Murphy, Auditor (Board Audit)
Amanda Sundstrom, Auditor (CFPB Audit)

Source: Notes taken by CFPB team member Amanda Sundstrom and Board team member Brian Murphy.

Summary of Discussions:
(b) (5)

(b) (5)

Next Steps:
(b) (5)

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

Restricted-FR

January 29, 2015

MEMORANDUM

TO: Audit of the Board's Diversity and Inclusion Processes Audit File

FROM: Brian Murphy

CC: Anna Saez

SUBJECT: Statistical Methodology for OIG Analysis

Purpose: (b) (5)

(b) (5)

PSSC: See E.3.PRG , wp "Performance Management- Data Analysis"

Source: Memo prepared by OIG Auditor Brian Murphy.

Restricted-FR

Office of Inspector General
Audit of the Board's Diversity and Inclusion Processes
Preliminary Exit Conference 11/24/2014

Purpose: To obtain the Board's preliminary thoughts on the discussion draft.

Source: Auditor's notes taken during meeting.

Scope: 2014 Audit of the Board's Diversity and Inclusion Processes

Conclusion: See "Next Steps"

Prepared by: S. Newman, Auditor and B. Murphy, Auditor
Reviewed by: K. Perteet, Senior Auditor/Project Lead

PSSC: See A.2.PRG, wp.

Conduct Exit Conference

Meeting minutes written up by project team member Sean Newman.

Attendees:

Board

Donald Hammond, Chief Operating Officer
Michell Clark, Director of the Management Division
Bill Mitchell, Director and Chief Financial Officer
Sheila Clark, ODI Program Director
Lewis Andrews, Manager of HR Analytics (via conference call)

OIG

Melissa Heist, Associate Inspector General for Audits and Evaluations
Tim Rogers, Senior OIG Manager
Anna Saez, OIG Manager
Kimberly Perteet, Senior Auditor/Project Lead
Sean Newman, Auditor
Brian Murphy, Auditor

Time, Date, and Location:
Meeting held at 2:00 PM on 11/24/14 in Room I-4240 at the International Square building (1850 K St. Washington, DC)

Documents Provided:

(b) (5)

[redacted]

(b) (5)

(b) (5)

(b) (5)

(b) (5)

Version 1

(b) (5)

(b) (5)

The EEO Tabulation 2006-2010 (5-year ACS data)

FTP Site Technical Documentation

EEOC
U. S. Equal Employment Opportunity Commission

Social, Economic, and Housing Statistics Division
American Community Survey Office
Version 1 January 8, 2013

Table of Contents

Chapter 1 Introduction

Introduction

The Census Bureau entered into a reimbursable agreement with a consortium of four Federal agencies, consisting of the Equal Employment Opportunity Commission (EEOC), the Department of Justice (DOJ), the Office of Federal Contract Compliance Programs (OFCCP) at the Department of Labor (DOL), and the Office of Personnel Management (OPM), to create a custom tabulation identified as the EEO Tabulation 2006-2010 (5-year ACS data). This tabulation was created according to the specifications of the agencies in the consortium based on the American Community Survey (ACS) 2006-2010 5-year data. The EEO Tabulation 2006-2010 (5-year ACS data) serves as the primary external benchmark for comparing the race, ethnicity, and sex composition of an organization's internal workforce, and the analogous external labor market, within a specified geography and job category. More detailed information on this tabulation can be found here: http://www.census.gov/people/eeotabulation/.

The American Community Survey

The American Community Survey (ACS) is a part of the U.S. Census Bureau's Decennial Census Program and is designed to provide more current demographic, social, economic, and housing estimates throughout the decade. The ACS provides information on more than 40 topics, including education, language ability, the foreign-born, marital status, migration and many more subjects. Each year, the survey randomly samples around 3.5 million addresses and produces statistics that cover 1-year, 3-year, and 5-year periods for geographic areas in the United States and Puerto Rico. The 5-year estimates are available for many distinct geographies, including the nation, all 50 states, DC, Puerto Rico, counties, places, census tracts, and block groups. For more information about the ACS, please visit our home page at: www.census.gov/acs.

The 107 tables on the EEO Tabulation 2006-2010 (5-year ACS data) are available through American FactFinder (AFF) (factfinder2.census.gov). On AFF, these are available for download in several forms, including .csv files. This document will brief data users on the contents of the EEO tables located on the Census FTP site and explain how they can use it to obtain these tables.

Chapter 2 How to Use the EEO Tabulation 2006-2010 (5-year ACS data) Files

2.1 Location of the EEO Tabulation (2006-2010) on the FTP site

The EEO Tabulation is located on the Census FTP site at
http://www2.census.gov/EEO_2006_2010/.

2.2 EEO Tabulation File Organization

The EEO Tabulation 2006-2010 (5-year ACS data) on the FTP site consists of a number of zipped files. Each file set consists of one version of each table that covers all areas. The contents of these files, how to use the datasets, and a description of the variables and geographies contained in the datasets are included in this documentation.

The EEO Tabulation (2006-2010) on the FTP site is organized in two folders as shown in the above screenshot. There are two directories that contain the same combination of files. These are simply arranged differently to accommodate various user needs.

EEO_2006_2010_Tables_All_In_2_Giant_Files

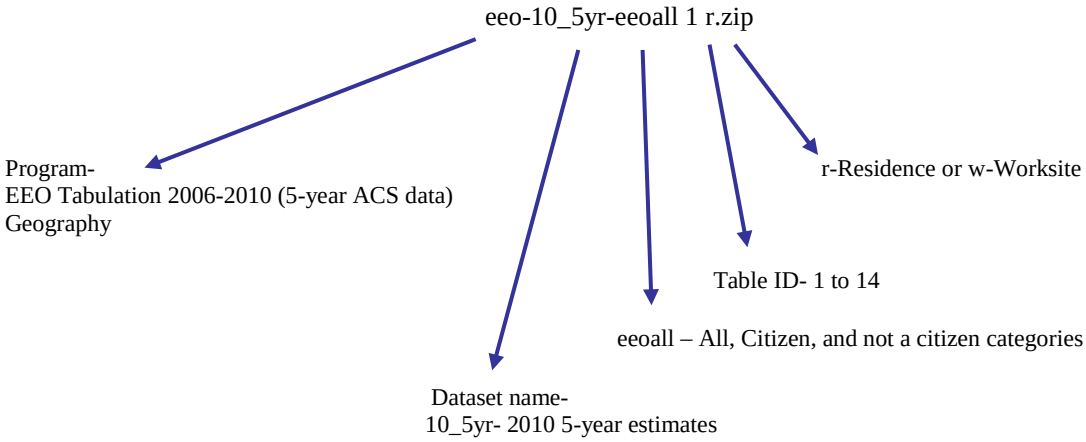
The "Tables All in 2 Giant Files" directory contains two zipped files, which includes one multiple data and annotation files divided by EEO Table sets 1 thru 7 and Table sets 8 thru 14. These zipped files are ideal for users who want estimates and margins of error for all EEO geographies throughout the nation at once. These files are very large and should only be used by those that can easily process very large files.

EEO_2006_2010_Tables_By_Table _Set

The "Tables By Table Set" directory contains files for each table set for all EEO geographic areas. Within those folders are geography files and files containing the data and annotation files, one per table set (table sets are explained in Section 2.3). Downloading from these folders is

ideal for users who only want an entire table set for EEO geographies. These tables will be divided up by residence and workplace geographies.

The naming convention used for the zipped files in this directory is the following:



File Name: eeo-10_5yr-eeoall1r.zip		
Example	**Name**	**Range or Type**
eeo	Program	EEO Tabulation 2006-2010 (5-year ACS data)
10	Reference Year	ACS data year 2006-2010
5yr	Period Covered	5yr- 5-year data
eeoall	Categories Covered	Contains tables for categories of All (citizen and not a citizen combined), Citizen, and Not a citizen
1	Table ID	1 to 14
r/w	Geography Type	r-Residence or w-Worksite

2.3 Data Format and Access

ACSII text versions of the EEO Tabulation 2006-2010 (5-year ACS data) tables that are disseminated through AFF are available for downloading via FTP site. These files include the (1) geographic header record file, (2) data files and (3) annotation files in pipe-delimited ("|") ASCII format. These three types of files contain shared identifiers so these can be joined together. Metadata and EEO table shells are contained in a Microsoft Excel spreadsheet. More information about the files and metadata is described in detail in the sections below.

2.4 Data and Annotation Files

The data and annotation files are named <program>-< dataset>-<custom tab abbreviation>< table id><r-residence,w-worksite>.dat (or .ann). The program for this EEO Tabulation (2006-2010) is "eeo," the dataset will be the 2010 5-year data set (e.g.10_5yr), the tabulation abbreviation "eeo," the tableid is the EEO Table id (e.g.1 thru 14), followed by an "r" or "w"

denoting that the table set consists of residence or worksite geography. The file extension is .dat for the data files and .ann for the annotation files.

For example, .dat table and .ann table for EEO Table Set 1 for the EEO Tabulation 2006-2010 (5-year ACS data) for the total population in residence geographies are named as follows:

eeo-10_5yr-eeoall1r.dat
eeo-10_5yr-eeoall1r.ann

For the worksite geographies, these are named as follows:

eeo-10_5yr-eeoall1w.dat
eeo-10_5yr-eeoall1w.ann

2.5 Geographic Header File

Two geographic header files are provided which contain information about all geographic entities for the EEO Tabulation (2006-2010), one for the residence geographies and one for worksite/flow geographies. The geographic header file is named with the structure <program>-< dataset>-"-geographic-header_file-"-r/w.xls. The program for this tabulation is "eeo." The dataset will be the current 5-year data set (e.g. 10_5yr). The file extension is .xls. For example, the geographic header files for the EEO Tabulation 2006-2010 data are named as follows:

eeo-10-5yr-geographic-header-file-r.xlsx
eeo-10-5yr-geographic-header-file-w.xlsx

The header row in these files contains a record layout and each following row contains a single geographic area with a unique geographic identifier (GEOID). All geographic codes for a geographic area are embedded within the GEOID. The GEOID is made up of a three-digit summary level, a two-digit component (always "00" for EEO), a constant "US," and the unique geographic area code within the summary level. The summary level field (SUMLEV) is the critical element in identifying the geographic area type for each record. The worksite file contains a FLOWID and its associated GEOID. Both of these geographic header files are located in the zipped file eeo-10-5yr-geographic-header-file.zip on the EEO FTP site at http://www.census.gov/EEO_2006_2010/.

The SUMLEV field represents a three-digit code, which represent the following geographic areas:

- Nation (010)
- State (040)
- CBSA (310)
- State-County (050)
- State-Place (160)
- County Set (902)

2.6 Metadata File

The spreadsheet called "The EEO Tabulation 2006-2010-5-Year-Table-shells.xls" contains all of the table shells in a single location. See Table 2-1 below for an example of a table shell applied to the .dat structure and the section under File Structure called "Table Shell Metadata" for details about the metadata file.

Table 2-1. Example of an EEO table shell

AFF Display ID	Table ID	Indent	Line Num	Stub	Estimate_1	MOE_1
EEO-ALL01R	EEOALL1R	0	0	EEO 1r. Detailed Census Occupation by Sex and Race/Ethnicity for Residence Geography		
EEO-ALL01R	EEOALL1R	0	0.3			
EEO-ALL01R	EEOALL1R	0	0.4		Total, race and ethnicity	Total, race and ethnicity
EEO-ALL01R	EEOALL1R	1	0.9	Total, both sexes		
EEO-ALL01R	EEOALL1R	2	1	Number	#	#
EEO-ALL01R	EEOALL1R	2	2	Percent	%	%
EEO-ALL01R	EEOALL1R	1	2.9	Male		
EEO-ALL01R	EEOALL1R	2	3	Number	#	#
EEO-ALL01R	EEOALL1R	2	4	Percent	%	%
EEO-ALL01R	EEOALL1R	1	4.9	Female		
EEO-ALL01R	EEOALL1R	2	5	Number	#	#
EEO-ALL01R	EEOALL1R	2	6	Percent	%	%

2.7 Data File Contents

There are two types of tables that contain EEO Tabulation data. The data files (file extension - .dat) contain estimates and margins of error, but include numeric values for jam values (see Chapter 3 for more information on jam values). The annotation files (file extension - .ann) complement the .dat files by containing clearer character values for jam values.

NOTE: All of the following structural references to the data files also apply to the annotation files. In order to simplify documentation in this chapter, descriptions about the structure of the annotation files are omitted because they are redundant with the descriptions of the data files.

Each data file is a single EEO table in a pipe-delimited (|) ASCII file format. Each row contains the estimates and margins of error for a single geographic area for a particular iteration. The geographic area is identified with the first column, GEOID. Flow geographies contain a GEOID followed by a FLOW ID (i.e. 0500000US01001| 0100100000|) in the second field of the data file shown as GEOID|FLOWID|. The iteration number is the second field in the data file for non-flow data and indicates the EEO occupation iterations that are tabulated, and is in the third field for flow data. The iterations are identified by their four-digit iteration number (EEO OCC). See the example file layout for eeo-10_5yr-eeoall1w.dat in table 2-2 below for more details concerning the structure the data files.

Table 2-2. Example File Layout for eeo-10_5yr-eeoall1w.dat

GEOID |FLOWID OCC|EST1|MOE1|EST2|MOE2|……..
1600000US5613900|56139000000000|9750|21|32|0|119|0|119|35|42|0|222|0|222|0|222|9
1600000US7206593|72065937206593|9750|22|23|20|23|0|222|0|222|0|222|0|222|0|222|9
1600000US7214290|721429072119B0|9750|23|34|20|34|0|222|0|222|0|222|0|222|0|222|9
1600000US7232522|72325227276770|9750|9|24|4|24|0|222|0|123|0|222|0|222|0|222|0|0
1600000US7263820|72638207263820|9750|29|39|25|29|0|222|0|222|0|222|0|222|0|222|9
1600000US7276770|72767700000000|9750|210|202|210|202|0|219|0|219|0|219|0|219|0|9
1600000US7276770|72767707206593|9750|35|40|0|222|35|40|0|222|0|222|0|222|0|222|9
1600000US7276770|727677072137B0|9750|20|26|0|222|20|26|0|222|0|222|0|222|0|222|9
1600000US7276770|72767707276770|9750|70|53|45|46|20|23|0|222|15|25|0|222|0|222|9

The remaining fields in the data files alternate estimates and margins of error in numerical order of the table cells. The recommended naming for the estimates is tblid_tblcell_EST and for margins of error is tblid_ tblcell _ME. In most tables, field 3 contains the estimate for table cell 1 (i.e. eeoall1_1_EST, eeoall1_2_EST, etc.) and field 4 contains the margin of error for table cell 1 (i.e. eeoall1_1_ME, eeoall1_2_ME, etc.). If there is more than one cell in the table, then field 5 contains the estimate for table cell 2 and field 6 contains the margin of error for table cell 2, and so on for all table cells.

Chapter 3 User Notes

Supplemental Documentation

Supplemental documentation concerning the American Community Survey, to assist users using this technical document, is located on the ACS Website at: www.census.gov/acs/www/data_documentation/documentation_main/.

Documents such as the Subject Definitions, Accuracy of the Data, and Code Lists are available on the URL listed above.

Geographic Terms and Concepts

The most updated geographic terms and concepts can be found at: http://www.census.gov/geo/www/reference.html.

The EEO Tabulation 2006-2010 (5-year ACS data) uses the December 2009 vintage for metropolitan and micropolitan statistical areas and components which can be found at: http://www.census.gov/population/metro/files/lists/2009/List1.txt.

Data Collection and Processing Procedures

The American Community Survey operations involve a complex set of data collection and processing procedures that are too extensive to discuss as a chapter in the EEO Tabulation (2006-2010) documentation. EEO data users interested in a technical discussion of ACS operational processes and survey design should review the ACS Design and Methodology Report located at: http://www.census.gov/acs/www/methodology/methodology_main/.

Questionnaire

Examples of the questionnaires that were sent to sample addresses can be found in the questionnaires section of the ACS website located at: http://www.census.gov/acs/www/SBasics/SQuest/SQuest1.htm.

ACS Standard Data Products in New AFF and User Handbook

The U.S. Census Bureau produces a variety of products that allow data users to access and research ACS data. These products are available in American FactFinder (AFF). Information about how to use AFF is located at: http://factfinder2.census.gov/faces/nav/jsf/pages/index.xhtml.
Data users looking for a summary overview of the ACS program or for discussion of annual changes in ACS data collection or product availability should refer to the Data and Documentation section on the ACS website at: http://www.census.gov/acs/www/data_documentation/data_main/.

Maps and Geographic Reference Materials

Detailed information about the ACS maps can be found in the reference maps section of the ACS website located at: http://www.census.gov/acs/www/data_documentation/reference_maps/.

Code Lists

The ACS provides code lists to identify all potential response categories for the variables included in the EEO Tabulation 2006-2010 (5-year ACS data). These variables are occupation, Hispanic origin, race, and industry. The code lists are available at: http://www.census.gov/acs/www/Downloads/data_documentation/pums/CodeLists/ACSPUMS2006_2010CodeLists.pdf.

Jam Values

Some data values represent unique situations where either the information to be conveyed is an explanation for the absence of data represented by a symbol in the data display, such as "(X). The data files (.dat) contain numeric values for jam values, while the annotation files (.ann) contain character values that are more descriptive.

The following list shows the special data values which can appear in any EEO Table on the FTP Site and on the American FactFinder website (AFF):

Special Data Values (Used in .dat files)	**Display Value (Used in .ann files.)**	**Description**
-999999999	N	Indicates that an estimate or its margin of error cannot be provided because the number of sample cases is too small for the given geographic area.
-888888888	(X)	Indicates that the estimate is not applicable or not available.
-666666666	-	Indicates that no sample observations were available to compute an estimate, or a ratio of medians cannot be calculated because one or both of the median estimates falls in the lowest interval or upper interval of an open-ended distribution.
-222222222	**	An '**' entry in the margin of error column indicates that either no sample observations or too few sample observations were available to compute a standard error and thus the margin of error. A statistical test is not appropriate.

A missing string indicates that the estimate is unavailable. This appears in the data files as two pipe-delimiters adjacent to each other without anything between them, or if the last cell in a data file is filtered then you get a pipe-delimiter followed immediately by a carriage return or EOF. A missing value indicates when an estimate is missing because of filtering for geographic restrictions or was removed due to the Disclosure Review Board's (DRB) Requirements.

Jam values are also used for the margins of error of controlled estimates. A statistical test for sampling variability is not appropriate. This is similar to the "*****" symbol used in American FactFinder.

Resources for using the FTP Site Files

The zipped file EEOTabulation2006-2010FTPSiteTableReferences.zip located on http://www2.census.gov/EEO_2006_2010/ contains the EEO-Tabulation-2006-2010-FTP-Site-Table-References.xlsx document, which consists of the following supplemental information for the EEO Tabulation 2006-2010 (5-year ACS data) disseminated via FTP.

- "**TableID-List**" defines the tables for EEO Tabulation (for FTP site).
- "**SummaryLevels-Table-Set**" defines the summary levels for EEO Special Tabulation.
- "**Tables-By-Geography**" defines all geographies used with which tables.
- "**Tables-By-Variables**" defines all variables used with which tables.
- "**Variables**" defines all variables that are referenced in the tables' lists, except for industry and for occupation.
- **"Industry"** defines the EEO 10W TableID suffix groupings, 2007 Census industry codes, corresponding 2007 NAICS industry codes, and EEO industry title.
- "**OccReCodesAggregatedOccs**" defines the EEO Tabulation 2006-2010 (5-year ACS) and 2008-2010 (3-year ACS) Occupation Code Crosswalk to Aggregated Occupations
- "**Guide-AggregatedOccups**" defines aggregated occupation group definitions.
- "**PUMSOCClist**" contains a crosswalk of full list of 2010 Census Detailed Occupation Codes to EEO Tabulation/PUMS Detailed Occupation Code List.
- "**EEOcrosswalk2000to0610**" contains an EEO Tabulation Crosswalk for the 2000 versus the 2006-2010 occupation codes.

User Notes

Other ACS user notes can be found on:
http://www.census.gov/acs/www/UseData/usernotes.html

PRELIMINARY PROGRAM OF THE ALLIED SOCIAL SCIENCE ASSOCIATIONS JANUARY 3-5, 2014, PHILADELPHIA, PA

NOTE: Everyone must register for the meeting, including speakers.

Please review your session(s) and let us know if you see anything that is amiss. Before making additions, please do a search to make sure you are not adding someone who is already scheduled at the same time.

We realize that there are some conflicts with participants. This was unavoidable, and in such cases a co-author will have to present the paper. Changes and corrections should be sent to gwyn.p.loftis@vanderbilt.edu.

All sessions will be equipped with a projector and screen for your presentation. ASSA will not provide computers.

Special Events listings are available here.

Location of Sessions for 2014 in Philadelphia, Pennsylvania

The beginning and ending times of sessions is shown below, with the exception being on the last day of the meeting when the last time slot will run from 1:00 pm to 3:00 pm.

8:00 am - 10:00 am
10:15 am - 12:15 pm
12:30 pm - 2:15 pm
2:30 pm - 4:30 pm

See also: JEL Classification System

Search
by Participant Last Name Exact Match

Filter By
All Associations
All JEL Classifications

Search Clear Search

Annual Meeting
Submissions
Registration/Housing
ASSA 2015 Preliminary Program
2015 Daily Program of Events
ASSA 2015 App
2015 Annual Meeting Webcasts
Previous Annual Meeting Papers and Webcasts
Archive of Past Programs
AEA Continuing Ed. Program
AEA Continuing Ed. Webcasts
Other Information
The next meeting is scheduled for January 3-5, 2016 in San Francisco, CA. The headquarters hotel is the Hilton San Francisco.
Papers and Proceedings of the Annual Meeting is published in the May issue of the *American Economic Review*. The guidelines for Papers and Proceedings are available online.
Contact Us

Jan 02, 2014

Jan 02, 2014 5:30 pm, Philadelphia Marriott, Grand Ballroom - Salon H
Econometric Society
Presidential Address
James J. Heckman (University of Chicago) The Economics and Econometrics of Human Development

Jan 02, 2014 6:30 pm, Loews Philadelphia Hotel, Regency Ballroom A & B
Association for Social Economics
Opening Plenary Session and Reception (A1)
Presiding: Mark D. White (City University New York)
Capabilities and Social Justice: Why Economics Needs Philosophy
Martha Nussbaum (University of Chicago)

Jan 03, 2014

Jan 03, 2014 8:00 am, Loews Philadelphia Hotel, Commonwealth Hall A1
Agricultural & Applied Economics Association
The Groundwater-Energy Nexus (Q2)

Presiding: Krishna Paudel (Louisiana State University)
Transboundary Allocation of Groundwater for Fracking under Threat of Salt Water Intrusion
Krishna Paudel (Louisiana State University)
Biswo Poudel (Louisiana State University)
[View Abstract]
The Effects of Energy Prices on Groundwater Extraction in Agriculture in the High Plains Aquifer
C.-Y. Cynthia Lin (University of California-Davis)
Lisa Pfeiffer (NOAA Fisheries)
[View Abstract] [Download Preview]
The Role of Energy Costs in Groundwater Pricing and Investments in Desalination and Wastewater Recycling
James Roumasset (University of Hawaii)
Christopher Wada (University of Hawaii)
[View Abstract] [Download Preview]
Discussants:
Nicholas Brozovic (University of Illinois)
David Zilberman (University of California-Berkeley)

Jan 03, 2014 8:00 am, Pennsylvania Convention Center, 202-B
American Economic Association
Assessing the Welfare Impacts of Economic Integration: Evidence from the 19th and 20th Centuries (F6)
Presiding: John Brown (Clark University)
How Large Are the Gains from Economic Integration? Theory and Evidence from United States Agriculture, 1880-2002
Arnaud Costinot (Massachusetts Institute of Technology)
Dave Donaldson (Massachusetts Institute of Technology)
[View Abstract] [Download Preview]
The Global Welfare Impact of China: Trade Integration and Technological Change
Julian di Giovanni (International Monetary Fund)
Andrei Levchenko (University of Michigan)
Jing Zhang (University of Michigan)
[View Abstract] [Download Preview]
The Link Between Fundamentals and Proximate Causes of Development
Wolfgang Keller (University of Colorado)
Carol H. Shiue (University of Colorado)
[View Abstract]
A Factor Augmentation Formulation of the Gains from Trade with an Application to Japan, 1865-1876
Daniel M. Bernhofen (American University)
John C. Brown (Clark University)
[View Abstract] [Download Preview]
Discussants:
Cecilia Fieler (University of Pennsylvania)
Marius Brülhart (University of Lausanne)
Sascha O. Becker (University of Warwick)
Douglas A. Irwin (Dartmouth College)

Jan 03, 2014 8:00 am, Pennsylvania Convention Center, 105-B
American Economic Association
Economics of Intergenerational Transfers and Wealth (J1)
Presiding: Karen Eggleston (Stanford University)
Education Policy and Intergenerational Transfers in Equilibrium
Brant Abbott (University of British Columbia)
Giovanni Gallipoli (University of British Columbia)
Costas Meghir (Yale University)
Gianluca Violante (New York University)
[View Abstract] [Download Preview]
Intergenerational Wealth Mobility: Evidence from Danish Wealth Records of Three Generations
Simon Halphen Boserup (University of Copenhagen)
Wojciech Kopczuk (Columbia University)
Claus Thustrup Kreiner (University of Copenhagen, CESifo and CEPR)
[View Abstract]
Housing Windfalls and Intergenerational Transfers in China
Maria Porter (Michigan State University)
Albert Park (Hong Kong University of Science and Technology)
[View Abstract]
The Intergenerational Impact of Rural Pensions in China: Transfers, Living Arrangements, and Off-Farm Employment of Adult Children
Ang Sun (Renmin University of China)

Xi Chen (Yale University)
Karen N. Eggleston (Stanford University)
[View Abstract]
Discussants:
Susan M. Dynarski (University of Michigan)
Costas Meghir (Yale University)
Xiaobo Zhang (International Food Policy Research Institute)
Albert Park (Hong Kong University of Science and Technology)

Jan 03, 2014 8:00 am, Philadelphia Marriott, Grand Ballroom - Salon J
American Economic Association
Effects on Preferences Regarding Risk & Ambiguity (D8)
Presiding: Luca Rigotti (University of Pittsburgh)
The Long-Run Impact of Traumatic Experience on Risk Aversion
Young-Il Kim (Sogang University)
Jungmin Lee (Sogang University & IZA)
[View Abstract] [Download Preview]
Self Confirming Long Run Biases
Pierpaolo Battigalli (University of Bocconi)
Fabio Maccheroni (University of Bocconi)
Massimo Marinacci (University of Bocconi)
Simone Cerreia-Vioglio (University of Bocconi)
[View Abstract]
The Legacy of Parental Time Preferences: Investment Behavior, and Children's Lifetime Outcomes
Hans Gronqvist (Stockholm University)
Lena Lindahl (Stockholm University)
Bart Golsteyn (Maastricht University)
[View Abstract]
Over-Caution of Large Committees of Experts
Justin Mattias Valasek (WZB)
Rune Midjord (University of the Basque Country)
Tomas Rodriguez Barraquer (Hebrew University)
[View Abstract] [Download Preview]
An Evolutionary Justification for Non-Bayesian Beliefs and Overconfidence
Hanzhe Zhang (University of Chicago)
[View Abstract] [Download Preview]
Primary-Market Auctions for Event Tickets: Eliminating the Rents of "Bob the Broker"
Eric Budish (University of Chicago)
Aditya Bhave (University of Chicago)
[View Abstract]

Jan 03, 2014 8:00 am, Philadelphia Marriott, Meeting Room 305
American Economic Association
Evaluation of Social Programs (H4)
Presiding: William Hoyt (University of Kentucky)
Smallpox and Human Capital Development: 1850-1930
Dara Lee Luca (University of Missouri and Harvard University)
[View Abstract]
The Power of Hydroelectric Dams: Agglomeration Spillovers
Edson R. Severnini (Carnegie Mellon University)
[View Abstract] [Download Preview]
Evaluating Long-Term Impacts of Sustained Mass Deworming: South Korea 1969-1995
Taejong Kim (KDI School of Public Policy and Management)
Jungho Kim (Ajou University)
Hyeok Jeong (KDI School of Public Policy and Management)
Sunjin Kim (KDI School of Public Policy and Management)
[View Abstract] [Download Preview]
Moving High-Performing Teachers to Low Achieving Schools
Bing-ru Teh (Mathematica Policy Research Inc.)
Steven Glazerman (Mathematica Policy Research Inc.)
Ali Protik (Mathematica Policy Research Inc.)
Julie Bruch (Mathematica Policy Research Inc.)
Jeffrey Max (Mathematica Policy Research Inc.)
[View Abstract]
John Papp (Highbridge Capital Management)

Jan 03, 2014 8:00 am, Philadelphia Marriott, Grand Ballroom - Salon I
American Economic Association
Fertility Decisions (J1)

Presiding: Tom Vogl (Princeton University)
Land Reform and Sex Selection in China
Douglas Almond (Columbia University)
Shuang Zhang (University of Colorada-Boulder)
Honbin Li (Tsinghua University)
[View Abstract] [Download Preview]
Heat Waves at Conception and Later Life Outcomes
Joshua Wilde (University of South Florida)
Benedicte Apouey (Paris School of Economics)
[View Abstract] [Download Preview]
Parenthood and Productivity of Highly Skilled Labor: Evidence From the Groves of Academe
Matthias Krapf (University of Zurich)
Heinrich Ursprung (University of Konstanz)
Christian Zimmermann (Federal Reserve Bank of St. Louis)
[View Abstract] [Download Preview]
School Cutoff Dates, and the Timing of Births
Hitoshi Shigeoka (Simon Fraser University)
[View Abstract] [Download Preview]
Intergenerational Dynamics and the Fertility Transition
Tom S. Vogl (Princeton University)
[View Abstract]
The Demographic Consequences of Gender Selection Technology
Qi Li (Peking University)
Juan Pantano (Washington University in St. Louis)
[View Abstract]

Jan 03, 2014 8:00 am, Philadelphia Marriott, Grand Ballroom - Salon L
American Economic Association
Gender Differences (J1)
Presiding: Joyce Jacobsen (Wesleyan University)
How the Design of a Pension System Influences Old Age Poverty and Gender Equity: A Study of Chile's Private Retirement Accounts System
Petra Todd (University of Pennsylvania)
Clement Joubert (University of North Carolina-Chapel Hill)
[View Abstract] [Download Preview]
Math and Gender: Is Math a Route to a High-Powered Career?
Juanna Joensen (Stockholm School of Economics)
Helena Skyt Nielsen (Aarhus University)
[View Abstract]
Firm Level Monopsony and the Gender Pay Gap
Douglas Webber (Temple University)
[View Abstract] [Download Preview]
Gender Differences and Dynamics in Competition: The Role of Luck
David Gill (University of Oxford)
Victoria Prowse (Cornell University)
[View Abstract] [Download Preview]
Are Women â€œNaturallyâ€ Better Credit Risks in Microcredit? Evidence from Field Experiments in Patriarchal and Matrilineal Societies in Bangladesh
Sugato Chakravarty (Purdue University)
Abu Zafar M. Shahriar (Monash University)
Zahid Iqbal (Purdue University)
[View Abstract] [Download Preview]

Jan 03, 2014 8:00 am, Philadelphia Marriott, Meeting Room 306
American Economic Association
Health Economics (I1)
Presiding: Kathleen Carey (Boston University)
Health Insurance and the Supply of Entrepreneurs: New Evidence from the Affordable Care Act's Dependent Coverage Mandate
James Benjamin Bailey (Temple University)
[View Abstract] [Download Preview]
The Effect of Health Shocks and Health Insurance on Employment and Earnings. Evidence from Chile
Vincent Pohl (Queen's University)
Christopher Neilson (Yale University)
Francisco Parro (Ministerio de Hacienda de Chile)
[View Abstract] [Download Preview]
Peer Effects Among Hospitalized Patients: Evidence from Roommate Assignments.
Olga Yakusheva (Marquette University)
[View Abstract] [Download Preview]

Digitizing Doctor Demand: The Impact of Online Reviews on Doctor Choice
Sonal Vats (Boston University)
Michael Luca (Harvard Business School)
[View Abstract] [Download Preview]
Does Employment Reduce Informal Caregiving?
Daifeng He (College of William and Mary)
Peter McHenry (College of William and Mary)
[View Abstract] [Download Preview]
Why Does the Health of Immigrants Deteriorate?
Osea Giuntella (University of Oxford)
[View Abstract] [Download Preview]

Jan 03, 2014 8:00 am, Pennsylvania Convention Center, 107-B
American Economic Association
Improving Student Performance (I2)
Presiding: Kristin Butcher (Wellesley College)
One Size Does Not Fit All: The Role of Vocational Ability on College Attendance and Labor Market Outcomes
Sergio Urzua (University of Maryland)
Maria F. Prada (University of Maryland)
[View Abstract]
The Effect of an Individualized Online Practice Tool on Math Performance - Evidence from a Randomized Field Experiment
Carla Haelermans (Maastricht University)
Joris Ghysels (Maastricht University)
[View Abstract] [Download Preview]
Not Just Test Scores: Parents' Demand Response to School Quality Information
Iftikhar Hussain (University of Sussex)
[View Abstract] [Download Preview]
High School Course Quality and Revealed Information
Jesse Bricker (Federal Reserve Board)
Hannah Allerdice Bricker (Unaffiliated)
[View Abstract] [Download Preview]
Educating Bright Students in Urban Schools
Kalena Cortes (Texas A&M University)
Wael Moussa (Syracuse University)
Jeffrey Weinstein (Syracuse University)
[View Abstract]
Rational Addiction and Video Games
Micah Pollak (Indiana University-Northwest)
[View Abstract]

Jan 03, 2014 8:00 am, Pennsylvania Convention Center, 103-A
American Economic Association
Individual and Employer Responses to Unemployment (J6)
Presiding: Laura Kawano (US Department of Treasury)
How Does Family Income Affect College Enrollment? Evidence from Timing of Parental Layoffs
Nate Hilger (Harvard University)
[View Abstract]
How Income Changes during Unemployment: Evidence from Tax Return Data
Laura Kawano (US Department of Treasury)
Sara LaLumia (Williams College)
[View Abstract]
Duration Dependence and Labor Market Conditions: Theory and Evidence from a Field Experiment
Kory Kroft (University of Toronto)
Fabian Lange (McGill University)
Matthew J. Notowidigdo (University of Chicago)
[View Abstract] [Download Preview]
A Contribution to the Empirics of Reservation Wages
Alan B Krueger (Princeton University)
Andreas Mueller (Columbia University)
[View Abstract] [Download Preview]
Discussants:
Ann Huff Stevens (University of California-Davis)
Till von Wachter (University of California-Los Angeles)

Jan 03, 2014 8:00 am, Pennsylvania Convention Center, 103-C
American Economic Association
Innovation (O3)

Presiding: Arthur Diamond (University of Nebraska-Omaha)
Why do Regions Vary in their Response to Crowdfunding? The Young, Restless, and Creative
Ajay Agrawal (University of Toronto)
Christian Catalini (Massachusetts Institute of Technology)
Avi Goldfarb (University of Toronto)
[View Abstract]
Retractions
Pierre Azoulay (Massachusetts Institute of Technology and NBER)
Jeffrey Furman (Boston University and NBER)
Joshua Krieger (Massachusetts Institute of Technology)
Fiona Murray (Massachusetts Institute of Technology)
[View Abstract] [Download Preview]
Buy, Keep or Sell: Economic Growth and the Market for Ideas
Ufuk Akcigit (University of Pennsylvania)
Murat Alp Celik (University of Pennsylvania)
Jeremy Greenwood (University of Pennsylvania)
[View Abstract]
Invisible Innovators: Historical Evidence from Mechanized Reapers and Cloud Computing
Richard Hunt (University of Colorado-Boulder)
[View Abstract]
The causal effect of labor unions on innovation
Daniel Bradley (University of South Florida)
Incheol Kim (University of South Florida)
Xuan Tian (Indiana University)
[View Abstract] [Download Preview]

Jan 03, 2014 8:00 am, Pennsylvania Convention Center, 201-B
American Economic Association
Macroeconomic Uncertainty and Asset Prices (G1)
Presiding: Ivan Shaliastovich (University of Pennsylvania)
Good and Bad Uncertainty: Macroeconomic and Financial Market Implications
Gill Segal (University of Pennsylvania)
Ivan Shaliastovich (University of Pennsylvania)
Amir Yaron (University of Pennsylvania)
[View Abstract] [Download Preview]
One-Sided Risk Shocks
Jesus Fernandez-Villaverde (University of Pennsylvania)
Pablo Guerron (Federal Reserve Bank of Philadelphia)
Juan Rubio-Ramirez (Duke University)
Uncertainty Shocks, Asset Supply and Pricing over the Business Cycle
Francesco Bianchi (Duke University)
Cosmin Ilut (Duke University)
Martin Schneider (Stanford University)
[View Abstract] [Download Preview]
Does Uncertainty Reduce Growth? Using Disasters as Natural Experiments
Scott R. Baker (Stanford University)
Nicholas Bloom (Stanford University)
[View Abstract] [Download Preview]

Jan 03, 2014 8:00 am, Pennsylvania Convention Center, 201-A
American Economic Association
Measuring Systemic Risk (G2)
Presiding: René Stulz (Ohio State University)
Enhanced Stress Testing and Financial Stability
Matthew Pritsker (Federal Reserve Bank of Boston)
[View Abstract] [Download Preview]
How Likely is Contagion in Financial Networks?
Paul Glasserman (Columbia University)
H. Peyton Young (University of Oxford)
[View Abstract] [Download Preview]
Taking the risk out of systemic risk measurement
Levent Guntay (Federal Deposit Insurance Corporation)
Paul H. Kupiec (The American Enterprise Institute)
[View Abstract] [Download Preview]
Can Top-down Banking Stress Tests Be Informative?
Pavel S. Kapinos (Federal Deposit Insurance Corporation)
Oscar A. Mitnik (Federal Deposit Insurance Corporation)
[View Abstract]
Discussants:

Sanjiv R. Das (Santa Clara University)
Mark J. Flannery (University of Florida)
Albert S. Kyle (University of Maryland)
Rene M. Stulz (Ohio State University)

Jan 03, 2014 8:00 am, Philadelphia Marriott, Grand Ballroom - Salon B
American Economic Association
Microeconometrics: Theory and Applications (C2)
Presiding: Bidisha Mandal (Washington State University)
Estimation of an Education Production Function under Random Assignment with Selection
Eleanor Choi (Hanyang University)
Hyungsik Roger Moon (University of Southern California)
Geert Ridder (University of Southern California)
[View Abstract] [Download Preview]
Specification and Estimation of Treatment Models in the Presence of Sample Selection
Angela Vossmeyer (University of California-Irvine)
[View Abstract] [Download Preview]
Gender Wage Gap in the United States: An Interactive Fixed Effects Approach
Kusum Mundra (Rutgers University)
Treatment Effect Analyses through Orthogonality Conditions Implied by a Fuzzy Regression Discontinuity Design, with Two Empirical Studies
Muzhe Yang (Lehigh University)
[View Abstract] [Download Preview]
Child Care Choices, Cognitive Development, and Kindergarten Enrollment
Bidisha Mandal (Washington State University)
[View Abstract] [Download Preview]

Jan 03, 2014 8:00 am, Pennsylvania Convention Center, 202-A
American Economic Association
Productivity (O4)
Presiding: Wayne Gray (Clark University)
Agricultural Production amidst Conflict: The Effects of Shocks, Uncertainty and Governance of Non-State Armed Actors
Andres Zambrano (Universidad de los Andes)
Maria Alejandra Arias (Universidad de los Andes)
Ana Maria Ibañez (Universidad de los Andes)
[View Abstract] [Download Preview]
Trade Liberalization, Supply Chains and Productivity
Carol Newman (Trinity College Dublin)
John Rand (University of Copenhagen)
Finn Tarp (UNU-WIDER and University of Copenhagen)
[View Abstract] [Download Preview]
How Do Firms Adjust Production Factors to the Cycle? The Role of Rigidities
Gilbert Cette (Banque de France)
Remy Lecat (Banque de France)
Ahmed Ould (Banque de France)
Ahmed Jiddou (Banque de France)
[View Abstract] [Download Preview]
Demand Shocks and Productivity: Technology Adoption During the U.S. Ethanol Boom
Danny McGowan (Bangor University)
Richard Kneller (University of Nottingham)
[View Abstract] [Download Preview]
Cumulative Innovation, Growth and Welfare-Improving Patent Policy
Edwin L. Lai (Hong Kong University of Science and Technology)
Davin Chor (National University of Singapore)
[View Abstract] [Download Preview]

Jan 03, 2014 8:00 am, Pennsylvania Convention Center, 203-B
American Economic Association
Public Finance and Policy (H1)
Presiding: Erin Bronchetti (Swarthmore College)
Post-Retirement Benefit Plans, Leverage, and Real Investment
Sohnke m Bartram (London Business School and Warwick Business School)
[View Abstract] [Download Preview]
The Impact of Longevity Improvements on U.S. Corporate Defined Benefit Pension Plans
Michael Kisser (Norwegian School of Economics)
John Kiff (International Monetary Fund)
Erik Oppers (International Monetary Fund)
Mauricio Soto (International Monetary Fund)

[View Abstract] [Download Preview]
The Impact of Numerical Constraints on Fiscal Policy in the EU27
Wolf Heinrich Reuter (Vienna University of Economics and Business)
[View Abstract]
The Effect of Government Spending in Construction on Job Creation: Evidence from Texas
Dakshina G. De Silva (Lancaster University)
Viplav Saini (Oberlin College)
[View Abstract]
Presidentialism, Parliamentarism and Fiscal Policy: Evidence from the Local Level in Germany
Thushyanthan Baskaran (University of Goettingen)
Zohal Hessami (University of Konstanz)
[View Abstract]

Jan 03, 2014 8:00 am, Pennsylvania Convention Center, 203-A
American Economic Association
Sources of Peer Effects (D8)
Presiding: Bruce Sacerdote (Dartmouth University)
Social Networks and the Decision to Insure
Jing Cai (University of Michigan)
Alain Janvry (University of California-Berkeley)
Elisabeth Sadoulet (University of California-Berkeley)
[View Abstract] [Download Preview]
Peer Effects in Risk Taking
Amrei Lahno (University of Munich)
Marta Serra-Garcia (University of Munich)
[View Abstract]
Academic Peer Effects with Different Group Assignment Policies: Residential Tracking versus Random Assignment
Robert Garlick (Duke University)
[View Abstract] [Download Preview]
Understanding Mechanisms Underlying Peer Effects: Evidence from a Field Experiment on Financial Decisions
Leonardo Bursztyn (University of California-Los Angeles)
Florian Ederer (University of California-Los Angeles)
Bruno Ferman (George Washington University)
Noam Yuchtman (University of California-Berkeley)
[View Abstract] [Download Preview]
Discussants:
Achyuta Adhvaryu (Yale University)
Kenneth Ahern (University of Southern California)
Scott Carrell (University of California-Davis)
John Beshears (Harvard University)

Jan 03, 2014 8:00 am, Pennsylvania Convention Center, 201-C
American Economic Association
The Demand for Insurance in Developing Countries (O1)
Presiding: Benjamin Olken (Massachusetts Institute of Technology)
Risk and Investment in Agriculture
Mark Rosenzweig (Yale University)
Christopher Udry (Yale University)
[View Abstract]
Dynamics of Demand for Index Insurance: Evidence from a Five-Year Panel in Gujarat
Shawn A. Cole (Harvard University)
Jeremy Tobacman (University of Pennsylvania)
Daniel Stein (The World Bank)
[View Abstract]
Adverse Selection in the Market for Catastrophic Health Insurance: Some Evidence from India
Abhijit Banerjee (Massachusetts Institute of Technology)
Esther Duflo (Massachusetts Institute of Technology)
Richard Hornbeck (Harvard University)
[View Abstract]
Discussants:
Seema Jayachandran (Northwestern University)
Tavneet Suri (Massachusetts Institute of Technology)
Jishnu Das (World Bank)

Jan 03, 2014 8:00 am, Pennsylvania Convention Center, 204-B
American Economic Association
The Price Theory of Selection Markets (D4)

Presiding: Michael Whinston (Massachusetts Institute of Technology)
Product Design in Selection Markets
André F. Veiga (University of Oxford)
Eric Glen Weyl (University of Chicago)
[View Abstract] [Download Preview]
Imperfect Competition in Selection Markets
Neale Mahoney (University of Chicago)
Eric Glen Weyl (University of Chicago)
[View Abstract] [Download Preview]
Unraveling versus Unraveling: Competitive Equilibriums and Trade in Insurance Markets
Nathaniel Hendren (Harvard University)
[View Abstract] [Download Preview]
Information Frictions and the Welfare Consequences of Adverse Selection
Benjamin R. Handel (University of California-Berkeley)
Jonathan T. Kolstad (University of Pennsylvania)
Johannes Spinnewijn (London School of Economics)
[View Abstract]
Discussants:
Jonathan Levin (Stanford University)
Liran Einav (Stanford University)
Amy N. Finkelstein (Massachusetts Institute of Technology)
Michael Whinston (Massachusetts Institute of Technology)

Jan 03, 2014 8:00 am, Philadelphia Marriott, Grand Ballroom - Salon E
American Economic Association
What's Natural? Key Macroeconomic Parameters after the Great Recession (E1)
Presiding: Matthew Shapiro (University of Michigan)
The Natural Rate of Interest and Its Usefulness for Monetary Policy Making
Robert Barsky (Federal Reserve Bank of Chicago and University of Michigan)
Alejandro Justiniano (Federal Reserve Bank of Chicago)
Leonardo Melosi (Federal Reserve Bank of Chicago)
[View Abstract] [Download Preview]
Natural Rate of Unemployment
Mark Watson (Princeton University)
[View Abstract]
Natural Rate of Growth
John Fernald (Federal Reserve Bank of San Francisco)
Charles I Jones (Stanford University)
[View Abstract] [Download Preview]
Discussants:
Michael Woodford (Columbia University)
Robert E. Hall (Stanford University)
Susanto Basu (Boston College)

Jan 03, 2014 8:00 am, Loews Philadelphia Hotel, Millennium Hall
American Finance Association
Asset Management and Market Efficiency (G2)
Presiding: Christopher Malloy (Harvard University)
Transparency and Talent Allocation in Money Management
Simon Gervais (Duke University)
Gunter Strobl (Frankfurt School of Finance & Management)
[View Abstract] [Download Preview]
The People in Your Neighborhood: Social Interactions and Mutual Fund Portfolio Choice
Veronika Pool (Indiana University)
Noah Stoffman (Indiana University)
Scott Yonker (Indiana University)
[View Abstract]
Peer Effects in Mutual Funds
Jesse Blocher (Vanderbilt University)
[View Abstract] [Download Preview]
Predation versus Cooperation in Mutual Fund Families
Alexander Eisele (University of Lugano)
Tamara Nefedova (University of Lugano)
Gianpaolo Parise (University of Lugano)
[View Abstract]
Discussants:
Bruce Carlin (University of California-Los Angeles)
Kelly Shue (University of Chicago)
Antti Petajisto (New York University)

Utpal Bhattacharya (Indiana University)

Jan 03, 2014 8:00 am, Loews Philadelphia Hotel, Regency Ballroom B
American Finance Association
Behavioral Asset Pricing (G1)
Presiding: Nicholas Barberis (Yale University)
No News is News: Do Markets Underreact to Nothing
Stefano Giglio (University of Chicago)
Kelly Shue (University of Chicago)
[View Abstract]
First Impressions: "System 1" Thinking and the Cross-Section of Stock Returns
Nicholas C. Barberis (Yale University)
Abhiroop Mukherjee (Hong Kong University of Science and Technology)
Baolian Wang (Hong Kong University of Science and Technology)
[View Abstract]
Waves in Ship Prices and Investment
Robin Greenwood (Harvard Business School)
Samuel Hanson (Harvard Business School)
[View Abstract]
Discussants:
Dong Lou (London School of Economics)
Byoung-Hyoun Hwang (Purdue University)
Kent Daniel (Columbia University)

Jan 03, 2014 8:00 am, Loews Philadelphia Hotel, Regency Ballroom A
American Finance Association
Credit Risk I (G1)
Presiding: Ilya Strebulaev (Stanford University)
CDS Auctions and Informative Biases in CDS Recovery Rates
Sudip Gupta (New York University)
Rangarajan K. Sundaram (New York University)
[View Abstract]
Synthetic or Real? The Equilibrium Effects of Credit Default Swaps on Bond Markets
Martin Oehmke (Columbia University)
Adam Zawadowski (Boston University)
[View Abstract] [Download Preview]
Does the Tail Wag the Dog? The Effect of Credit Default Swaps on Credit Risk
Marti Subrahmanyam (New York University)
Dragon Tang (University of Hong Kong)
Sarah Qian Wang (Warwick University)
[View Abstract] [Download Preview]

Jan 03, 2014 8:00 am, Loews Philadelphia Hotel, Commonwealth Hall C
American Finance Association
Institutional Investors' Portfolio Choices (G1)
Presiding: Luis Viceira (Harvard Business School)
Why Do University Endowments Invest So Much In Risky Assets?
Thomas Gilbert (University of Washington)
Christopher Hrdlicka (University of Washington)
[View Abstract]
Informed Trading and Expected Returns
James Choi (Yale University)
Li Jin (Harvard University)
Hongjun Yan (Yale University)
[View Abstract] [Download Preview]
Dynamic Portfolio Choice with Frictions
Nicolae Garleanu (University of California-Berkeley)
Lasse Pedersen (New York University)
[View Abstract] [Download Preview]
Deleveraging Risk
Scott Richardson (London Business School)
Pedro Saffi (University of Cambridge)
Kari Sigurdsson (Reykjavik University)
[View Abstract] [Download Preview]
Discussants:
Stephen G. Dimmock (Nanyang Technological University)
Lauren H. Cohen (Harvard Business School)
Bryan T. Kelly (University of Chicago)
Jakub W. Jurek (Princeton University)

Jan 03, 2014 8:00 am, Loews Philadelphia Hotel, Commonwealth Hall D
American Finance Association
Macro Finance (G1)
Presiding: Ralph Koijen (University of Chicago)
Nominal Bonds, Real Bonds, and Equity
Andrew Ang (Columbia University)
Maxim Ulrich (Columbia University)
[View Abstract]
Forecasting through the Rear-View Mirror: Data Revisions and Bond Return Predictability
Eric Ghysels (University of North Carolina)
Casidhe Horan (University of Michigan)
Emanuel Moench (Federal Reserve Bank of New York)
[View Abstract]
Rare Booms and Disasters in a Multi-Sector Endowment Economy
Jerry Tsai (University of Pennsylvania)
Jessica Wachter (University of Pennsylvania)
[View Abstract]
Discussants:
Jules van Binsbergen (Stanford University)
Lars A. Lochstoer (Columbia University)
Leonid Kogan (Massachusetts Institute of Technology)

Jan 03, 2014 8:00 am, Loews Philadelphia Hotel, Commonwealth Hall B
American Finance Association
Macroeconomics, Deflation and Liquidity (G1)
Presiding: Markus Brunnermeier (Princeton University)
Deflation Risk
Matthias Fleckenstein (University of California-Los Angeles)
Francis Longstaff (University of California-Los Angeles)
Hanno Lustig (University of California-Los Angeles)
[View Abstract]
Banks Exposure to Interest Rate Risk and the Transmission of Monetary Policy
Augustin Landier (University of Toulouse)
David Sraer (Princeton University)
David Thesmar (HEC Paris)
[View Abstract]
Corporate Cash Hoarding: The Role of Just-in-Time Adoption
Xiaodan Gao (National University of Singapore)
[View Abstract] [Download Preview]
Funding Liquidity Risk and the Cross-Section of Stock Returns
Jean-Sebastien Fontaine (Bank of Canada)
Rene Garcia (EDHEC)
Sermin Gungor (Bank of Canada)
[View Abstract] [Download Preview]
Discussants:
Cesaire Meh (Bank of Canada)
Anil Kashyap (University of Chicago)
Thomas Eisenbach (Federal Reserve Bank of New York)
Tyler Muir (Yale University)

Jan 03, 2014 8:00 am, Loews Philadelphia Hotel, Washington B
American Real Estate & Urban Economic Association
Commercial Real Estate (G1)
Presiding: Andra Ghent (Arizona State University)
Real Earnings Management, Liquidity and SEO dynamics: Evidence from United States REITs
Xiaoying Deng (National University of Singapore)
Seow Eng Ong (National University of Singapore)
[View Abstract] [Download Preview]
Using Cash Flow Dynamics to Price Thinly Traded Assets: The Case of Commercial Real Estate
Walter Boudry (Cornell University)
Crocker Liu (Cornell University)
Tobias Muhlhofer (Indiana University)
Walter Torous (Massachusetts Institute of Technology)
[View Abstract] [Download Preview]
What Drives Building-Level Investment Returns?
Serguei Chervachidze (CBRE Econometric Advisors)
Jeffery Fisher (Indiana University)
William Wheaton (Massachusetts Institute of Technology)

[View Abstract] [Download Preview]
Commercial Real Estate, Distress and Capital Recovery: Analysis of the Special Servicer
David Downs (Virginia Commonwealth University)
Tracy Xu (University of Denver)
[View Abstract] [Download Preview]
Discussants:
Moussa Diop (University of Wisconsin)
Rossen Valkanov (University of California-San Diego)
Xudong An (San Diego State University)
David T. Brown (University of Florida)

Jan 03, 2014 8:00 am, Loews Philadelphia Hotel, Washington C
American Real Estate & Urban Economic Association
Urban Development and Dynamics (R3)
Presiding: Eleonora Patacchini (Syracuse University)
Transportation Technologies, Agglomeration, and the Structure of Cities
Jeffrey Brinkman (Federal Reserve Bank of Philadelphia)
[View Abstract] [Download Preview]
The Decline of the Rust Belt: A Dynamic Spatial Equilbrium Analysis
Chamna Yoon (Baruch College City University of New York)
[View Abstract]
The Settlement of the United States, 1800 to 2000: The Long Transition Towards Gibrat's Law
Klaus Desmet (Carlos III)
Jordan Rappaport (Federal Reserve Bank of Kansas City)
[View Abstract] [Download Preview]
Driving to Opportunity: Local Wages, Commuting, and Sub-Metropolitan Quality of Life
David Albouy (University of Michigan)
Bert Lue (University of Michigan)
[View Abstract] [Download Preview]
Discussants:
Ronni Pavan (University of Rochester)
Giorgio Topa (Federal Reserve Bank of New York)
Matthew Turner (University of Toronto)
Jessie Handbury (University of Pennsylvania)

Jan 03, 2014 8:00 am, Philadelphia Marriott, Grand Ballroom - Salon A
Association for Comparative Economic Studies
Exploration of New and Existing Macro Data for the Chinese Economy (E2)
Presiding: Carsten Holz (Stanford University)
The Quality of Chinese GDP Statistics
Carsten Holz (Stanford University)
[View Abstract]
Chinese Capital Flight: Questions of Data and Policy
Frank Gunter (Lehigh University)
[View Abstract] [Download Preview]
China's Provincial Capital Stock by Sector: Data and Preliminary Analysis
Yanrui Wu (University of Western Australia)
[View Abstract]
China's Human Capital Stock
Haizheng Li (Georgia Institute of Technology)
[View Abstract]
Discussants:
Belton M. Fleisher (Ohio State University)
Zheng Michael Song (University of Chicago)

Jan 03, 2014 8:00 am, Loews Philadelphia Hotel, Regency Ballroom C1
Association for Evolutionary Economics
Macro Policy and Financial Stability in the Age of Turbulence (B5)
Presiding: Abu Shonchoy (Institute of Developing Economies)
Understanding Long-Term Japanese Government Bonds' Low Nominal Yields
Tanweer Akram (Ing Investment Management)
[View Abstract] [Download Preview]
Shadow Banking and Credit Driven Growth in China
Yan Liang (Willamette University)
[View Abstract]
Economic Consequences of the TARP
Heather Montgomery (International Christian University)
[View Abstract] [Download Preview]
Three Sector Balance Approach and the Economic Crisis

Eric Tymoigne (Lewis and Clark College)
[View Abstract]
Discussants:
Abu Shonchoy (Institute of Developing Economies)
Yuki Takahashi (State University of New York-Stony Brook)

Jan 03, 2014 8:00 am, Loews Philadelphia Hotel, Congress A
Association for Social Economics
Social Entrepreneurship: Maximizing Impact and Innovation (L3)
Presiding: Tonia Warnecke (Rollins College)
Social Enterprises as Networks of Innovators in the Social Economy
Zohreh Emami (Alverno College)
[View Abstract]
Social Enterprises and the Analysis of Space to Alleviate Financial Constraints
Benjamin Wilson (University of Missouri-Kansas City)
[View Abstract]
Workers' Cooperatives: New Strategies for Finance
Daniel Fireside (Equal Exchange)
Christopher Gunn (Hobart and William Smith Colleges)
[View Abstract]
Social Entrepreneurship, Alternative Currencies, and Post-Transactional Civil Society: The Case of the Sunshine Bank
Matthias Klaes (University of Dundee)
[View Abstract]
Social Entrepreneurship for Students: The Rollins Microfinance Fund
Tonia Warnecke (Rollins College)
[View Abstract]

Jan 03, 2014 8:00 am, Philadelphia Marriott, Grand Ballroom - Salon K
Association of Environmental & Resource Economists
Options for a New International Climate Regime Arising from the Durban Platform for Enhanced Action (Q5) (Panel Discussion)
Panel Moderator: Robert Stavins (Harvard University)
Joseph Aldy (Harvard University)
Ottmar Edenhofer (Technical University of Berlin)
Geoffrey Heal (Columbia University)
Gilbert Metcalf (Tufts University)
William Pizer (Duke University)

Jan 03, 2014 8:00 am, Loews Philadelphia Hotel, Congress B
Association of Financial Economists/American Economic Association
Moral Attitudes and Financial Decision-Making (G3)
Presiding: Michael Jensen (Harvard University)
Moral Attitudes and Financial Decision-Making
Jonathan Haidt (New York University)
David Hirshleifer (University of California-Irvine)
Siew Hong Teoh (University of California-Irvine)
[View Abstract]
The Impact of Cultural Aversion on Economic Exchange: Evidence from Shocks to Sino-Japanese Relations
Raymond Fisman (Columbia University)
Yasushi Hamao (University of Southern California)
Yongxiang Wang (University of Southern California)
[View Abstract] [Download Preview]
Honoring One's Word: CEO Integrity and Accruals Quality
Shane S. Dikolli (Duke University)
William J. Mayew (Duke University)
Thomas D. Steffen (Duke University)
[View Abstract] [Download Preview]
Trust, Consumer Debt, and Household Finance
Danling Jiang (Florida State University)
Sonya S. Lim (DePaul University)
[View Abstract] [Download Preview]
Discussants:
Harrison Hong (Princeton University)
Paola Sapienza (Northwestern University)
Alexander Dyck (University of Toronto)
Adair Morse (University of California-Berkeley)
Michael Jensen (Harvard University)

Jan 03, 2014 8:00 am, Philadelphia Marriott, Meeting Room 401
Econometric Society
Big Data and High-Dimensional Problems (C3)
Presiding: Jushan Bai (Columbia University)
Incidental Endogeneity in High Dimensions
Jianqing Fan (Princeton University)
[View Abstract]
Program Evaluation with High-Dimensional Data
Victor Chernozhukov (Massachusetts Institute of Technology)
[View Abstract] [Download Preview]
Asymptotic Analysis of the Squared Estimation Error in Misspecified Factor Models
Alexei Onatski (University of Cambridge)
[View Abstract] [Download Preview]
Shrinkage Estimation of High-Dimensional Factor Models with Structural Instabilities
Xu Cheng (University of Pennsylvania)
Zhipeng Liao (University of Pennsylvania)
Frank Schorfheide (University of Pennsylvania)
[View Abstract] [Download Preview]

Jan 03, 2014 8:00 am, Philadelphia Marriott, Meeting Room 402
Econometric Society
Estimation of Industrial Organization Models (L2)
Presiding: Che-Lin Su (University of Chicago)
Relaxing Competition Through Speculation: Committing to a Negative Supply Slope
Pär Holmberg (Research Institute of Industrial Economics)
Bert Willems (Tilburg University)
[View Abstract] [Download Preview]
Estimating Dynamic Discrete-Choice Games of Incomplete Information
Michael Dannen Egesdal (Harvard University)
Zhenyu Lai (Harvard University)
Che-Lin Su (University of Chicago)
[View Abstract] [Download Preview]
Identification and Estimation of Heterogeneous Production Functions
Jorge Balat (Johns Hopkins University)
Yuya Sasaki (Johns Hopkins University)
[View Abstract]
Supply Function Competition and Exporters: Nonparametric Identification and Estimation of Productivity Distributions and Marginal Costs
Ayse Ozgur Pehlivan (Bilkent University)
Quang Vuong (New York University)
[View Abstract] [Download Preview]
Primary Dealers, Indirect Bidders, and Direct Bidding: A Structural Model of United States Treasury Auctions
Eiichiro Kazumori (State University of New York)
Leonard Tchuindjo (United States Treasury and George Washington University)
[View Abstract] [Download Preview]
Discussants:
Ayse Ozgur Pehlivan (Bilkent University)
Jorge Balat (Johns Hopkins University)
Che-Lin Su (University of Chicago)
Pär Holmberg (Research Institute of Industrial Economics)

Jan 03, 2014 8:00 am, Philadelphia Marriott, Meeting Room 404
Econometric Society
Long Run Changes in Labor Market Outcomes (J1)
Presiding: Sephorah Mangin (Monash University)
The Role of Allocative Efficiency in a Decade of Recovery
Kaiji Chen (Emory University)
[View Abstract] [Download Preview]
Factors Affecting College Completion and Student Ability in the United States since 1900
Christopher Michael Herrington (Arizona State University)
Kevin Donovan (Arizona State University)
[View Abstract] [Download Preview]
EPL and Capital-Labor Ratios
Alexandre Janiak (University of Chile)
Etienne Wasmer (Sciences-Po)
[View Abstract]
A Theory of Factor Shares

Sephorah Joanne Mangin (Monash University)
[View Abstract] [Download Preview]

Jan 03, 2014 8:00 am, Philadelphia Marriott, Meeting Room 405
Econometric Society
The Real Effects of Financial Markets (G1)
Presiding: Franklin Allen (University of Pennsylvania)
Market Efficiency and Real Efficiency
Itay Goldstein (University of Pennsylvania)
Liyan Yang (University of Toronto)
[View Abstract]
Informational Frictions and Commodity Markets
Michael Sockin (Princeton University)
Wei Xiong (Princeton University)
[View Abstract] [Download Preview]
Learning from Peers' Stock Prices and Corporate Investment
Thierry Foucault (HEC, Paris)
Laurent Fresard (University of Maryland)
[View Abstract]
Financial Market Shocks and the Macroeconomy
Avanidhar Subrahmanyam (University of California-Los Angeles)
Sheridan Titman (University of Texas-Austin)
[View Abstract] [Download Preview]
Discussants:
Alexi Savov (New York University)
Thomas Michael Mertens (New York University)
Wei Jiang (Columbia University)
Gustavo Manso (University of California-Berkeley)

Jan 03, 2014 8:00 am, Loews Philadelphia Hotel, Commonwealth Hall A2
International Banking, Economics & Finance Association
Finance and Development/ International Finance (G2)
Presiding: Gillian Garcia (Gillian Garcia Associates)
Competition, Loan Rates and Information Dispersion in Microcredit Markets
Guillermo Baquero (European School of Management and Technology, Berlin)
Malika Hamadi (University of Sassari-Italy)
Andreas Heinen (Université de Cergy-Pontoise)
[View Abstract]
Investment in Relationship-Specific Assets: Does Finance Matter?
Martin Strieborny (Lund University)
Madina Kukenova (International Trade Center, Geneva)
[View Abstract] [Download Preview]
Finance and Growth: Time Series Evidence on Causality
Oana Peia (Université de Cergy-Pontoise)
Kasper Roszbach (Sveriges Riksbank and University of Groningen)
[View Abstract] [Download Preview]
Trilemma Stability and International Macroeconomic Archetypes
Helen Popper (Santa Clara University)
Alex Mandilaris (University of Surrey)
Graham Bird (University of Surrey)
[View Abstract] [Download Preview]
Discussants:
Matt Osborne (University of Toronto)
Jihad Dagher (International Monetary Fund)
Gibran Rezavi (University of Illinois-Chicago)
Andrei Zlate (Federal Reserve Board)

Jan 03, 2014 8:00 am, Pennsylvania Convention Center, 104-A
Labor & Employment Relations Association
Democratic Workplace Practices and Employee Ownership (J5)
Presiding: Stephen Woodbury (Michigan State University)
How Did Employee Ownership Firms Weather the Last Two Recessions? Employee Ownership and Employment Stability in the United States.
Fidan Ana Kurtulus (University of Massachusetts-Amherst)
Douglas Kruse (Rutgers University)
[View Abstract]
The Citizen's Share: The Context for Employee Stock Ownership and Profit Sharing in American History
Joseph Blasi (Rutgers University)

Richard B. Freeman (Harvard University)
Douglas Kruse (Rutgers University)
[View Abstract]
Profit Sharing and Workplace Productivity: Does Teamwork Play a Role?
Tony Fang (Monash University)
Richard Long (University of Saskatchewan)
[View Abstract] [Download Preview]
Does Employee Ownership Affect Attitudes and Behaviors? Selection, Status, and Size of Stake
Dan Weltmann (Rutgers University)
[View Abstract] [Download Preview]
Discussants:
Brad Hershbein (W.E. Upjohn Institute for Employment Research)
Stephen Woodbury (Michigan State University)

Jan 03, 2014 8:00 am, Pennsylvania Convention Center, 104-B
Labor & Employment Relations Association/International Association for Feminist Economics
Employment Policies for the Modern Era: Understanding Who Has Access to Policies on Care and How they Affect Employment (J5)
Presiding: Randy Albelda (University of Massachusetts-Boston)
Good for Business? The Case of Paid Sick Leave Legislation in Connecticut
Eileen Appelbaum (Center for Economic and Policy Research)
Ruth Milkman (City University of New York)
[View Abstract]
Impact of Child Care Policies on Parental Employment
Liana Fox (Stockholm University)
Wen-Jui Han (New York University)
Christopher Ruhm (University of Virginia)
Jane Waldfogel (Columbia University)
[View Abstract]
Workplace Flexibility: a Workplace Perk for the Most Valued Workers or Compensation for Those Who Need It Most?
Peter Berg (Michigan State University)
Heather Boushey (Center for American Progress)
Sarah Jane Glynn (Center for American Progress)
[View Abstract]
Discussants:
Heather Boushey (Center for American Progress)
Elaine McCrate (University of Vermont-Burlington)

Jan 03, 2014 8:00 am, Pennsylvania Convention Center, 102-A
Labor & Employment Relations Association
Organizing Low-Wage Workers (J5)
Presiding: Janice Fine (Rutgers University)
Promoting Economic Justice for Home Care Workers in Washington: From Warfare to Kumbayya
Patrice Mareschal (Rutgers University)
[View Abstract] [Download Preview]
Organizing and Raising Standards for Restaurant Workers: The ROC Model
Teofilo Reyes (ROC Restaurant Opportunities Center)
The New York City Carwashero Campaign
Hilary Klein (Make The Road New York)
Creating a New Union Model: Taxi Drivers in Philadelphia
Ronald Blount (Taxi Workers Alliance of Pennsylvania)
Farmworker Organizing for the Long Haul and an Introduction to Food Chain Workers' Alliance
Nelson Carrasquillo (CATA The Farmworkers Support Committee)

Jan 03, 2014 8:00 am, Pennsylvania Convention Center, 106-B
Society of Government Economists
Externalities and the Power of Perceptions for Cash Transfer Programs (D1)
Presiding: David Seidenfeld (American Institutes for Research)
Power of Perceptions: Impacts of Perceived Conditionality in an Unconditional Cash Transfer Program
David Seidenfeld (American Institutes for Research)
Sudhanshu Handa (University of North Carolina)
[View Abstract]
The Impact of a Large Scale Poverty Program on Time Discounting
Sudhanshu Handa (University of North Carolina)
David Seidenfeld (American Institutes for Research)
[View Abstract]
Evaluating Local General Equilibrium Impacts of Zambia's Child Grant Program
Karen Thome (University of California-Davis)

[View Abstract]
The Impact of Immigration on the Well-Being of Natives
Amelie Constant (IZA, Temple University and George Washington Unversity)
[View Abstract]

Jan 03, 2014 8:00 am, Philadelphia Marriott, Meeting Room 406
Transportation & Public Utilities Group
Pricing Digital Delivery of Services (L9)
Presiding: Carolyn Gideon (Tufts University)
Nonlinear Pricing: Self-Selecting Tariffs and Regulation
James Alleman (University of Colorado-Boulder)
Edmond Baranes (Temple University and Centris)
Paul Rappaport (University Montpellier 1)
[View Abstract]
A Comparative Study of Regulation and Pricing in Mobile Communications
Jun-Ji Shih (Academia Sinica)
[View Abstract] [Download Preview]
Evolution of Telephone Markets: A Choice Model of Cell and Land Line Telephone Communication
Wesley W. Wilson (University of Oregon)
[View Abstract]
Spillovers and Marginal Cost Pricing
Christaan Hogendorn (Wesleyan University)
[View Abstract]
Discussants:
David Gabel (Queens College)

Jan 03, 2014 8:00 am, Loews Philadelphia Hotel, P1 Parlor
Union for Radical Political Economists
Heterodox Analysis of the Great Recession (E3)
Presiding: James Devine (Loyola Marymount University)
From the Oil Crisis to the Great Recession: Five Crises of the World Economy
J. A. Tapia Granados (University of Michigan-Ann Arbor)
[View Abstract] [Download Preview]
Capitalism, Crisis and Class: The United States Economy After 2007-2008 Financial Crisis
Özgür Orhangazi (Kadir Has University)
Mathieu Dufour (John Jay College)
[View Abstract] [Download Preview]
Flaws in the Marxian Explanations of the Great Recession
Ismael Hossein-zadeh (Drake University)
[View Abstract] [Download Preview]
Income Inequality and the Appalachian Region Before, During and After the Great Recession
John Hisnanick (US Census Bureau)
[View Abstract] [Download Preview]
Everyday Economics: The 2007 Economic Crisis Through Internet Memes
Elizabeth Ramey (Hobart and William Smith Colleges)
[View Abstract]
Discussants:
James Devine (Loyola Marymount University)
Tim Koechlin (Vassar College)
Michael Perelman (California State University-Chico)

Jan 03, 2014 8:00 am, Loews Philadelphia Hotel, P2 Parlor
Union for Radical Political Economists
Heterodox International Economics (F2)
Presiding: Mehrene Larudee (Al Quds Bard Honors College)
Neoliberalism With a "State Capitalist" Face: The Case of BRIC Countries
Anna Klimina (University of Saskatchewan)
[View Abstract]
Macroprudential Regulations and Capital Flows: The Case of Turkey
Bilge Erten (Columbia University)
Armagan Gezici (Keene State College)
[View Abstract]
The Role of Remittance Flow in the Nepalese Economy
Kalpana Khanal (University of Missouri-Kansas City)
[View Abstract]
Gender and Decent Work in Manufacturing: The Indonesia Case
Shaianne Osterreich (Ithaca College)
[View Abstract]
Discussants:

Mehrene Larudee (Al Quds Bard Honors College)
Firat Demir (University of Oklahoma)

Jan 03, 2014 10:15 am, Philadelphia Marriott, Meeting Room 413
African Finance & Economics Association
African Economic Growth and Development (O1)
Presiding: Gregory Price (Morehouse College)
The Fundamental Determinants of International Competitiveness in African Countries with Special Reference to the CFA Zone
Julius Agbor (Stellenbosch University)
Taiwo Olumide (Centre for the Study of the Economies of Africa)
[View Abstract] [Download Preview]
Financial Development and Manufactured Exports: The African Experience
Evelyn Wamboye (Pennsylvania State University-DuBois)
Rajen Mookerjee (Pennsylvania State University-Monaca)
[View Abstract] [Download Preview]
Efficient Public Sector Audit
Gregory Iyke Ibe (Gregory University)
Moses O. Anuolam (Gregory University)
A.N. Orisakwe (Gregory University)
[View Abstract]
Governance, Growth and Development in Selected West African Countries
Akpan Ekpo (West African Institute for Financial and Economic Management)
[View Abstract] [Download Preview]
Analysis of Chinese Investment in the ECOWAS Region
Jane Karonga (United Nations)
[View Abstract]
Does Education Influence Clean-Tech Venture Capital and Private Equity Exits in Africa?
Jonathan O. Adongo (Missouri Southern State University)
[View Abstract] [Download Preview]
Discussants:
Thouraya Triki (African Development Bank)
David Poyer (Morehouse College)
Fekru Debebe (Educational Testing Service)
Malokele Nanivazo (United Nations University)
Kidaya Ntoko (City University of New York and Queens College)

Jan 03, 2014 10:15 am, Loews Philadelphia Hotel, Commonwealth Hall A1
Agricultural & Applied Economics Association
How Innovation and Technology Affect Contract Terms in Farming (O1)
Presiding: David Zilberman (University of California-Berkeley)
The Economics of Contract Farming: A Credit and Investment Perspective
Liang Lu (University of California-Berkeley)
Xiaoxue Du (University of California-Berkeley)
David Zilberman (University of California-Berkeley)
[View Abstract] [Download Preview]
Contracting for Energy Crops: Effect of Risk Preferences and Land Quality
Xi Yang (University of Illinois)
Nick Paulson (University of Illinois)
Madhu Khanna (University of Illinois)
[View Abstract] [Download Preview]
Adapting Contract Theory to Fit Contract Farming
Steven Wu (Purdue University)
[View Abstract]
The Transition to Modern Agriculture: Contract Farming in Developing Countries
H. Holly Wang (Purdue University)
[View Abstract] [Download Preview]

Jan 03, 2014 10:15 am, Philadelphia Marriott, Liberty Ballroom
American Economic Association
Capital Controls and Macro-Prudential Policies (F4)
Presiding: Mark Spiegel (Federal Reserve Bank of San Francisco)
Capital Controls: Myth and Reality
Nicolas Magud (International Monetary Fund)
Kenneth Rogoff (Harvard University)
Carmen M. Reinhart (Harvard University)
[View Abstract] [Download Preview]
Prudential Policy for Peggers
Stephanie Schmitt-Grohe (Columbia University)

Martin Uribe (Columbia University)
[View Abstract]
Capital Controls and Optimal Chinese Monetary Policy
Chun Chang (Shanghai Advanced Institute of Finance)
Zheng Liu (Federal Reserve Bank of San Francisco)
Mark Spiegel (Federal Reserve Bank of San Francisco)
[View Abstract] [Download Preview]
Capital Controls or Macroprudential Regulation?
Anton Korinek (Johns Hopkins University and NBER)
Damiano Sandri (International Monetary Fund)
[View Abstract]
Discussants:
Javier Bianchi (University of Wisconsin-Madison)
Alessandro Rebucci (Johns Hopkins University)
Xiaodong Zhu (University of Toronto)
Suman Basu (International Monetary Fund)

Load More Load All

2015 Annual Meeting

Registration for the ASSA and AEA Continuing Education Meetings is NOW OPEN.

The 2015 Annual Meeting will take place in Boston, MA on January 3-5, 2015. *Please note this is a Saturday/Sunday/Monday meeting this year*. The headquarters hotel will be the Sheraton Boston.

2015 Preliminary Program
2015 Daily Program of Events

Deadlines

Registration: Deadline to cancel on conference registration is December 3, 2014.
Housing: Deadline to guarantee convention hotel rate is December 3, 2014. You may continue to make and modify reservations until December 15 at 3:00 pm. *No refunds if registering after December 3 or on-site.*

Registration Fee	Received by Dec. 3	After Dec. 3 on-line only
Regular Attendee	$55.00	$115.00
Full-time Student (Student ID required to pickup badge)	$25.00	$45.00
Spouse, Guest or Administrators (If affiliation is needed you must register separately and pay the full fee.)	$25.00	$45.00

General Information
ASSA Registration Form (PDF)
AEA Continuing Education Program (New location: Hyatt Regency Downtown)
AEA Continuing Education Registration Form (PDF)
Job Placements Services/Disclosure Codes
ASSA Hotel Map
ASSA Hotel Rates (Do not call the hotels direct - you will not get the convention rate.)
Housing Instructions and Reservation Form (PDF)
Online Housing (Registration ID Required)
Suites and Suite Diagrams

KiddieCorp Child Care
Amtrak
Airport/Hotel Transportation
Parking

Links For Organizers and Exhibitors

Exhibit Booth Registration is NOW OPEN.
Special Events Form *(for group organizers to schedule events)*
Exhibit Hall Floorplan
Exhibitor Registration Packet
Advertising Contract

AEA in conjunction with approximately 55 associations in related disciplines, holds a three-day meeting each January to present papers on general economic subjects. Over 520 scholarly sessions are held. In 2014, 12,218 registered.

SCHEDULE OF FUTURE MEETINGS:

January, 3-5, 2015 (Saturday, Sunday & Monday)
Boston, MA - Sheraton Boston

Annual Meeting
Submissions
Registration/Housing
ASSA 2015 Preliminary Program
2015 Daily Program of Events
Previous Annual Meeting Papers and Webcasts
Archive of Past Programs
AEA Continuing Ed. Program
AEA Continuing Ed. Webcasts
Crossword Puzzles

Other Information

The next meeting is scheduled for January 3-5, 2015 in Boston, MA. The headquarters hotel is the Sheraton Boston.

Enhance your core skills and stay abreast of key developments in research and teaching from leading scholars at the 2015 Continuing Education Program in Boston.

Papers and Proceedings of the Annual Meeting is published in the May issue of the *American Economic Review*. The guidelines for Papers and Proceedings are available online.

Contact Us

January 3-5, 2016 (Sunday, Monday & Tuesday)
San Francisco, CA - Hilton San Francisco

January 6-8, 2017 (Friday, Saturday, & Sunday)
Chicago, IL - Hyatt Regency Chicago

January 5-7, 2018 (Friday, Saturday, & Sunday)
Atlanta, GA - Atlanta Marriott Marquis

January 4-6, 2019 (Friday, Saturday, & Sunday)
Philadelphia, PA - Philadelphia Marriott

January 3-5, 2020 (Friday, Saturday, & Sunday)
San Diego, CA - San Diego Marriott Marquis & Marina

January 3-5, 2021 (Sunday, Monday & Tuesday)
Chicago, IL - Hyatt Regency Chicago

January 7-9, 2022 (Friday, Saturday & Sunday)
Boston, MA - Sheraton Boston

Dictionary

SAVE POPULARITY

affinity group

affinity group

noun

Definition of AFFINITY GROUP

: a group of people having a common interest or goal or acting together for a specific purpose (as for a chartered tour)

Quick read: **10 gorgeous winter quotes** »

First Known Use of AFFINITY GROUP

1970

Rhymes with AFFINITY GROUP

primordial soup

Browse

Next Word in the Dictionary: affinity marketing
Previous Word in the Dictionary: affinity chromatography
All Words Near: affinity group

Ask The Editor Videos

Is It 'Attorney Generals' Or 'Attorneys General'?

Fun, Funner, Funnest

Seen & Heard

What made you want to look up *affinity group*? Please tell us where you read or heard it (including the quote, if possible).

10 Charming Words Nasty People

Put-downs with flair

Learn More »

9 comments

Add a comment...

Comment using...

Diana Michel · Patent & Trademark Office

I want to know if a health and wellness council can be called an affinity group.

Reply · Like · April 19, 2014 at 9:56am

When "literally" isn't literal

How to use a word that (literally) drives some people nuts

Watch Now »

Ashleigh Fisher · University of Pretoria

An academic article exploring the use of links on facebook

Reply · Like · Edited · March 5, 2014 at 3:16am

Whitely Joan · University of Phoenix Alumni Association

Question from my professor.

Reply · Like · April 17, 2013 at 6:05am

Sammy Wann · Florida State University

Based off of the last end of the year call...I thought I'd go ahead and look up Webster's Definition :)

Reply · Like · 1 · December 7, 2012 at 12:53pm

Sammy Wann · Florida State University

Sofia Reed has been running the calls phenomenally. Great job ladies! with Ameerah Mukayed

Reply · Like · 2 · December 7, 2012 at 12:59pm

Sofia Reed

Thank you both for a great job too :)

Reply · Like · December 7, 2012 at 1:16pm

Dot Mi

I get calls which are unwanted

Reply · Like · October 26, 2012 at 7:15am

View 2 more

Facebook social plugin

Fear of cats?

Ailurophobia, and 9 other unusual fears

Learn More »

Know what this is?

Test your vocab with our fun, fast game

Go Play »

Join Us

Merriam-Webster on Facebook »

Merriam-Webster on Twitter »

Book: Digital and Print

Merriam-Webster references for Mobile, Kindle, print, and more.

See All »

Other Merriam-Webster Dictionaries

Spanish Central »

Learner's ESL Dictionary »

WordCentral for Kids »

Visual Dictionary »

SCRABBLE® Word Finder »

Webster's Unabridged Dictionary »

Britannica English - Arabic Translation »

Deloitte.

March 21, 2011

Deloitte Consulting LLP

Final Report

Evaluation of the EPA Office of Civil Rights

Environmental Protection Agency
Order # EP10H002058
SOW Task 4: Final report

Audit . Tax . Consulting . Financial Advisory.

Environmental Protection Agency

Evaluation of the EPA Office of Civil Rights

Final Report

March 21, 2011

Presented by

Deloitte Consulting LLP

1001 G Street NW, Suite 900

Washington, DC 20001

Technical POC:

Tracy Haugen, Director

Tel. 202-758-1750

Email: thaugen@deloitte.com

Submitted To:

Martine Carrillo

Project Officer

Environmental Protection Agency

Email: Carrillo.Martine@epamail.epa.gov

Deloitte.

Deloitte Consulting LLP
1001 G Street NW, Suite 900
Washington, DC 20001
USA

Tel: +1 703 885 6000
www.deloitte.com

March 21, 2011

Martine Carrillo, Project Officer
Office of Acquisition Management
Environmental Protection Agency
1200 Pennsylvania Avenue, NW
Washington, DC 20460

RE: Final Report on the Evaluation of the EPA Office of Civil Rights

Dear Ms. Carrillo:

This document serves as the final deliverable for the Office of Civil Rights (OCR) project. This deliverable presents our findings and recommendations to improve the overall efficiency and effectiveness of the Office of Civil Rights and its three program offices:

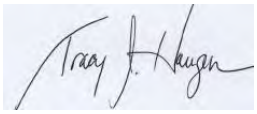
- External Complaints and Compliance (Title VI);
- Employment Complaints Resolution (Title VII); and,
- Affirmative Employment and Diversity (AED).

Given the urgency within the Agency to rapidly transform the OCR function, Deloitte developed a plan that highlights the priority and sequencing for implementing each recommendation.

We have very much enjoyed working with the Agency on this engagement. Civil Rights and Diversity and Inclusion are core tenets that are promoted within Deloitte's culture. We hope you find our firm's passion for this subject matter is reflected in the depth of the analysis and quality of the recommendations within this report. Moreover, we are looking forward to continued discussions with the Agency regarding our findings and recommendations.

Please do not hesitate to contact me at 202-758-1750, or by e-mail at thaugen@deloitte.com.

Sincerely,



Tracy Haugen, Director
Deloitte Consulting LLP

Table of Contents

Document Information and Approval

Document Information

Title	Final Report
Revision	6.0

Issue Date	March 21, 2011
Author (s)	Deloitte Consulting LLP

Security Level	For Internal Use Only – Not for Distribution

Filename	EPA-OCR_FinalReport.docx

Approval Statement

I have read and understood the above named document and accordingly wish to formally convey Sign-Off to the above named document.

Program Director: _____ Date: _____

: _____ Date: _____

: _____ Date: _____

: _____ Date: _____

Revision History

ID	Issue Date	Changed by	Change Summary
1	01/19/2011	N/A	Original submission of annotated outline for review and approval by EPA project team
2	01/24/2011	Deloitte	Submission of Sections 1 and 2 for feedback and approval to proceed with full revision
3	02/11/2011	Deloitte	Submission of Draft Final Report for review and approval by EPA project team
4	02/28/2011	EPA	Comments on Draft Final report
5	03/07/2011	Deloitte	Response to comments and updates to Final Report
6	03/21/2011	Deloitte	Final edits

1. Executive Summary

The Environmental Protection Agency (EPA) contracted with Deloitte Consulting (Deloitte) to conduct an assessment of the Office of Civil Rights (OCR). The contract objectives were to:

- Conduct a comprehensive review and program evaluation to determine how effectively OCR is meeting its mission and regulatory mandates.
- Complete a comprehensive review of the OCR structure, staff and functions to pinpoint strengths and weaknesses.
- Assess Headquarters, field office, and laboratory interactions, present findings and deliver high-level recommendations.
- Deliver an objective evaluation which EPA officers can use to guide improvements for OCR functions and day-to-day operations.

Findings and Conclusions

EPA's senior leadership has increased the Agency's emphasis on resolving civil rights issues that are critical to fulfilling its mission. Recently, EPA leaders have been providing significant support to OCR, investing both time and resources needed to address significant performance challenges, including the following:

- The Office has not adequately adjudicated Title VI complaints – those addressing allegations of discrimination against communities of citizens affected to environmental rules promulgated by the EPA.
- OCR has struggled to track, investigate, and resolve Title VII cases – those addressing Equal Employment Opportunity (EEO) violations inside the Agency – in a timely or effective manner.
- OCR has not completed compliance checks of EPA grantees, in a timely or effective manner, to ensure that grantees are not engaging in discrimination in their work.
- OCR has not consistently filed its statutory affirmative employment reports over the past five years, although the 2010 MD-715 was submitted on time.

These challenges emerged over the past decade and have continued to erode OCR's performance. To a significant extent, they are attributable to OCR's difficulty in building a staff with the qualifications, knowledge and training to effectively complete its mission-related work, much of which is highly technical and complex. Over a period of several years, required competencies have not been well-defined, nor has there been any attempt to determine the extent to which staff possess the necessary competencies to perform successfully. There are limited formal training or career development programs to provide training in the work they have been assigned to perform, despite the challenging, sensitive, and often complex nature of the work.

OCR staff members also suffer from the absence of the rudiments of organizational infrastructure – well-documented policies and procedures, standardized processes, and effective systems. Staff members are often confused about their job duties. Managers lack the performance tracking and management systems and processes needed to manage the office's business and hold staff members accountable for effectively executing their jobs. OCR has not implemented the processes needed to collect and maintain information needed to fulfill statutory recordkeeping requirements.

Finally, OCR has operated in an insular fashion that has limited its effectiveness. It has not taken full advantage of the extensive technical expertise available in the program areas of EPA that would enable it to conduct better investigations and achieve more expeditious resolutions. OCR has not provided sufficient clarity to the program management, human resources and EEO offices to secure the data it needs to complete its submissions in a timely fashion. Nor has it effectively leveraged other EPA and state government officials whose relationships, contacts and local knowledge would enhance its field investigations. Additionally, OCR has not conducted much outreach to state government departments of environmental quality to build awareness of circumstances that can give rise to allegations of discrimination from communities with environmental concerns.

This set of circumstances has resulted in a record of poor performance:

- Only 6% of the 247 Title VI complaints have been accepted or dismissed within the Agency 20-day time limit.[1] [2]
- OCR's backlog of Title VI cases stretches back to 2001. At the time of this report's publication, there were numerous cases that have been awaiting action for up to four years. Two cases have been in the queue for more than eight years.
- In the area of Affirmative Employment and Diversity, OCR did not even complete its annual Management Directive 715 (MD-715) EEO report (a basic administrative task required of all Federal agencies) for 2006, 2007, and 2008.[3] [4] It is our understanding that 2010 MD-715 was filed on time.
- OCR's Title VII function is known for poor investigative quality and a lack of responsiveness. It has not been able to perform its most fundamental Title VII administrative tasks related to filing mandatory reports and processing complaints and writing final agency decisions.

This situation has exposed EPA's Civil Rights programs to significant consequences which have damaged its reputation internally and externally. In the Rosemere Neighborhood Association case regarding the timeliness of a Title VI complaint response, it was found that "OCR's failure to process the Retaliation Complaint in accordance with the timeline set forth in 40 C.F.R. S7.115(c)(1) constitutes agency action unlawfully withheld pursuant to the Administrative Procedures Act, 5 U.S.C. S706(1)." [5] OCR's performance has also damaged its reputation within EPA. It was noted repeatedly in interviews with EPA staff and management that OCR has been viewed as an organization that performs poorly and does not offer specialized expertise.

Much of this owes to OCR's challenges at the leadership levels over a period of years, [redacted] As leaders and staff struggled within this turbulent environment, OCR seemed to lose sight of its mission and priorities. It appeared to place too much emphasis on minor responsibilities, like executing heritage events, and not enough on the critical discrimination cases affecting employees and disadvantaged communities. In addition to not setting the right tone, past OCR leaders seemingly abdicated responsibility for crafting a vision, developing strategies, setting objectives, tracking performance and

[1] "Settlement Agreement" 3/17/2010 between Rosemere Neighborhood Association (RNA) and EPA, p 3, paragraph 1.
[2]. "Final OCR T6 Complaint Listing (10.15.2010).xls" received from Helena Wooden-Aguilar, Friday 11/19/2010 at 3:10 PM.
[3] "Inside EPA: Personnel Disputes Roil EPA's Rights Office, Undermining Equity Agenda." February 19, 2010.
[4] Confirmed during AED staff interviews.
[5] "Settlement Agreement" between Rosemere Neighborhood Association (RNA) and EPA. March, 17, 2010. p3, paragraph 1.

making critical decisions that would have improved OCR's effectiveness. While a new Director was recently appointed, other key leadership positions remain unfilled.

Recommendations

EPA has taken the initial steps to address OCR's current challenges. First, the Agency commissioned this study as a vehicle to engage OCR and its stakeholders in the process of evaluating organizational performance improvement opportunities. Second, it has appointed an experienced Director with a strong understanding of OCR priorities. Third, and most importantly, it has made improving the OCR function a top priority, recognizing its importance to achieving the overall objectives of the EPA.

Yet, much work remains. The recommendations in this report are intended to address the near term need to effectively perform fundamental processes such as complaint resolution, while establishing the organizational and operational infrastructure needed to transform OCR into a model Civil Rights organization for the longer term. Immediate steps should focus on making OCR more effective in its day-to-day operations and expanding responsibilities for civil rights across EPA. In the long run, EPA should develop a strategy anchored in complaint prevention in order to effectively address both Title VI and Title VII issues.

EPA's first improvement actions must address current deficiencies in OCR's leadership and workforce competencies:

- Complete efforts to fill OCR's leadership positions expeditiously with qualified, experienced, and motivated civil rights professionals. A competent leadership team will enable OCR to implement all of the other needed changes, while building its credibility.
- Reevaluate all staff job roles and formally document required skills, competencies and experiences for each role. With well-defined job roles, OCR can evaluate its current workforce against the requirements and identify gaps.
- Develop and execute a workforce plan that includes creation of well-defined career paths, employee performance management processes, new training programs and employee recruiting and selection processes.

Building a more capable workforce from top to bottom will enable EPA and OCR to address its significant day-to-day operating issues and implement the other more strategic changes that are required.

To expand responsibility for achieving the Agency's civil rights objectives and to bring needed Agency support to OCR, the Administrator should establish two cross-functional or "networked" teams. A networked team brings together people from different areas within EPA to work as a project team in accomplishing a set of specific goals but does not alter formal reporting relationships,

These "networked" teams should help OCR set priorities, marshal resources and remove obstacles that challenge timely and effective completion of important tasks. These teams should be accountable and report to the Administrator for driving achievement of the EPA's civil rights objectives through broad involvement of program offices, field offices, and the other Headquarters human capital and legal functions.

The External Civil Rights Networked Team (External Team) should be established to address the pressing need to expedite effective resolution of complex Title VI cases. It should adopt a standard process to charter cross-functional investigative teams that bring together the right expertise to address each complaint. Specifically, the External Team should:

- Assist the OCR to prioritize complaints, ensuring their alignment with overall EPA and Administration objectives.
- Bring the right program and field leaders together to assess the investigative requirements of each complaint.
- Work with program and field leaders to identify and commit the right experts to each cross-functional investigative team.
- Hold those outside of OCR accountable for fulfilling their commitments to investigative analysis on behalf of the Administrator.

The External Team should be chaired by the Environmental Justice Lead. It should be composed of leaders from Office of Enforcement and Compliance Assurance (OECA), the Civil Rights and Finance Law Office (CRFLO), ORD, the Office of Grants and Debarment (OGD), and the Title VI program office.

The Internal Diversity and Inclusion Networked Team (Internal Team) should be established to address OCR's deficiency in gathering, analyzing and reporting important EEO data for reporting and remedial actions. It should help Affirmative Employment and Diversity (AED) facilitate the participation of other EPA departments in the timely collection of accurate data. Additionally, AED should:

- Clarify and reinforce to staff that its primary role is to identify barriers and implement remediation strategies.
- Use the MD-715 submission as the focal point to guide all communications with stakeholders across the Agency.
- Hire, train, or realign staff members who possess a balance of barrier analysis expertise and passion for civil rights and diversity.
- Coordinate programming, guidance and direction through its network of EEO Officers.
- Develop awareness and training programs that will help managers across EPA preclude complaints and promote the agency's civil rights objectives.

The Internal Team should be chaired by the AA for the Office of Diversity, Outreach and Collaboration (ODOC). It should be composed of leaders from Associate Regional Administrator (ARA) EEO, the Office of Human Resources (OHR), CRFLO, Title VII and AED.

Two other organizational changes should be adopted. EPA should re-establish the dotted line relationship between ARA EEO Officers and the Director of OCR for tighter integration and collaboration with the field. In addition, OCR should establish a Headquarters EEO Officer position to develop and manage EEO and AED programs for the staff at headquarters, which currently represents a significant percentage of overall EEO complaints. (For additional background information and alternatives, see Section 4.1). [6] Executing these initiatives should greatly enhance EPA's ability to achieve and maintain compliance with Equal Employment Opportunity Commission (EEOC) reporting requirements, while providing a firmer foundation for AED to identify and address barriers.

To achieve its Title VII objectives, OCR must upgrade its workforce capabilities in the areas of analysis, legal research and communications. It should also develop standard quality assurance processes and use

[6] Recommendation based on analysis and interviews. Section 4.1 begins on page 20.

them to identify performance issues. A number of other operational improvements are required to reduce backlog and increase quality. OCR should:

- Implement a case management tool to enable case tracking, reporting, analysis, and performance measurement.
- Increase the use of the Alternative Dispute Resolution program at both the Headquarters and field offices, and institute conflict management training program targeted for staff and management.
- Assign high-performing field-level EEO Officers on a temporary basis.
- Prepare staff to manage investigations function performed by contractors.

Implementing these improvements should lead to significant reductions in the backlog while instituting higher standards for quality.

Implementation Considerations

The changes needed to address current organizational and operational issues will require a 12-24 month timeframe. Instituting changes that have the potential to make OCR a model civil rights organization is likely to take longer. While EPA should be thinking long term, it must focus implementation efforts initially to address specific performance gaps, such as the quality of work products and an ad hoc approach to coordination with key internal operating partners, i.e., Human Resources (HR), Office of General Counsel (OGC), and OGD. Implementation should proceed in phases to address both immediate operational needs and the agency's desire to fulfill a higher order of objectives for its civil rights function:

- **Stabilize** (March to October, 2011) – Address operational challenges to improve current effectiveness.
- **Reassess** (October, 2011) – Review progress of improvement efforts and develop strategies to institutionalize changes.
- **Institutionalize** (October, 2011 to March, 2013) – Drive institutional changes and make strategic investments.

In the Stabilize Phase, EPA should focus on implementing recommendations that address current deficiencies in leadership and workforce competencies, organizational changes, and basic process improvements. The Reassess Phase should be a time to assemble key leaders and stakeholders to take stock in progress to date, revisit civil rights objectives drawing on new insights, and develop plans for longer-term institutional changes and strategic investments. The Institutionalize Phase should focus on implementing strategic investments in training, awareness and prevention programs, and new information systems. Subject to constraints posed by conflicting priorities, new initiatives, and emerging directives from outside EPA, the Agency should set a goal to implement the recommendations within a 12-24-month period.

2. Introduction

2.1 Purpose and Scope

The Environmental Protection Agency (EPA) contracted with Deloitte Consulting (Deloitte) to conduct a comprehensive review and program evaluation of the Office of Civil Rights. The purpose of the assessment was to determine the extent to which the structure, policies, procedures, and resources of the Office of Civil Rights (OCR) facilitate accomplishment of EPA's equal employment opportunity and equal opportunity mission, and to assess whether OCR operates in accordance with applicable laws and regulations (e.g., Equal Employment Opportunity Commission (EEOC) regulations set forth at 29 C.F.R. Part 1614, 40 C.F.R. Part 5 & 7, EEOC's MD-110 and MD-715 and external statutes including Title VI).

This study evaluated the organizational structure, external civil rights programs, non-discrimination laws and statutes, internal operations, staff competencies, and resources of the Office of Civil Rights to determine its ability to meet its functional responsibilities and operations. In addition, the study conducted interviews with nine federal agencies and other external research to benchmark EPA's civil rights function. Below is the listing of agencies and interviewed personnel:

Figure 2-1. Agencies and Personnel Interviewed

Federal Agencies Interviewed	
Federal Highway Administration	**Office of Civil Rights** Brenda Armstead, Internal Programs and External Investigations and Adjudications Director Thalia Williams, EEO Specialist-Title VI
Department of the Interior	**Office of Civil Rights** Sharon D. Eller, Director Office of Civil Rights Lola Hatcher-Capers, Deputy Director, Office for Civil Rights Alvin Dillings, Senior EO Policy Advisor Jack Andre, Chief, Public Civil Rights Division Sylvia Jones, Special Emphasis Program Manager
Department of Energy	**Office of Civil Rights** Bill Valdez, Acting Director Sharon Wyatt, Attorney-Advisor Neil Schuldenfrei, Senior Attorney-Advisor C. Lloyd Buddoo, Senior Attorney-Advisor Bill Lewis, Deputy Director of Civil Rights
NASA	**Office of Equal Opportunity and Diversity** Brenda Manual, Associate Administrator Frederick Dalton, Conflict Management Program
Department of Housing and Urban Development (HUD)	**Fair Housing and Equal Opportunity** Sara Pratt, Deputy Assistant Secretary-Enforcement and Programs Lynn Grosso, Director-Office of Enforcement Will Brandt, Information Services and Communication Tracy Mullins, Acting Director-Compliance and Disability Rights
Department of State	**Office of Civil Rights** John M. Robinson, Director & Chief Diversity Officer Pamela Britton, Law Clerk
U.S. Forest Service	**Office of Civil Rights** Debra A. Muse, Director, Office of Civil Rights Deborah Lombardino, Branch Chief Eurial Turner, Assistant Director of Programs
Department of Labor	**Civil Rights Center** Julia Mankata-Tamakloe, Chief-Office of External Compliance Violet Parker, Chief- Diversity Management

	Naomi Barry-Perez, Chief- Office of Internal Enforcement
National Institute of Health	**Office of Equal Opportunity and Diversity Management** Lawrence N. Self, Director Sheila Stokes, Director-Complaints Management and Resolution Rose Pruitt, Manager

Lastly, the study looked for opportunities for OCR to become more effective and move towards its vision to become a "model Office of Civil Rights for the government."

During the project kickoff held on September 8, 2010, EPA and Deloitte project team leadership confirmed the list of deliverables for each task as follows:

- Tasks 1 and 2: Develop Interim Report and Deliver Preliminary Briefing
- Tasks 3 and 4: Develop Final Report and Deliver Final Briefing

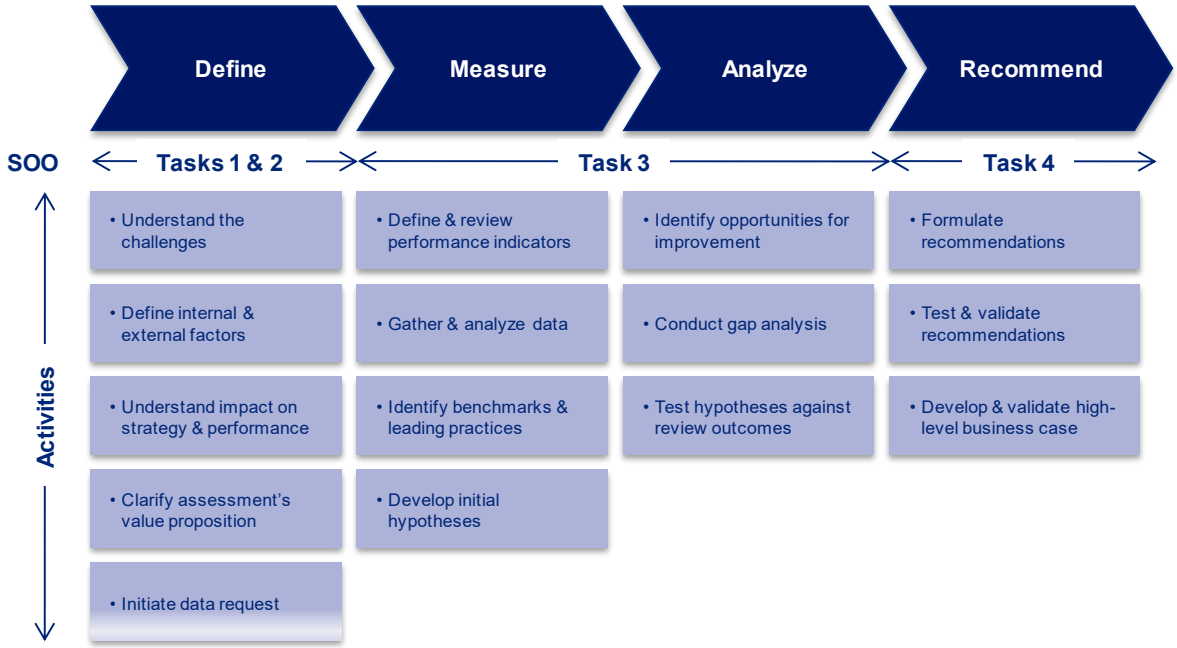
2.2 Approach

Deloitte's approach included a large number of internal and external interviews, a benchmark effort and a comprehensive desk study of leading practices. The Deloitte team conducted one-on-one interviews and focus group sessions with more than one hundred EPA employees to ensure broad inputs across organizational functions and hierarchies. The team conducted a benchmark study that included interviews at nine other federal agencies and with senior leadership at the Equal Employment Opportunity Commission (EEOC). In addition, Deloitte completed comprehensive desk study of leading practices in civil rights, and where relevant to the study, diversity and inclusion.

During the course of the project, Deloitte solicited continuous feedback during its status meetings to address any scheduling or other project issues, ensure findings and recommendations consistent with EPA's unique requirements, and to incorporate any missing data points that we may have overlooked. In addition, Deloitte conducted executive briefings to review preliminary findings and themes with EPA executives, including the Chief of Staff and Deputy Chiefs of Staff.

As depicted in Figure 2.2, the Statement of Objectives (SOO) for the evaluation divided the study into four sets of tasks that are aligned with Deloitte's Organizational Assessment Approach. This final report is the culmination of that work and offers EPA leadership recommendations to revitalize the EPA Office of Civil Rights (OCR) and position it to become a model civil rights organization.

Figure 2-2. Deloitte's Organizational Assessment Approach



2.3 Data Collection

Deloitte collected both qualitative and quantitative data to inform its research activities.

Interviews: Deloitte interviewed agency executives, key stakeholders, and OCR staff to gather current state information and seek validation that proposed recommendations align with EPA's unique culture and values, business strategies, politics and bureaucracy.

Job Analysis: Deloitte administered a web-based job analysis survey as a part of this assessment to 45 OCR and EEO Officer resources from the 10 regions, three laboratories, and Headquarters (HQ). The survey involved 22 questions across the following four categories: workload distribution; skill requirements; internal and external contacts; employee morale and workplace satisfaction; and an open forum to add additional comments.

OCR Document Review: Deloitte reviewed relevant EPA, OCR, and working group documents to better understand the processes, people, structure, and resources of OCR. Additionally, Deloitte sought copies of past "Diversity Action Plans" and any copies available of previously completed OCR Program Reviews though these were not provided.

Leading Practices Analysis: Deloitte interviewed executives and staff of nine other federal agencies' Civil Rights offices (or equivalent naming convention) to assess their approach to people, processes, structure, technology, and other relevant factors contributing to "model" design across Title VI, Title VII, AED, and Reasonable Accommodations functions. Deloitte also reviewed reference material from the Equal Employment Opportunity Commission and the Department of Justice's Federal Coordination and Compliance Section.

EPA Intranet: Deloitte sought access to the EPA Intranet to review stakeholder communications, consistency of mission statements and functional descriptions between HQ and field offices, and to

assess the breadth of recommendation options around web-based technologies.[7] (Note: EPA was not able to grant access until January 5, 2011, two days before the draft Final report was submitted. EPA did produce a thumb drive on January 5 as an alternative. However due to the timing, it was not considered for this report.)

2.4 Stakeholder Interviews

In an effort to obtain inputs from all parties involved with or affected by OCR's performance, Deloitte recommended representation from staff, oversight organizations, partners, and customers. The project team worked with EPA project leadership to finalize the interviewees, which included all the recommended groups and stakeholders from internal management groups, such as the EPA Human Resources Council. At a high level, the interviews represented the following key stakeholder groups:

- *Office of the Administrator* – Interviews with the top executive team including the EPA Administrator, Deputy Administrator, Chief of Staff;
- *Office of Civil Rights* – Interviews with more than 40 OCR managers and line employees;
- *Office of General Counsel and Office of Inspector General* – Interviews with 5 members, including the General Counsel;
- *EPA Program Offices* – Interviews with 7 senior and mid-level leadership staff from multiple program areas; and
- *Equal Employment Opportunity Commission* – Interview with the senior representative for Federal programs at the EEOC, the main oversight body for the Civil Rights Act.

Deloitte advised participants that interviews were confidential and non-attributable, and provided interviewees the opportunity to give additional input by contacting either the EPA Project Officer or through direct contact with the Deloitte interviewer via email or telephone. The project team aggregated the information collected in these discussions and considered it in conjunction with existing documentation so that no single source had more influence than another, regardless of role.

Two experienced interviewers facilitated each interview, using standardized interview guides focused on six primary questions that were provided to respondents prior to the interview session. The staff interview questions, which covered two areas – organization and job analysis – are listed below:

PART 1: ORGANIZATIONAL QUESTIONS

- What do you think the vision and mission of OCR should be?
- What are the top three priorities for your particular team?
- What would you consider positive and negative about the overall work environment within OCR?
- Does your immediate supervisor provide you with sufficient feedback and guidance?
- What are the resources that you need to do your job effectively and efficiently?
- What are you held accountable for with regards to your work performance? How and when are you evaluated?

[7] Deloitte was notified on January 05, 2011 at 1:42 PM that the tokens were available. This report was submitted two days later on January 07, 2011. As a result, Deloitte was unable to complete its review of the EPA intranet.

PART 2: JOB ANALYSIS QUESTIONS

- What is your role within the organization?
- What level of knowledge does your job need to have in order to be successful? Please refer to specific product/professional knowledge.
- What previous experience do you believe is needed to be successful?
- What qualifications/training does the job holder need to have to undertake this job successfully?
- What are the job holder's daily, weekly, monthly, and yearly deliverables?
- What processes are the deliverables of this position dependent on?
- What other comments would you like to make regarding your job role?

The EPA non-OCR interview questions are listed below:

NON-OCR INTERVIEW QUESIONS

- What are your expectations for OCR?
- What do you believe are strengths and successes of OCR?
- Where do you see shortcomings/deficiencies within OCR?
- From your perspective what are the priorities for OCR?
- What do you perceive are the major challenges for change?
- What other stakeholders should we make sure to meet with, such as informal influencers?

3 Overview of the Office of Civil Rights (OCR)

3.1 Background

Federal agencies implement The Civil Rights Act of 1964 (i.e., "the Act"), as amended, which prohibits discrimination on the basis of race, color, religion, national origin or sex[8]. Federal agencies commonly organize their civil rights functions into three distinct programs, including Equal Employment Opportunity (EEO), External Civil Rights, and Affirmative Employment.

3.2 OCR Overview

The Office of Civil Rights (OCR) similarly divides the Environmental Protection Agency's (EPA) civil rights responsibilities into three program offices[9]: External Complaints and Compliance (Title VI); Employment Complaints Resolution (Title VII); and Affirmative Employment and Diversity (AED). Each program office is headed by an Assistant Director who manages headquarters employees and provides leadership, direction, and guidance to carry out the Agency's equal employment and equal opportunity programs. These programs provide policy and technical assistance to EPA's Headquarters, regional offices, and laboratories located throughout the country. OCR's headquarters office also has a Reasonable Accommodations function that serves the needs of both headquarters and field staff.

The Director of OCR has a direct line reporting relationship to the EPA Administrator and takes administrative direction from the Chief of Staff or Deputy Chief of Staff on a day-to-day basis. The Director serves as the principal adviser on EPA's nationwide internal and external Civil Rights programs and policies. OCR's principal role is to uphold the Agency's commitment to EEO, equity, and diversity in the workplace and foster an environment that is free from discrimination, reprisal, and harassment.

Figure 3-1. OCR's Primary Responsibilities

OCR's Primary Responsibilities

- **External Complaints and Compliance (Title VI)** monitors compliance, processes complaints and conducts outreach and training related to Federal Title VI statutes and EPA's nondiscrimination regulations, 40 C.F.R. § 7.130(b).
- **Affirmative Employment and Diversity (AED)** analyzes barriers to employment and advancement opportunities for women, minorities, and persons with disabilities and implements and reports remediation measures.
- **Employment Complaints Resolution (Title VII)** processes discrimination complaints related to Federal Title VII statutes and provides guidance for applying the alternative dispute resolution mechanism.

[8] Source: http://www.eeoc.gov/laws/statutes/index.cfm
[9] Source: http://www.epa.gov/civilrights/aboutocr.htm

External Complaints and Compliance (Title VI) Program

The mission of EPA's External Compliance (Title VI) program is to ensure that recipients of EPA financial assistance comply with relevant non-discrimination requirements under Federal law.[10] The Title VI division is staffed by an Assistant Director, six case managers, and one senior case manager, reflecting the heavy emphasis on the complaints function.

The program has three primary functional responsibilities including outreach and training, compliance and enforcement, and complaints management. The outreach and training responsibility is administered primarily through OCR's web presence which includes a series of links to laws, regulations, and online training. Compliance and enforcement is administered through a pre-award form (form number 4700-4) that is attached to all grant applications and included in grant packages issued by the Office of Grants and Debarment (OGD) and implemented through OCR's network of field-based EEO Officers. The Title VI case management process is divided into three discreet stages: 1) Jurisdictional Review, 2) Investigation, and 3) Final Agency Decision. Each stage concludes in a quality checkpoint with the Assistant Director, the Civil Rights and Finance Law Office (CRFLO), or both and always returns to the Case Manager before moving to the next stage. Jurisdictional Review and Investigation stages have set targeted timeframes. In the Jurisdictional Review stage, Case Managers have twenty days to prepare and finalize an Acceptance Letter. The investigation stage must be completed within one hundred and eighty days unless requests for information from the complainant are not provided in a timely manner.

The Title VI division is staffed by an Assistant Director, six case managers, and one senior case manager, reflecting the heavy emphasis on the complaints function. Case managers are assigned approximately five cases, while senior case managers are assigned up to seven cases.

Affirmative Employment and Diversity (AED) Program

AED is responsible for providing the leadership, direction and advice to managers and supervisors in carrying out their equal opportunity and civil rights responsibilities[11]. AED staff manage and oversee the Agency's Affirmative Employment and Special Emphasis and Diversity Programs. The National Special Emphasis and Diversity Program Managers develop internal EEO policies and procedures, develop and implement training, and provide oversight and technical assistance to Headquarters program management offices, regional offices and laboratories.

EPA's Affirmative Employment and Diversity (AED) program implements the following seven National special emphasis programs:[12]

- Black Employment Program
- Federal Women's Program
- Hispanic Employment Program
- Asian American/Pacific Islander Employment Program
- American Indian/Alaska Native Employment Program
- Diversity Programs for Older Workers and Sexual Orientation
- Disability Employment Program

[10] Source: http://www.epa.gov/civilrights/extcom.htm
[11] Source: http://www.epa.gov/civilrights/summ.htm
[12] Source: http://www.epa.gov/civilrights/summ.htm

AED has a staff of nine full-time time employees including an Assistant Director (GS-15), an Affirmative Employment Program Manager (GS-14) who serves as the custodian of the workforce data, and six Equal Employment Managers (GS-14 and GS-13) who are the lead representatives for their respective employment programs which include targeted recruiting. The Assistant Director and Disabilities Equal Employment Manager positions were vacant at the time of this report. The majority of Equal Employment Managers (EEMs) have previous experience in employment complaints programs or counseling, though few have experience or education directly related to their affirmative employment program area to assist in developing remediation strategies to address the affirmative employment barriers.

Employment Complaints Resolution (Title VII) Program

The mission of EPA's Employment Complaints (Title VII) program is to provide equal employment opportunity; eliminate discrimination in employment; and maintain an environment that is free from any form of prohibited discrimination.[13] Employees can pursue their allegation through either the informal or Alternative Dispute Resolution (ADR) mechanism, or file a formal complaint with OCR or directly with the Equal Employment Opportunity Commission (EEOC).

When employees choose to file a formal complaint of discrimination with OCR, the case is processed at the Headquarters OCR office by Equal Employment Specialists (EES) directly aligned to the region or laboratory of the case's origination. The formal complaints process moves through three stages including: (1) Jurisdictional Review, (2) Investigation, and (3) Final Agency Decision (FAD).

OCR has a staff of eight EESs reporting to an Assistant Director who reviews outputs along each stage of the case management process and moves completed work products to CRFLO for legal sufficiency review and, finally, the Director of OCR for approval and signature. Six of the eight EES positions are responsible for completing the Jurisdictional Review and Investigation stages while the remaining two EES positions are dedicated FAD writers. Two of the EES positions also hold collateral duty for, respectively, managing intake of formal cases and coordinating the Alternative Dispute Resolution (ADR) mechanism.

3.3 Organizational Context

OCR operates in a highly complex organizational environment and must carefully manage its inter- and intra-agency relationships in order to successfully deliver its statutory and administrative responsibilities. These operating partnerships vary by frequency of interaction and level of authority. Effectively managing these relationships is integral to maintaining OCR's credibility and retaining the neutrality of EPA's civil rights programs.

By placing the OCR within the Office of the Administrator, EPA is well-positioned to achieve several efficiencies, including:

- **Executive Sponsorship** – the Administrator is eager to champion OCR's mission as she is directly held accountable for its success.
- **Organizational Alignment** – OCR can more easily coordinate EPA's Civil Rights programs and meet the Agency's changing priorities by ensuring its neutrality and reinforcing the importance of civil rights within the context of EPA's overall mission.

[13] Source: http://www.epa.gov/civilrights/crshome3.htm

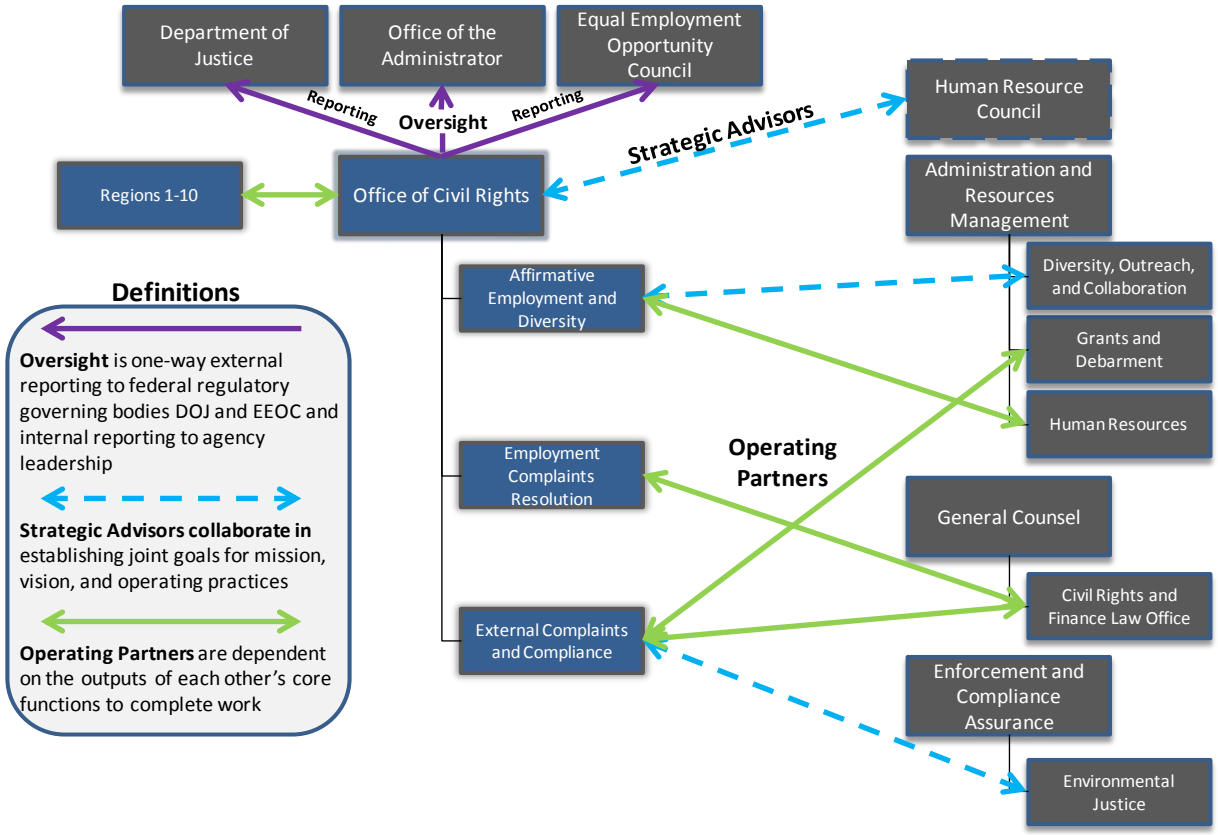
- **Oversight** – the Administrator's Chief of Staff and Deputy Chief of Staff regularly provide strategic direction to OCR and continuous feedback to the Administrator.
- **Visibility –** OCR's position in the Office of the Administrator enhances its visibility with program and regional leadership.

As illustrated in Figure 3-2, OCR must regularly interact with two outside oversight bodies, the EEOC and the U.S. Department of Justice (DOJ). EEOC and DOJ also provide training and procedural guidance to assist civil rights professionals to implement best practice programs and complete reporting requirements in a timely and accurate manner. EEOC and DOJ oversight is explained below:

Equal Employment Opportunity Commission (EEOC) – EEOC requires federal agencies to complete Management Directive 715 report (MD-715), which details the status of activities undertaken pursuant to its Affirmative Employment program under AED, and activities undertaken pursuant to its affirmative employment obligations under the Rehabilitation Act, Section 501. Additionally, agencies are required to complete the EEOC Form 462, which provides information on Federal equal employment opportunity complaints and ADR activities completed by the Title VII program.

Department of Justice (DOJ) – DOJ requests federal agencies to regularly report in regards to Executive Order 12250, which ensures the consistent and effective implementation of Title VI and other civil rights laws that prohibit discriminatory practices in Federal programs and programs receiving Federal financial assistance.

Figure 3-2. Internal and External EPA Civil Rights Reporting Relationships



Internally, OCR maintains operating partnerships with several EPA offices, including the Office of Human Resources (OHR), CRFLO (within the Office of General Counsel (OGC)), the Office of Grants and Debarment (OGD) and its network of field offices at the regions and laboratories; and OCR has an emerging relationship with the Office of Diversity, Outreach and Collaboration (ODOC) and strives to meet more regularly with Office of Environmental Justice (OEJ).

4 Current State Assessment

Deloitte Consulting (Deloitte) identified a reoccurring set of challenges that have impacted the ability of the Office of Civil Rights (OCR) to fulfill its mission:

- The OCR function has lacked stable leadership. While a new director has been appointed, [redacted] the organization's inability to fill subordinate leadership positions continues to be problematic.
- Management practices such as Standard Operating Procedures and operational goals are not well defined.
- OCR and the program offices have not established processes for collaborating to resolve civil rights and Equal Employment Opportunity Commission (EEOC) issues
- OCR staff lack the competencies and skills to get their job done effectively. Information systems support is also lacking.

The following sections discuss the challenges OCR faces. The first addresses organization- wide challenges. The other three address the OCR program offices (Title VI, Title VII and Affirmative Employment and Diversity (AED)). Within each section, we present our current state findings, benchmark practices from other federal agencies, and recommendations to implement corrective actions.

4.1 Organization-wide Challenges

Historically OCR's leadership had been relatively stable. However in a 16-month period, OCR lost four of its five top leaders [redacted]. Below is a summary of OCR Director, Deputy Director and Assistant Director tenure:

Name	Date Started	Date Left
Director		
[redacted]		
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Key Observations

- Focus has been on reactive, tactical complaint processing with limited effort to implement more proactive, preventative trend analysis and interventions
- 80% leadership attrition [redacted] in the last year
- Staff self report confusion on OCR mission
- Processes are non-standard and not repeatable
- Incomplete operating procedures and handbooks
- Lack of case management tracking system
- Internally supplied conflicting information on MD-715 and 462 report on Title VII FADs timeliness[14]
- Backlog in Title VI and VII cases
- Failure to meet MD-715 deadlines
- Lack of core competencies such as legal analysis

[14] "Summary of OCR Complaint Processing Issues 12-1-10to 1-3-11.doc)". 01/03/2011, 12:41 p.m. (Page 2-3)

[redacted]

Deputy Director

[redacted]

Assistant Directors

[redacted]

As a result of this leadership turnover, OCR has struggled to clarify its organizational vision and articulate its value and relevance to internal operating partners and employees, thereby compromising its credibility with external stakeholders. As such, the overall Agency has little confidence in OCR's programs ability to achieve its goals and objectives.

Without strong and consistent leadership and vision, OCR has drifted in focus and struggled to perform fundamental tasks. There has been a "seesaw" in emphasis between Title VI and VII programs, depending on which had the greatest backlog. Historically, this fire drill mentality has resulted in significant financial and reputational consequences for the Agency. For example, a Title VII case in 2000 led to a $600,000 settlement and resulted in the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (No FEAR), drawing attention to EPA's employment discrimination challenges. More recently in 2010, a Title VI infraction led to a settlement and publicized criticism that EPA is ineffective in managing its External Civil Rights caseload. At the same time, OCR's AED program has continually failed to meet its MD-715 reporting deadline for several years. In the 2010 462 report, the Title VII program had to report that when the complainant requested an immediate FAD, EPA delivered "none on time", and seven were delivered after an average of 282.43 days had passed. Where the complainant did not elect a hearing or a Final Agency Decision (FAD), the Environmental Protection Agency (EPA) issued one on time, and the remaining 13 after an average of 332.38 days had passed.[15]

These challenges, coupled with dwindling credibility, have inhibited OCR's ability to champion a culture of inclusion, fairness, and respect, values that are fundamental to its mission. Furthermore, the current leadership environment has to address low employee morale, isolated program activities, and ineffective or unclear direction or guidance to the field. As a result, several duplicative civil rights

[15] MD-715 - Inside EPA, Feb 19, 2010, "Personnel Disputes Roil EPA's Rights Office, Undermining Equity Agenda", "Summary of OCR Complaint Processing Issues 12-1-10 to 1-3-11.doc)". 01/03/2011, 12:41 p.m. (Page 2-3).

functions have emerged throughout EPA, outside of OCR.[16] In this environment, OCR staff struggle to perform fundamental tasks and creativity and innovation is stymied.

Management and Infrastructure

OCR has not been well-managed. Lack of clear expectations, governance, and processes has created an environment where employees are not provided the structure and guidance required for their roles. Furthermore, inadequate oversight has led OCR to operate as a silo without influence on the greater EPA organization.

At the time of the study in Fall 2010, OCR lacked a clearly articulated strategy to achieve its organizational goals and objectives. Roles and responsibilities lack strategic focus and basic understanding of the core set of tasks and, as a result, staff operates without clear guidance and managerial direction. Meaningful job descriptions, annual work plans, standard and repeatable processes, and performance monitoring and management are limited or altogether absent. While there was evidence of individual ad hoc initiatives to develop manuals, job aids, or performance plans, few were completed and implemented to sustain consistent performance.

Moreover, some staff are not given proper guidance on desired competencies and skills development. For example, the web-based skills survey indicated that less than half of OCR staff felt that EPA programs knowledge was very important to do their job and only 55% of leadership rated legislative awareness as critical/very important. Other civil rights organizations have a required competency for knowledge of Equal Employment Opportunity (EEO) law, regulations and policies[17]. If this EEO and program knowledge is not seen as valued, OCR may struggle to connect to the EPA mission and stay current on civil rights legislative mandates.

[redacted]

Inadequate infrastructure is an additional concern. OCR lacks documented processes and standard operating procedures necessary to sustain performance. Additionally, performance management programs and career paths have not been consistently developed and applied resulting in unclear performance feedback and career progression.

Collaboration

Finally, OCR has a heavy reliance on Office of General Counsel (OGC), Office of Human Resources (OHR) and other internal collaboration partners to complete its core tasks yet lacks mechanisms to secure necessary resources and support. For OCR to be successful, it needs to be seen as relevant and part of the Administrator's agenda.

There is concern that OCR may not have the same clout as other management initiatives raised by Associate/ Assistant Administrators, particularly with the Director in a non-political position, and therefore seen as less of a priority. However, there was equal concern that OCR would be subject to the political whims of each administration if the Director became a political appointee.

When asked about the Director reporting relationship, the nine benchmarking agencies were consistent in their recommendation to leverage the mandated direct reporting line to the head of the Agency to be

[16] See Section 3.3, Figure 3-6, for additional background on "Redundant" civil rights functions outside of OCR.

[17] National Institutes of Health Competency Model, Equal Employment Opportunity Specialist GS-260, Occupation Competency Model

the advocate and voice of civil rights. Each Civil Rights Director indicated they would use the direct access to personally voice concern to the head of the Agency if they felt civil rights were not being upheld. Therefore, the sanctity of this reporting relationship was emphasized as the part of the OCR stewardship during our interviews.

From 1993 to October 2010, OCR has received 247 Title VI complaints, according to the complaint tracking log provided to Deloitte. The tracking file notes the month and year the complaint is received and the month and year the complaint is accepted or closed. Only 6%, or 15 out of 247, were moved to either accepted or rejected within 1-month period, in alignment to the EPA targeted 20 day timeframe for acknowledgement. In fact, half of the complaints have taken one year or more to move to accepted or dismissed status[18].

The staff and management interviews indicated a core challenge with Title VI is the complexity of each case with complicated investigation plans often requiring health impact modeling as reflected in the investigation plan examples provided to Deloitte. The Title VI complaint backlog was directly attributable to OCR's difficulty in securing the time of the resources in the program and regional offices that have the required technical and regulatory expertise to execute the highly analytical investigation plan.

As of November 19, 2010 when Deloitte received the complaint log, there was an open case submitted in November 1994 with a status of Partial Informally Resolved. [redacted] has assisted in locating the appropriate expertise and securing support within EPA, but it may be difficult to sustain commitment to the complaint resolution process due to competing priorities.

Similarly, AED and Title VII need to coordinate diversity efforts with OHR to embed into Human Resources (HR) programs such as recruiting and promotions. Additionally, the newly formed Office of Diversity, Outreach and Collaboration (ODOC) also plays a role in advocating diversity. OCR, OHR and ODOC are in the process of aligning missions and plans.

Benchmark Approaches

Figure 4-1 compares a summary of Deloitte's key findings to example benchmark approaches from civil rights functions outside of EPA. Model civil rights offices ensure the relevancy to their organizations by integrating civil rights into the larger Agency strategy and goals. The majority of civil rights offices interviewed during the benchmark study participated in regular meetings as part of the top Agency leadership team to discuss civil rights as a mission critical function. This encourages active executive participation in addressing barriers and implementing remediation plans as well as supporting complaint timely resolution.

Figure 4-1. Summary Findings and Example Benchmark Approaches

Summary Findings	Benchmark Approaches
• **OCR staff have varying interpretations of the mission and vision**	• **U.S. Department of State** OCR mission, vision, values, and goals were designed and ratified by all State Department civil rights employees[19]
• **MD-715 is seen as an administrative task with**	• **National Institutes of Health** MD-715 is produced quarterly at the Institute and Center level and actions and progress reported at the Executive level[20].

[18] "Final OCR T6 Complaint Listing (10.15.2010).xls" received from Helena Wooden-Aguilar, Friday 11/19/2010 at 3:10 p.m.

[19] Copy is provided in Appendix A

disjointed process of collecting each element	
• **OCR does not have a cohesive leadership team regularly sharing insights into program and regions**	• **U.S. Department of Labor Civil Rights Center (CRC)** Title VI, Title VII, and AED program leads are a cohesive team that is able to articulate innovations and tools in all program areas, and share staff
• **EPA leadership lacks confidence in OCR program offices**	• **National Aeronautics and Space Administration (NASA) Office of Diversity and Equal Opportunity (ODEO)** Administrator champions diversity and oversees a strategic diversity partnership within NASA that involves top leadership across the agency in influencing and addressing diversity and inclusion. As a result, the Office of Diversity and Equal Opportunity can harness agency wide leadership support for initiatives and programs
• **OCR does not have a strategic plan or consistent performance tracking**	• **NASA** ODEO established a policy to incorporate specific and measurable diversity and inclusion metrics into SES, Managers, and Supervisors performance ratings
• **OCR, OHR, and OGC have not engaged in consistent discussion of formalized roles, responsibilities, and data sharing requirements**	• **U.S. Forest Service** OCR, Solicitor's office, and Human Resources collaborated to map processes from informal to formal complaints and integrated mapping into action plans
• **Work product quality is inconsistent and often rejected by partnering offices (e.g. OGC).**	• **U.S. Commission on Civil Rights** suggests agency head offices develop guidelines for mandatory quality assurance review procedures that require review at various stages of development, and uniformly track witness contact to ensure accountability

Recommendations

The following recommendations are intended to help address these organization-wide challenges:

- Develop the model OCR vision and strategy to more proactive, prevention mindset for civil rights protection.
- Emphasize complaint trend analysis and predictive modeling to pinpoint potential problem areas for early interventions.
- Increase the effort and expertise to develop and implement remediation strategies to reduce barriers and prevent complaints.
- Develop External Networked Team to include Title VI, Office of Environmental Justice (EJ), Office of Enforcement and Compliance Assessment (OECA), and Office of Research and Development (ORD) resources chaired by overall champion to aggressively resolve Title VI backlog, enhance compliance reviews and develop proactive guidance for recipients to reduce potential for complaints.

Develop a strategic roadmap to direct a complete overhaul of every OCR program area to align with model OCR and institute improvement management system. The roadmap should be coordinated by a senior leader, such as the Chief of Staff or Deputy Chief of Staff. By positioning the effort above OCR, it can create greater confidence that OCR has the Administrator level access to receive all the necessary support and is not trying to make all the improvements by itself.

[20] Sample Quarterly NIH MD-715 was not provided to Deloitte. EPA may need to request directly.

The Chief of Staff or Deputy Chief of Staff should formally launch the initiative and serve as an informal ombudsman to both OCR employees and the broader community of EPA and external stakeholders. This concerted effort will restore the trust and confidence in the Office of Civil Rights as well as indicate the significant priority the Administrator has placed on developing a model OCR. The Chief of Staff or Deputy Chief of Staff governs the overall initiative – through regular status meetings – and facilitates access to Agency executives to build consensus among internal partners (e.g., OHR, OGC) and to ensure new OCR work plans are aligned with Agency goals and strategy. The roadmap should overhaul management systems, redefine job roles, and realign staff, as illustrated in Figure 4-2 below.

Figure 4-2. Recommended Management and Resource-Related Improvements

Improve Management Systems	Redefine Job Roles and Realign Staff
1. Update Responsibility Assignment Matrix, or RACI charts, and develop Operating Level Agreements with key process partners to clarify roles, responsibilities, and interdependencies 2. Conduct an end-to-end process improvement program to update processes, embed quality control measures, and define performance measures for all core OCR functions 3. Formulate templates, checklists, handbooks (for new and rotating employees), and other job aids which are critical to empowering employees and ensuring consistent, repeatable processes	1. Define the roles and responsibilities, competencies, and performance elements for each position 2. Map current staff to newly defined roles according to Knowledge, Skills and Abilities (KSA) and career fit 3. Conduct skills gap analysis and plans to develop the employees 4. Provide necessary training and development to close gaps 5. Formulate career paths and implement formal employee performance coaching

Monitor performance to track progress and course correct. OCR will restore its credibility by improving performance (e.g., reduce backlog) and articulating its value and relevancy to EPA's goals and strategy through communications which are targeted to specific audiences and make practical sense in the day-to-day lives of EPA employees and other relevant stakeholders.

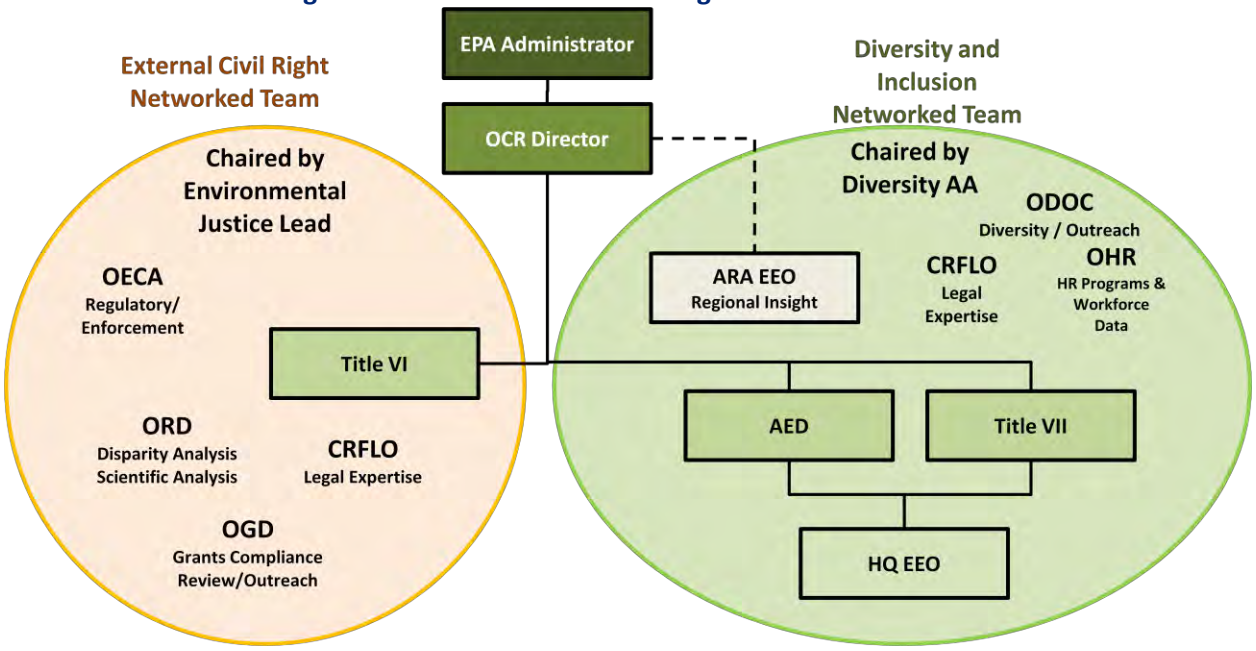
Make a few key changes to the organization of its civil rights functions

Like most federal agencies, EPA has multiple options for organizing the civil rights function and optimizing its ability to accomplish its mission. In order to determine the optimal organizational model for EPA, the Agency should consider the following organizational goals:

- Clarity on civil rights function;
- Dedicated focus on rebuilding and maintaining robust civil rights program;
- Greater influence on the programs and regions; and
- Agility to tap into ad hoc expertise to resolve complex Title VI complaints.

With these goals in mind, we recommend implementing a new OCR organizational structure as depicted in Figure 4-3.

Figure 4-3. Recommended OCR Organizational Structure



The diagram illustrates two "networked" teams. A networked team brings together people from different areas within EPA to work as a project team in accomplishing a set of specific goals but does not alter formal reporting relationships. The networked teams should have a Champion or Chair to lead and sponsor the effort. These teams should supplement, rather than supplant, the OCR organization. One focuses on internal diversity and inclusion and the other focuses on external community civil rights. Each network has a Champion to drive participation and address issues as they arise with his/her Associate/Assistant Administrator peer level.

In addition, Deloitte proposes a champion program to provide integration and coordination across collaboration partners for single point of accountability. The ODOC Associate Assistant Administrator can serve as the Diversity Champion. The Diversity Champion is goaled with action plans to address diversity barriers as identified in MD-715 and other internal EEO analyses. The Diversity Champion sponsors collaboration between OHR, ARA EEO, Affinity groups, Title VII and AED in developing remediation plans to address barriers. If team members are not fulfilling their role, the Diversity Champion can address with the respective Associate/Assistant Administrators for agreement on priority and time commitment. For example, MD-715 might indicate low advancement rates of Hispanic

engineers in region X. The Diversity Champion charters a diversity team of Region Lead, AED, Region X EEO, Region X SEPM, Hispanic Affinity group and OHR to identify underlying root cause and offer suggestions to address. The Diversity Champion holds Region X accountable for finalizing and executing the action plan, which gets monitored at senior management meetings. This championship model provides shared accountability for barrier analysis and remediation plans at the leadership level with an executive sponsor yet still provides the OCR Director with direct line escalation access to the Administrator if issues are too politically sensitive or not getting the adequate attention.

Similarly, Title VI would become part of External Civil Rights Networked Team under Environmental Justice (EJ) Champion linked with Office of Enforcement and Compliance Assurance (OECA), Office of Research and Development (ORD), Civil Rights and Finance Law Office (CRFLO), and Office of Grants and Debarment (OGD). By selecting the Champion from Office of Environmental Justice (OEJ), the External Team will align under the overall EJ mission of "fair treatment and meaningful involvement of all people regardless of race, color, national origin, or income with respect to the development, implementation, and enforcement of environmental laws, regulations and policies."[21] The EJ Champion would review with the OCR Director the Title VI complaint backlog to proactively work with the programs to resolve the complaints as well as take preventative measures based on case trend analysis (i.e., 55 percent of complaints related to public participation). This External Civil Right Networked Team works with DOJ in defining the framework for complaint investigations and compliance guidance.

For example, ORD coordinates the development of scientific analyses and overall benchmarking data such as average number of superfund sites within different minority neighborhoods as part of the disparate impact analysis. When a complaint comes in, Title VI is able to leverage ORD's benchmark/control group analytics for its investigation plan. OECA supplies the environmental program requirements for public participation, enforcement and permitting which Title VI layers on the civil rights requirements. Title VI provides the civil rights criteria and threshold while OECA determines the regulatory requirements under each program (i.e. public participation steps for Clean Air) with DOJ validating the overall approach. These guidelines can then be integrated into the grants management process, bolstering the current 4700 self assessment during the application phase as well as program evaluation which also considers civil rights requirements.

By allocating the Title VI work elements to the appropriate EPA organizations, this mitigates the current challenge of Title VI having the full spectrum of possible skills required to process highly complex complaints. Title VI supplies the civil rights expertise working with OECA/EJ to supply the environmental regulatory and analysis expertise. With a single EJ Champion, the different parts of the organization receive regular monitoring to ensure the cases are prioritized appropriately.

The Champion program addresses the concern that the non-political OCR Director is not on equal ground with the Associate/Assistant Administrators. With two champions supporting the main mission of external and internal compliance, they are able to support the Director in peer executive meetings. However, the OCR Director's direct access to the Administrator is maintained since the formal reporting relationship is preserved and the benefit of confidential sensitive discussions can take place. It is highly recommended that supporting linked performance goals and Standard Operating Procedures (SOPs) are developed to reflect the specialized teams in order to institutionalize these informal structures and

[21] http://www.epa.gov/environmentaljustice/basics/index.html

provide sustainability into future administrations subject to shifts in political appointee focus and preferences.

In this concept, the current Office of Civil Rights structure of the three program areas remains intact for dedicated focus on civil rights. However Title VII adds Headquarter (HQ) focused EEO Officer to handle HQ intake and complaint resolution and administer EEO programs. Over 32% of overall Title VII complaints are from Headquarters, warranting dedicated resource to proactive address and monitor EEO issues.

Further, the proposed model facilitates better coordination with the field**.** ARA EEO Officers have a dotted line relationship with the OCR Director yet remain solid line to the region to maintain position on regional management team. However OCR Director should be involved in selection, certifying, input and feedback on performance goals, and promotion consideration for ARA EEOs. Similarly, EEOs should provide input for Special Emphasis Program Managers (SEPM) within their region, often 20% collateral duties assignment. This structural matrix addresses the need to be embedded in the mission but yet provides venue for escalation and objective oversight.

Alternative changes to organization of its civil rights functions

The OECA Assistant Administrator (AA) can also be considered for the External Team Chair. As OECA's mission to "aggressively goes after pollution problems that make a difference in communities through vigorous civil and criminal enforcement…advance environmental justice by protecting vulnerable communities [22]", it will bring the enforcement prowess and expertise to adjudicate Title VI cases. OECA, through its main website, has also stated it is "resetting our relationship with states" which is a practice Department of Labor, Fair Housing Equal Opportunity and Federal Highways Transit Authority emphasized in their benchmark interviews. The advantage Deloitte sees with the OEJ Champion is the momentum from the White House in naming EPA as overall EJ Lead. However, given that OEJ sits within OECA, either the EJ lead or OCEA AA will bring the enforcement and environmental justice perspective as chair.

EPA can also consider moving Title VI function to OECA as part of overall enforcement. The advantage is the organizational legal competence required to assess cases and the outreach to the states and EPA programs. The disadvantage is the core knowledge and singular focus of civil rights law and regulations resident in OCR. Civil rights offices in other agencies expressed concerns about diluted access to resources, leadership attention if they were integrated into larger offices. This would be of concern as EPA embarks on transforming OCR into a model civil rights office.

Another option for Title VI is to fold the function into OGD as part of grants management. U.S. Department of the Interior's (DOI) Fish and Wildlife Services (FWS) administers Title VI within its grants management. However, FWS Title VI complaints tend to be related mostly to reasonable accommodations, which is much less complex than EPA's Title VI complaint portfolio.

[22] http://www.epa.gov/about epa/oeca.html

4.2 Title VI Program Management

Current State Findings

Administering the Title VI program for environmental regulation is highly complex and may require conducting technical analyses such as causal connection between these facially neutral procedures or practices, if there a disproportionate impact on the protected group and modeling for adverse health claims. This often requires Title VI to request support across EPA's scientific program offices, and OECA.

Key Observations

- 50% of Title VI cases took over 1 year to be accepted, versus EPA target 20 day turnaround
- 55 percent of the Title VI cases coming in to EPA's OCR are related to permitting, enforcement and public participation/involvement
- No tracking system to monitor investigations and complaints and lengthy case management timelines.
- EPA does not provide Title VI compliance guidance to recipients.
- OCR only conducts outreach and training for Title VI through web-based programs.
- Much needed expertise in program and regional offices has no incentive for prioritizing Title VI work

Due to this complexity, the Title VI program has struggled to develop a consistent framework to analyze complaints, resulting in a lengthy and time-consuming effort to evaluate the complaints and once accepted, to adequately investigate the cases. Only 6%, or 15 out of 247, were compliant with EPA targeted 20-day timeframe for acknowledgement. In fact, half of the complaints have taken one year or more to move to accepted or dismissed status. One case was accepted after nine years and a second case was accepted only after ten years.

Feedback from Title VI employees indicated that major delays result primarily from the complexity of determining whether cases fall within jurisdiction because there is little or no legal precedence for comparison. Investigations are further challenged by a lack of scientific methods to conduct needed analyses. [redacted] has assisted in locating the appropriate expertise and securing support but the overall complaint process is too often subject to competing priorities; mission related staff are in high-demand for mission related tasks.

The Title VI program office has taken steps, however, to improve its programmatic success by:

- Relocating the Title VI team to the main OCR office to increase contact with Headquarters Civil Rights, program and Agency executive offices;
- Developing draft Standard Operating Procedures (SOPs) for the investigative process and the compliance process; and
- Supporting training for environmental law proficiency of staff in the Title VI function.

Repeatable Complaints Process

Because each Title VI complaint often must be analyzed with the environmental science in addition to the civil rights regulations, EPA has not been able to develop a repeatable complaint resolution process and framework. As a result, OCR lacks finalized operational documents to govern the program's internal functions, or to communicate meaningful guidance to external stakeholders. Existing standard operating procedures, templates, and job aids are in draft format. Title VI also lacks meaningful compliance guidance for grant applicants. Title VI office has developed draft investigative report templates and outlines, as well as draft investigative procedures. When Deloitte inquired in November 2010 if Title VI complaints portfolio analysis had ever been done, the response was Title VI has not tried to group the complaints. The grouping of potentially related complaints can help determine if the scientific analysis

could address a series of like complaints as well as trigger broader Environmental Justice inquiry due to the emerging patterns.

OCR Title VI is just beginning to develop a network of environmental analysis technical expertise to bring together the right skill sets to investigate complaints. However, these resources are often overloaded with their own workload and may not be able to prioritize the complaint resolution in the timely manner required by OCR. The prolonged history of backlog has reinforced a persistent internal perception that EPA intentionally avoids making decisions in its Title VI program amongst OCR staff that further confirms unawareness on overall priority and urgency in Title VI function.

Staff Skills and Competencies

As mentioned in the Approach section, Deloitte administered a web-based job analysis. Responses indicate Title VI employees lack clarity regarding the technical skillset they require for their role. A high variability of answers points to a significant lack of common job role understanding. Furthermore, program staff's competencies are inconsistent and/or misaligned with the highly technical nature of complex Title VI complaints investigations.

The staff competencies required for EPA's Title VI program are unique to EPA in comparison to other Title VI programs due to the highly technical environmental law and policy requirements which are layered on traditional civil rights case law skills. Currently, Title VI staff competencies are largely process-based and many staff do not have the expected environmental policy or law background expected of their role, particularly necessary in completing the investigation plan as indicated in the template provided. Only 42% of the overall staff indicated knowledge of EPA programs to be important (breakdown by program office not available). For Title VI, each complaint must adhere to both civil rights requirements as well as each regulatory act (e.g. Clean Air).

Process Impediments

The highly technical nature of Title VI complaints requires investigative support from subject matter experts in EPA's programs and regions. Although the Title VI Program has started to build a supportive network of technical expertise for environmental analysis, the program and regions have little incentive to prioritize OCR support above their increasing workload. Deloitte identified only one example of successful deployment of intra-agency expertise. This example occurred in 1998 during an investigation of a Title VI case against Select Steel. This investigation concluded in a 'no finding' decision.

Deloitte noted that Final Agency Decisions (FADs) for Title VI has required EPA executives, including Chief of Staff and General Counsel, to meet on a regular basis for review and approval. While a lack of management systems and required expertise are partially the cause for the program's backlog, the necessity to mobilize an executive decision making committee including membership from the General Counsel and Chief of Staff may become a standard process. [redacted] was successful in mobilizing this executive body for several months and concluded fifteen cases from the extensive backlog this year.

The higher caseload volume and equally poor work quality from the Title VII program draws resources and attention from Title VI needs, further challenging its opportunities to devise and implement strategies to improve operational performance. [redacted] The Title VI collaboration has been augmented by a Special Assistant for Title VI who reports directly to the Administrator; however, the role is a temporary detail leaving a void of mentorship, reputational credibility, and access to Agency leaders once the term expires.

Compliance Review and Recipient Guidance

The only compliance review identified during the study is by the field-based EEO Officers in collecting and signing EPA's 4700-4 mandatory external civil rights compliance form required of all grant recipients. The 4700-4 is a self-assessment web-based form the grant applicants complete. Title VI staff expressed concern in the current practice of requesting their signature on the form without any interaction with the recipient and opportunity to verify the data supplied in the 4700-4. Deloitte was not able to find a management control system that flagged current plaintiffs charged with a Title VI compliant violation if they were to apply for additional grants. Federal Highway Administration has a similarly complex Title VI program with economic, environmental impact and adverse impact assessments. They have been able to develop an extensive recipient handbook that identifies potential issues and recommends actionable and measurable mitigation strategies to prevent complaints. EPA is not currently in a position to develop and communicate similar guidance to applicants and recipients.

Benchmark Approaches

Figure 4-4 compares the Deloitte's summary findings for the Title VI program to example benchmarked approaches from other U.S. government organizations.

Figure 4-4. Summary Findings and Example Benchmark Approaches

Summary Findings	Benchmark Approaches
• **EPA does not drive recipients to be Title VI compliant** • **EPA underutilizes field staff for pre-award and post-award compliance and there is no indication that the Office of Grants and Debarment (OGD) is integrated into the compliance process**	• **Federal Highway Administration (FHWA)** Title VI program has placed responsibility on the State Transportation Authority to develop proactive Title VI programs, conduct annual reviews, develop procedures for collecting statistical data, and annual reviews of special emphasis programming. • **U.S. Department of Housing and Urban Development (HUD)** processes over 10,000 external civil rights complaint cases annually. The regions handle the majority of cases and there is heavy reliance on external partners.
• **EPA has not finalized its operating tools and templates**	• **US Commission on Civil Rights** suggests federal agencies should develop management plans that include clear procedures, and classification system regarding case priority.
• **EPA has not conducted statistical analysis of higher incidence cases, committed to developing investigative procedures, or implemented preventive measures**	• **HUD's** Fair Housing and Equal Opportunity (FHEO) conducts a risk analysis using random sampling based on factors considered high risk to select entities for compliance review.
• **EPA has difficulty meeting timelines for complex cases with little or no legal precedence**	• **U.S. Department of Labor** The majority of OCR senior leadership staff had extensive experience (10 years or more) in civil rights functions, human resources/personnel management, or in an agency's Solicitor's General office providing expertise and leadership needed for complex cases.
• **Leadership requires further training in project management and effective staff supervision**	• **National Institute of Health (NIH)** Office of Equal Opportunity and Diversity Management (OEODM) requires Title VII staff to be trained in legal writing and legal analysis. EPA Title VI leadership could have a similar requirement.

Summary Findings	Benchmark Approaches
• **Staff competencies are inconsistent and/or**	• **NIH** OEODM has a detailed competency model outlines

misaligned with the highly technical nature of complex Title VI complaints investigations	skills required for Title VII work, and provides customized training curriculum for each employee. The competency model also serves as a basis for conversations regarding performance.
• **There is a lack of focus on long-term strategic resources that integrate ADR and trend analysis to proactively work with repeat offenders**	• **HUD** FHEO is upgrading its IT system, TEAPOTs, to perform predictive modeling to identify potential non-compliance, based on extensive available case data. Currently, the system is a real time web-accessible automated system used in the investigation and tracking of complaints and compliance reviews.
• **OCR only conducts outreach and training for Title VI through web-based programs**	• **U.S. Department of Labor** Civil Rights Center (CRC) Annual National Equal Opportunity Training Symposium educates recipients of Federal financial assistance about their nondiscrimination and equal opportunity responsibilities. • **Federal Highway Administration (FHWA)** OCR program specialists, civil rights specialists, and contracted investigators are provided with a Title VI desk reference book. Title VI funding recipients receive a handbook to assess their implementation, compliance, and enforcement efforts.
• **Much needed expertise in program and regional offices has no incentive for prioritizing Title VI work**	• **HUD** FHEO regional offices handle the majority of cases, and there is heavy reliance on external partners. Title VI intake, jurisdictional review, investigations, and decisions are all done at regional level.
• **Concluding Final Agency Decision (FADs) requires General Counsel and Chief of Staff input**	• **Department of Energy** OCR, General Counsel, and Human Resources have joint monthly meetings. The Office of General Counsel gets involved with cases during very early stages, but is not involved in FAD or managerial processes.
• **Strain from Title VII and AED issues reduces resources and attention from addressing Title VI challenges**	• **HUD** FHEO separates its external civil rights function from its internal civil rights function because the functions do not interact with one another, and have uniquely different relationships internally and externally.

Recommendations

As discussed in Section 4.1, the development of an improvement roadmap will address defining Title VI core functions and related staff development plans and corresponding SOPs and tools. Below are additional Title VI recommendations, based on the findings.

Define a framework to delineate the cross functional teams needed to respond. Building on the recommendation stated in the "Management" section of the report, Title VI should prioritize its management documentation according to highest priority or highest volume cases. Specifically, approximately 55 percent of cases originate from permitting, enforcement, and public participation, therefore, Title VI should concentrate its resources on developing standard, repeatable processes to address these types of cases. Title VI should work closely with DOJ to finalize processes and procedures. Additional stakeholders who should be consulted in developing SOPs including Civil Rights and Finance Law Office (CRFLO), Headquarters (HQ) and field-level OGD staff, subject matter experts from program areas, and the regional employees who maintain relationships with grantees. Coordinating stakeholders is needed to ensure uniformity across regional enforcement offices, particularly for high incidence complaints such as permits, enforcement, and public participation.

Clearly define guidance documents for funding grant recipients and establish formal Title VI compliance processes and procedures. Model agencies can seamlessly integrate a compliance program to help support and hold recipients accountable while also strategically addressing the use of federal funds.

Implement a formal information management system to track, analyze, and forecast important Title VI data. The system should be capable of prioritizing compliance data and complaints cases, escalate high risk issues, and analyze data as required to prevent and proactively address unnecessary exposure.

4.3 Affirmative Employment and Diversity (AED)

Current State Findings

OCR's AED program does not perform to the expectations of its mandated role, including the annual submission of the MD-715. Annual work plans include sections for structure goals, activities and persons responsible, timelines aligned to quarters, goals for recruitment, career development, and advancement of the employee groups. The document review indicated that content varied in breadth and depth. Interviews with program staff, EPA employees, and work plans revealed that AED primarily hosts special observance events – one event for each program area (e.g. Black History Month, etc.) – and compiles data required for the annual MD-715 report.[23] However, AED staff rely on contractors for barrier and trend analysis of underrepresented workforce populations with untimely data. The MD-715 report was not completed between 2006 and 2008. It is our understanding the 2010 MD-715 was submitted on time January 31, 2011.

Key Observations

- AED has difficulty accessing data from multiple sources for the MD-715.
- Tendency to complete responsibilities (e.g., MD-715) as last minute exercises
- MD-715 contractor analysis capabilities are underutilized and serve as a redundant function to AED staff. Data accuracy is frequently questioned.
- Redundancy in guidance and inconsistent direction provided to SEPMs.Content and timing of guidance to SEPMs not coordinated with EEO offices
- AED staff tend to have higher grade levels without unique KSAs or competencies typically required to justify high non-supervisory grade level.
- EPA staff lacks focus on staff training and customer service.
- Minimal collaboration with the Title VII program and little engagement with other EPA functions.
- No formal meetings, reporting relationships or operational guidelines to ensure consistency, strategic messaging, and resource allocation.
- Redundant OCR functions have developed outside the purview of OCR.

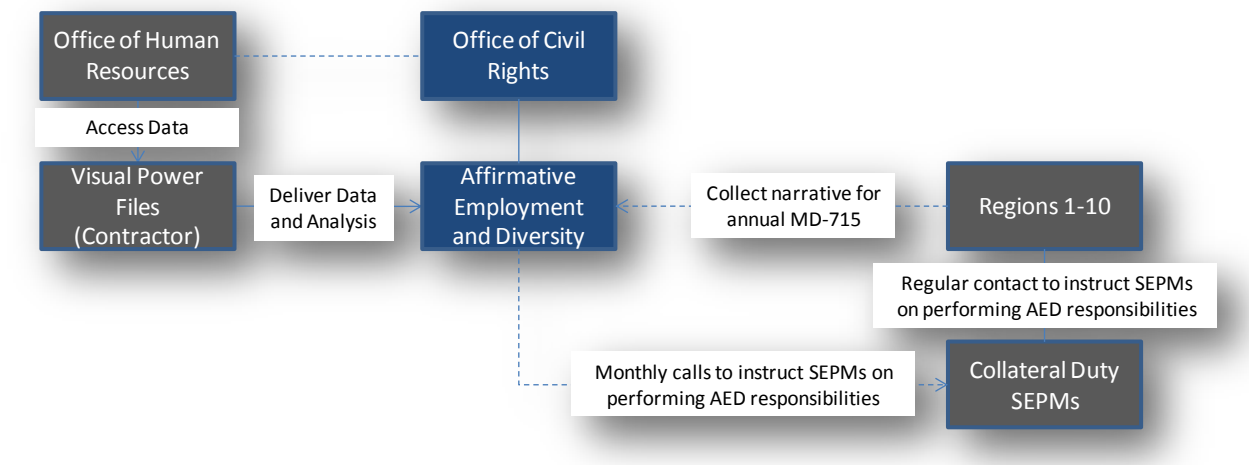
AED historically has requested narrative information for MD-715 from Program Management Officers (PMO), Human Resource Officers (HRO)s, and Equal Employment Opportunity (EEO) Officers with insufficient clarity (i.e., templates or examples of requested materials), resulting in incomplete and/or untimely submissions[24].

[23] Agencies are required to submit the MD-715 report annually by January 31.

[24] Based on interviews with PMOs and HROs requesting templates to ensure they are providing the correct type of narrative, ideally related to barriers identified.

Figure 4-5 depicts the workflow for compiling MD-715 data, including regional participation.

Figure 4-5. AED Interactions



Note the barrier analysis is not shared by AED with the regions yet they are asked to submit narrative for the annual report. [redacted]

Additionally, OHR and ODOC question the accuracy and validity of the numbers and analysis leading ODOC to begin developing its own dashboard tracking diversity workforce demographics based on the same HR database used by OCR for the MD-715 demographic analyses.

Alternatively, it appears the majority of AED's interactions involve coordinating national observance events (e.g. Women's History Month) with the Headquarters PMOs and the collateral duty Special Emphasis Program Managers (SEPM) located in the Headquarters, regions, and laboratories. The affirmative employment work plans vary in structure although generally include sections for goals, activities and persons responsible, and timelines aligned to quarters. The content also varied in breadth and depth, though generally included goals for recruitment, career development, and advancement of the employee groups to be conducted in concert with the SEPMs, EEO and OHR.

Collateral duty SEPMs located in the regions and EPA laboratories report to EEO Officers and receive direction from AED Headquarters. AED provides inconsistent centralized guidance and direction to EEO Officers as well as SEPMs. Furthermore, EEO Officers interviewed indicated that they are providing separate guidance and direction to SEPMs. SEPMs are tasked to spend 20 percent to AED functions; however, interviews indicated that SEPMs workload is disproportionate.

Staff Skills and Competencies

[redacted] AED has a staff of nine full-time time employees including a Director (GS-15), an Affirmative Employment Program Manager (GS-14) who serves as the custodian of the workforce data, and six Equal Employment Managers (GS-14 and GS-13) who are the lead representatives for their respective employment programs. AED has seven GS-14's and above, Title VI and Title VII each have only two GS-14's and above in their similarly sized offices. The Assistant Director and Disabilities Equal Employment Manager positions were vacant at the time of this report was completed.

[redacted] AED staff are not conducting analysis nor embedding results into on-going communications with program and regional managers and executives. Furthermore, there is no indication that barriers and trends or Equal Employment Opportunity Commission (EEOC) recommendations are proactively being identified and/or remedied.

As with other OCR program areas, there is a general lack of focus on defining a training curriculum and developing staff competencies. [redacted]

Collaboration Partners

Deloitte's assessment indicates that AED does not actively collaborate with other functions in OCR, and minimally partners with other EPA functions, including three program areas outside that support AED's mandate: Minority Academic Institutions (MAI) Program; White House Initiatives (WHI); and the Office of Diversity, Outreach, and Collaboration (ODOC). Several redundant functions now operate outside of OCR, as illustrated in Figure 4-6. Currently, no formal meetings, reporting relationships, and/or operational guidelines exist to ensure consistent and strategic messaging and resource allocation across these similar, yet separate functions.

Figure 4-6. Example Redundant OCR Functions Across EPA

Location	OCR Function	Finding	Redundancy
Office of Human Resources (OHR)	Targeted Recruitment	• AED is responsible for designing and coordinating targeted recruitment plans[25]. • Lack of coordination and outreach from AED has led to OHR designing and implementing their own targeted recruitment plans.	• OHR duplicates AED's responsibility for targeted recruitment
Office of Small Business Programs (OSBP)	Minority Academic Institutions	• AED is responsible for coordinating outreach and targeted recruitment, and cultivating mission-related relationships with Minority Academic Institution26 • [redacted]	• OSBP coordinates Minority Academic Institutions
Office of Diversity, Outreach and Collaboration (ODOC)	Diversity and Related Workforce Analysis	• AED is responsible for continually measuring and reporting disparities amongst protected classes of EPA's workforce • [redacted], ineffective use of contracting, and limited or no outreach to programs, regions, or EPA executives has left a void • ODOC conducts workforce analysis demographics (i.e., AED's barrier analysis) to be included in a executive dashboard for on-going diversity performance reporting	• ODOC duplicates AED's core responsibility for statistical analysis and reporting

Benchmark Approaches

Figure 4-7 compares the Deloitte's summary findings for the AED program to example benchmark approaches from other U.S. government organizations.

Figure 4-7. Summary Findings and Example Benchmark Approaches

Summary Findings	Benchmark Approaches
• **AED has outsourced its primary focus, MD-715, of which the data accuracy is frequently questioned** • **AED has difficulty accessing data from multiple sources for the MD-715** • **Tendency to complete responsibilities (e.g., MD-715) as last minute exercises**	• **NIH** OEODM uses quarterly briefings to Executive Offices, Institutes, and Centers to ensure accuracy of data and analysis needed for the MD-715 and staff accountability. • OEODM has direct access to HR databases for MD-715 that can drill down to 27 Institutes and Centers.
• **Redundancy in guidance and inconsistent direction provided to SEPMs** • **Content and timing of guidance to SEPMs not coordinated with EEO offices** • **AED uses a contractor to conduct periodic barrier analysis workshops for SEPMs** • **AED work plans varied in content and structure**	• **National Nuclear Security Administration** SEPMs are issued a comprehensive guide which includes the background and history of the federal program, SEPM roles and responsibilities, activity guidelines and detailed descriptions, guidance on purchasing requisitions, and an annual report of activities.

[25] Based on AED position description and sample workplans

Summary Findings	Benchmark Approaches
• **AED has a disproportionately higher grade levels yet does not require nor sponsor development plans for specialized knowledge, skills, abilities**	• **NIH** OEODM has a detailed competency model which they use to assess Title VII skills and provide customized training curriculum for each employee. The competency model also serves as a basis for conversations regarding performance
• [redacted]	• **NIH** OEODM staff training is available online. Staff can also request training outside of the agency if they can justify that it adds value to their core work and fits within the budget. Title VII staff is provided with online aids such as Cyberfeds, ELI training, and the EEOC Institute.
• **EPA OCR staff lacks focus on staff training and customer service**	• **U.S. Department of State** OCR FY11 Strategic Plan requests customer service training for staff in addition to a dedicated customer service staff role.
• **Minimal collaboration with the Title VII program and little engagement with other EPA functions**	• **U.S. Department of Labor** CRC Title VI, Title VII, and AED program leads are a cohesive team that is able to articulate innovations and tools in all program areas, and share staff.
• **No formal meetings, reporting relationships or operational guidelines to ensure consistency, strategic messaging, and resource allocation**	• **National Nuclear Security Administration's (NNSA)** EEO and Diversity Program Manager issued a comprehensive Special Emphasis Program Manager's guide. The guide includes background, roles and responsibilities of OCR and SEPMs, activity guidelines and descriptions, logistics guidance, sample materials, and annual report of activities.
• **Redundant functions exist outside the purview of OCR**	• **NIH** OEODM Director restructured the office to ensure that field officers report directly to the director, creating a centralized strategy and eliminating duplicate efforts.

Recommendations

As mentioned in Section 4.1, the improvement roadmap will address defining AED core functions and related staff development plans and corresponding SOPs and tools. Below are additional AED recommendations, based on the findings.

Emphasize AED's primary role in alleviating barriers and implementing remediation strategies and use the MD-715 as the focal point to guide all communications with stakeholders across the Agency, and with executives on a quarterly basis. AED is the public face of EPA's civil rights programs and should lead the development of outreach and training materials which further the cause of fairness, respect, and inclusion in the workplace.

Tactically, AED needs to develop a standard template for work plans which outlines its program of activities and links activities to their impact on identifying and reducing barriers. For example, AED should coordinate with EPA's various Affinity groups to understand their workplace challenges and research these challenges by reviewing data from Human Resource (HR) records (i.e., the number of employees promoted, trained, rewarded, etc.) from the Federal and EPA implemented Affirmative Employment programs.

AED should use this analysis as the basis for advising Affinity groups interested in hosting National Observance events to ensure the events focus on challenges for the employee population. National

Observance events should not be part of AED's program of activities; they should only communicate relevant barriers and recommend speakers, activities or other targeted measures to be included in events as a further means for addressing barriers.

AED should use SEPMs to implement barrier remediation strategies – such as training events, brownbag diversity discussion, town hall meetings, panels, workshops on barrier-related issues – and, as a means to collect additional qualitative data on workplace issues, validate the quantitative data AED uses in its annual MD-715 representation to EEOC. Additionally, Title VII complaints analysis should be included in the barrier analysis as well as assessing the preventative programs such as conflict management training and its subsequent impact on complaints for remediation consideration.

Hire, train, or realign staff that possesses a balance of barrier analysis expertise and experience with a strong passion for civil rights and diversity. Successful AED staff have a command of barrier analysis – both statistical analysis and remediation strategies – and have strong interpersonal skills capable of building persuasive arguments for fairness, respect, and inclusion with both the executive staff and line employees. AED should implement a formal curriculum to ensure all staff have a common understanding for key functions (i.e., barrier analysis, presentation skills, and executive communications) and phase out reliance on contractor support for core statistical analysis responsibilities.

Coordinate programming, guidance, and direction through its network of EEO Officers. AED should not circumvent field-based EEO Officers by providing input and direction to regional SEPMs, but rather leverage the existing network of EEO Officers as the focal point for all AED programming. EEO Officers translate the guidance and direction into specific measures unique to their local context and strengthen relationships with their network of SEPMs while reporting progress against barriers to AED for inclusion in the annual MD-715 report. Furthermore, a headquarters EEO Officer role should be established to coordinate AED functions across the employment programs. The Headquarters EEO Officer would act as the single point of contact for all AED programming, including the data collection and analysis for the annual MD-715 report, and eliminate the current tendency of AED staff to concentrate disproportionately on headquarters needs.

4.4 Title VII Program Management

Current State Findings

Analysis of interview records and Title VII program documentation pointed to a program lacking consistent, repeatable processes [redacted] and a resulting perception that the Title VII program's neutrality is at risk. CRFLO is involved in every stage of case processing which is the highest observed interaction between the CRFLO and OCR in comparison to benchmark agencies. EPA's law office currently provides a high level of editing, notations, and rejections of Title VII staff findings. While much of this is explained by a lack of competence and ineffective quality controls within the Title VII program itself, there remains a need to delineate roles and responsibilities between CRFLO and OCR to clarify who holds the ultimate decision making authority and avoid external scrutiny of the grey area between providing legal advice and performing responsibilities on behalf of OCR.

Key Observations

- Title VII guidelines do not include templates, supporting quick reference guides, or other job aids integral for implementing standard, repeatable processes.
- A formal performance measurement, reporting, and evaluation framework has not been institutionalized in the Title VII program.
- Performance monitoring systems for tracking settlement costs, types, and case durations are limited, inconsistent, and include errors and omissions.
- Staff have inconsistent skills and competencies, and lack formalized resources and managerial support.
- No established formal training curriculum and limited emphasis on performance coaching and staff development.
- [redacted]
- Title VII's heavy reliance on CRFLO threatens the program's neutrality and delays processing.
- Significant delays and quality control issues experienced in completion of several mandated reports.

The Title VII program focuses almost exclusively on meeting the one hundred and eighty day timeline for completing Final Agency Decisions (FADs). EEONet, the database used to track overdue cases, is being reviewed by OCR for the quality and accuracy of EEONet data and reports. Therefore the specific quantity and days past due of FADs are not reliable statistics. On January 3, 2011, Title VII management provided past due FADs data for this report, as a substitute for the EEONet figures.

Example: 462 Reports in 2010 Show Delays

- On December 13, 2010, when the 462 Report was submitted, 15 FADs were over 200 days overdue, 21 FADs were over 100 days overdue.
- As of the same date, one case was 630 days overdue and seven others with deadlines in December and January were not yet assigned.

Source: Title VII Special Assistant

One possible explanation for the delays is the minimal attention to quality when investigating cases, or more specifically, managing the work of contract EEO investigators.

The Investigative Reports (IRs) which conclude this stage of the process are routinely insufficient both in terms of legal research and analysis, questioning the complainant and other persons involved, and lack comprehensible, logical writing. The result is a heavier burden on FAD writers to address the routine shortcomings or rely on the Special Assistant and OCR leadership to provide support. Deloitte's assessment identified several shortcomings, including:

- IRs contain references to outdated anti-discrimination policies;

- Critical investigative records are absent, incomplete, or illegible;
- IRs lack reference to the Agency policy/guidelines involved in the complaint;
- Complete lack of comparative data, for example, by race, EEO activity, and disability; and
- Record of other instances where employees other than the complainant were denied/approved opportunities (e.g., training) and when such occurrences took place.

[redacted] has led to continuous intervention from OCR leadership and a process that embeds CRFLO into reviewing outputs at the conclusion of each stage of the investigative process. While CRFLO is independent from the Employment Law Division which represents EPA management, there are still perceptual risks when Office of General Counsel (OGC) is involved at such a granular level.

Performance Management and Guidance

EPA adheres to EEOC's "Management Directive 110: Federal Sector Complaint Processing Manual" and 29 C.F.R. Part 1614 as the standard operating procedures for implementing its formal complaints function and has adapted its own "EEO Investigator Guidelines". However, the guidelines do not include templates, supporting quick reference guides or other job aids integral for implementing standard, repeatable processes. As a remedial step, OCR appointed a Special Assistant for Title VII to implement quality controls – such as a "Quality Assurance Checklist for FADs" – and provide on-going subject matter expertise and performance coaching to assist the Assistant Director and Equal Employment Specialists (EES) staff in improving the quality and timeliness of outputs.

Performance monitoring systems for tracking settlement cost, type, case duration from open to close, and other aspects relevant to employment complaints, are limited and include errors and omissions. For instance, the settlement tracking workbook provided to the research team captured only the settlement fee and not associated attorney fees. Furthermore, the taxonomy of the classification system was non-standard and lacked unique identifiers between the descriptors of complaint sources. The tracking sheet provided to the team only listed cases settled and does not indicate what judgments were awarded by the courts. Available data suggests that only two million dollars in settlement costs were issued over the ten year tracking period, while the real cost to the Agency could be much greater when court ordered fees are accounted.

Management also does not track performance of EEO investigative contractors according to a performance checklist provided by the Title VII program. The program does not maintain records of supplemental investigations, nor attempt to determine whether these costs can be avoided in the future. Supplemental investigations are viewed as normal business practice and not associated with quality problems of contracted EEO investigators.[26] Furthermore, OCR management provided Deloitte

[26] Note: The number of supplemental investigations, while not known by program leadership specifically, was said to be two or similarly nominal.

with a summary of complaint processing issues that identified 18 quality issues spanning from one month's timeframe, requiring rework.[27]

Complaints Case Tracking System

Title VII lacks a formal complaints case tracking system. The study team learned that a system was purchased, but it was not evident at the time when or how the system would be implemented. The current approach to managing cases is largely paper-based and relies on the Assistant Director who reviews each new case and assigns to a case manager. During the three proceeding stages of case management: 1)Jurisdictional Review, 2) Investigation, and 3)Final Agency Decision – the document frequently changes hands between the case manager, CRFLO legal advisor, FAD writer, Special Assistant to Title VII, and the Assistant Director before proceeding to the Director of OCR for final signature. The handoffs are not recorded and there is no mechanism to capture comments for post mortem quality review; the current paper-based approach is inadequate for tracking and reporting case progress as it moves through the case management cycle and does not enable continuous process improvement.

Staff Skills and Competencies

Some staff members are consistently high performers, but others demonstrate a need for additional development. Staff roles have been compartmentalized into managing a stage of the complaints lifecycle such as Jurisdictional Review and Investigation, rather than owning a case from intake to close. This level of specialization should lead to standard, repeatable and quality controlled processes and yet work products lack attention to detail and exhibit the spectrum from easy to fix mistakes to incomplete IRs or acceptance of cases which do not meet legal sufficiency requirements for admittance into the formal complaints program. There is no evidence of a formalized learning and development curriculum. Furthermore, the majority of staff did not have routine performance coaching and career development discussions with supervisors. The results of Deloitte's web-based survey highlight that the lack of formal career development appears to be linked to low employee morale and workplace satisfaction.

Proactive and Preventative Program

As Title VII struggles in its basic complaint intake and processes, little emphasis has been given to greater use of Alternative Dispute Resolution (ADR) program or development of conflict management courses to facilitate difficult conversations between employee and management. Deloitte was not able to find evidence of complaint trend analysis to determine repeat offenders or incident anomalies to proactively conduct interventions. These types of programs focus on reducing the likelihood of complaints being generated rather than passively waiting for incidents to occur.

[27] Fentonmiller, Laura. "Summary of OCR Complaint Processing Issues 12-1-10 to 1-3-11.doc)". January 3, 2011. 12:41 PM. pp 2-3.

Benchmark Approaches

Figure 4-8 compares the Deloitte's summary findings for the Title VII program to example benchmark approaches from other U.S. government organizations.

Figure 4-8. Summary Findings and Example Benchmark Approaches

Summary Findings	Benchmark Approaches
• **Title VII guidelines do not include templates, supporting quick reference guides, or other job aids integral for implementing standard, repeatable processes**	• **Department of the Interior** OCR has a repository of past cases and templates for commonly occurring cases. Boiler plates have been developed for common processes and procedures.
• **A formal performance measurement, reporting, and evaluation framework has not been institutionalized in the Title VII program** • **Performance monitoring systems for tracking settlement costs, types, and case durations are limited, inconsistent, and include errors and omissions**[28]	• **The Department of the Interior and the National Institutes for Health** use iComplaints, a universal system for inputting and tracking complaints. The system also tracks staff pay and how long it takes staff to process the inputs of the system.
• **Staff have inconsistent skills and competencies, and lack formalized resources** [redacted]	• **NIH:** Title VII EEO specialists are all certified counselors and mediators, and are required to be trained in legal writing and legal analysis. • **NIH** staff training is available online. In addition, staff has access to training outside of the agency, and online aids such as Cyberfeds, ELI training, and the EEOC Institute.
• [redacted]	• The MOU between the United States Postal Service (**USPS)** and the **U.S. Department of Labor** allows the Department of Labor to use USPS investigations contractors to ease their procurement process, reduce costs, and share the burden for quality control.
• **Title VII's heavily reliance on CRFLO threatens the program's neutrality and delays processing**	• **Forest Service** OCR and General Counsel collaborated to design standard operating procedures for the EEO complaint process. The SOPs outline every step in the process, process owner, and process time breakdown. • **NASA** has an attorney assigned to the ODEO from the Solicitor General's office. The attorney is only asked to advise when there is an overload. The ODEO Associate Administrator has all final decision rights.
• **Significant delays and quality control issues experienced in completion of several mandated reports**	• **U.S. Commission on Civil Rights** suggests mandatory quality assurance review procedures. The guidelines should require review at various stages of development, and uniformly track witness contact so that investigators are held accountable for quality work.

Recommendations

As mentioned in Section 4.1, the improvement roadmap will address defining Title VII core functions and related staff development plans and corresponding SOPs and tools. Below are additional Title VII recommendations, based on the findings.

[28] Although OCR currently lacks a case management system, it has initiated the implementation of a system.

Enforce a performance management and quality assurance program. The Title VII program should institute a formal performance tracking program which defines specific targets for: timeliness; quality of writing; accuracy of legal research and analysis; and ability to effectively manage contract investigators, specifically to avoid unnecessary costs and rework. The performance tracking program should be preceded by an internal workshop on roles, responsibilities, and individual performance expectations which concludes with a commitment by staff to team and collaborate to take advantage of strengths where others have weaknesses and accept an 'as-one' approach to quality management.

Strengthen legal research and analysis skills. Title VII staff should have attorneys on staff to advise the Civil Rights Director on Title VII issues, and perform leadership roles for the office. The lawyers do not need litigation experience, but should be able to provide a deep understanding of Title VII and civil rights related laws, whether through experience, formal education, or a combination of both. Furthermore, this legal acumen will help Title VII program provide prompt, fair and impartial review, and adjudication of any allegation of discrimination.

Develop deep analytical and communication skills. OCR staff should have strong analytical, communication, and writing skills. The frequent interface with complainants and other parties necessitates competence in translating legal jargon into common language. Strong interpersonal skills should be emphasized. Additionally, Title VII staff should have the ability to or at least understand statistical analysis of case origin, issue, and other parameters to proactively identify hot spots of employment complaints and coordinate with the AED program to institute remedial actions, as feasible and appropriate.

Implement a case management tool to manage Title VII workload, track timeliness and results, and complete mandatory reporting. (Deloitte learned this is already underway.) The case management tool should incorporate access rights for each stakeholder involved in the process. Currently, field-based staff are left out of the case management process once they submit a case to Headquarters which turned from informal to formal status. It is important that EPA leverage technology as a vehicle to not only organize, streamline, and track operational performance, but also trigger alerts to inform stakeholders of outcomes which help civil rights colleagues and relevant parties learn from the decisions and outcomes resultant from case closure.

Strengthen the Alternative Dispute Resolution (ADR) mechanism and Conflict Management programs. Assess the statistical outcomes of discrimination complaint origins and issues and develop specific ADR and Conflict Management measures to proactively conduct outreach in high incidence regions and for high incidence issues. Coordinate implementation through EEO Officers in the field who participate in ADR and Conflict Management training and set specific goals for number of supervisors and line employees in high incidence areas trained. The program should be supplemented by specific Affirmative Employment programming from AED wherever the complaint trends indicate higher incidence within one employee thread (i.e. Hispanics, women, American Indians and Native Alaskans, etc.). The training and intervention program should be tracked to measure increased instances of informal complaints resolved through ADR instead of moving into the formal complaints process, as well as an overall reduction in total informal complaints lodged as a result of supervisors and line employees trained in Conflict Management skills and techniques. Executive sponsorship for the ADR and Conflict Management initiative should originate from the top of the Agency, for example, through messaging from the Administrator to relevant regional or program leaders acknowledging high incidences of discrimination complaints and championing the intervention program.

Assign high-performing field-level EEO Officers to part-time or full-time detail to provide a better source of skilled labor to reduce Title VII backlog. The OCR Director coordinates with regional administration to assign high performing EEO Officers to a part-time detail. The Title VII Assistant Director coordinates the assignment of workload according to greatest need, either at the Jurisdictional Review and Investigation stages, or the Final Agency Decision stage. EEO Officers avoid handling cases where there could be a conflict of interest, such as EEO cases originating from their regions. The addition of quality inputs contributes to reducing backlog and also reinforcing a sense of common purpose and shared responsibility between HQ and field-level EEO Officers. The EEO Officers also gain insight into the mechanics of the formal investigation process enhancing their ability to inform prospective complainants through real-life experience.

Document rules of engagement for collaborating with OGC staff to mitigate perceptions that neutrality is compromised by OGC involvement in the formal complaints management stages. Establish appropriate boundaries within OGC to protect OCR's neutrality and its use of firewalled CRFLO staff.

Restructure the Contract Investigations Function. Title VII should develop a more stringent standard for selecting and replacing contracted investigators, such as an approach for blocking underperforming contractors from reenlisting in EPA's investigative program. Title VII should also explore alternatives to its contract management program, by either in-sourcing or outsourcing the function. Given Title VII's inability to consistently meet their existing requirements, Deloitte recommends contracting with the USPS which has an established center of excellence for EEO contract investigators. The DOL uses the USPS contract investigative service and described as a benefit both cost reductions and ease of quality control.

5 Approach to Implementation

5.1 Implementation Plan

This Implementation Plan addresses the activities and milestones to put into operation the recommendations for each of the five areas discussed: 1) Leadership; 2) Management; 3) Title VI Program Management; 4) AED; and 5) Title VII Program Management. Given the urgency within the Agency to rapidly transform the Office of Civil Rights (OCR) function, Deloitte Consulting (Deloitte) developed an Implementation Plan assuming a start date of March 1, 2011 and end date of March, 2013. A Gantt chart illustrating tasks and timeline is on the following pages.

We realize that both the number of recommendations proposed, and subsequent effort, would require a tremendous amount of Agency resources and commitment to accomplish within a one year timeframe. Further constraining matters will be the likelihood of budget reductions that will make it more difficult for the Agency to implement all of our proposed recommendations within a short time. Given this likelihood, we have presented a sequence of activities that would have the most immediate impact. Therefore, the Environmental Protection Agency (EPA) can choose to stretch these recommendations over a two-year time table to better balance resources.

Our plan begins with recognizing that EPA must address its current deficiencies in leadership and workforce competencies. We propose a Stabilize Phase that will begin in March, 2011 and carry through to October, 2011. The intended purpose of this phase is to implement the recommendations that help fill OCR's leadership positions expeditiously with qualified, experienced and motivated senior civil rights professionals; develop and implement a plan that will fundamentally improve OCR's processes; and secure the right overall staff resources, including those who can carry out the fundamental pursuit of improving the specific Title VI program objectives.

We begin by addressing how OCR can overcome problems in the core process areas impeding its effectiveness. This includes determining how the OCR programs can better interact with other EPA offices. For example, OCR can establish a stronger relationship with ORD and OECA to better collect and analyze data that will proactively predict the likelihood of potential Title VI cases. These activities, which include a great deal of interaction and outreach with internal EPA stakeholders, will take approximately two months.

An equally important part of this Stabilize Phase is realignment and improvement of the core workforce to support OCR needs and Title VI extended network of resources. These activities will carry into late October 2011, including documenting all staff job roles and determining required skills, competencies and experiences for each role. With well-defined job roles, OCR can evaluate its current overall workforce against the requirements and identify gaps. Then, a comprehensive workforce plan will help OCR fill the gaps through a combination of new training programs and/or targeted staff hiring or alignment. It will also include the development of well-defined career paths and performance management processes.

The other critical aspect of this Stabilize Phase is addressing OCR's pressing need to expedite effective resolution of complex Title VI cases. This begins by helping OCR adopt a standard process to charter cross-functional investigative teams that bring together the right expertise to address each complaint. To catalyze these efforts, a senior leader in the Office of the Administrator should be identified as a "champion" to drive greater cooperation and collaboration between OCR, the program offices that possess unique technical expertise, and the field offices that understand the local context of individual complaints.

Upon the completion of the Stabilize Phase, it is recommended that OCR leadership set aside six weeks to conduct a long-term strategic planning session. This session will address a number of objectives, first and foremost being an assessment of its overall effectiveness. Also, it will give OCR leadership an opportunity to prioritize further improvements in the administering of the Title VI and Title VII programs and last, but not least, AED. Moreover, the group will review and refine the proposed organizational design recommendation. Once refined and approved, OCR will implement the new organizational structure.

Most importantly, the purpose of this session will be to determine how the OCR leadership, in concert with the EPA Administrator, will be able to institutionalize the current Title VI program objectives. This institutionalization will be designed to protect the Title VI program objectives from the shifting political priorities – especially those common as a result of changes in Administrations. The likely result of these planning sessions will be recommendations to draw upon existing environmental authorization legislation in order to fashion a legal basis for regulations that can further justify Title VI objectives.

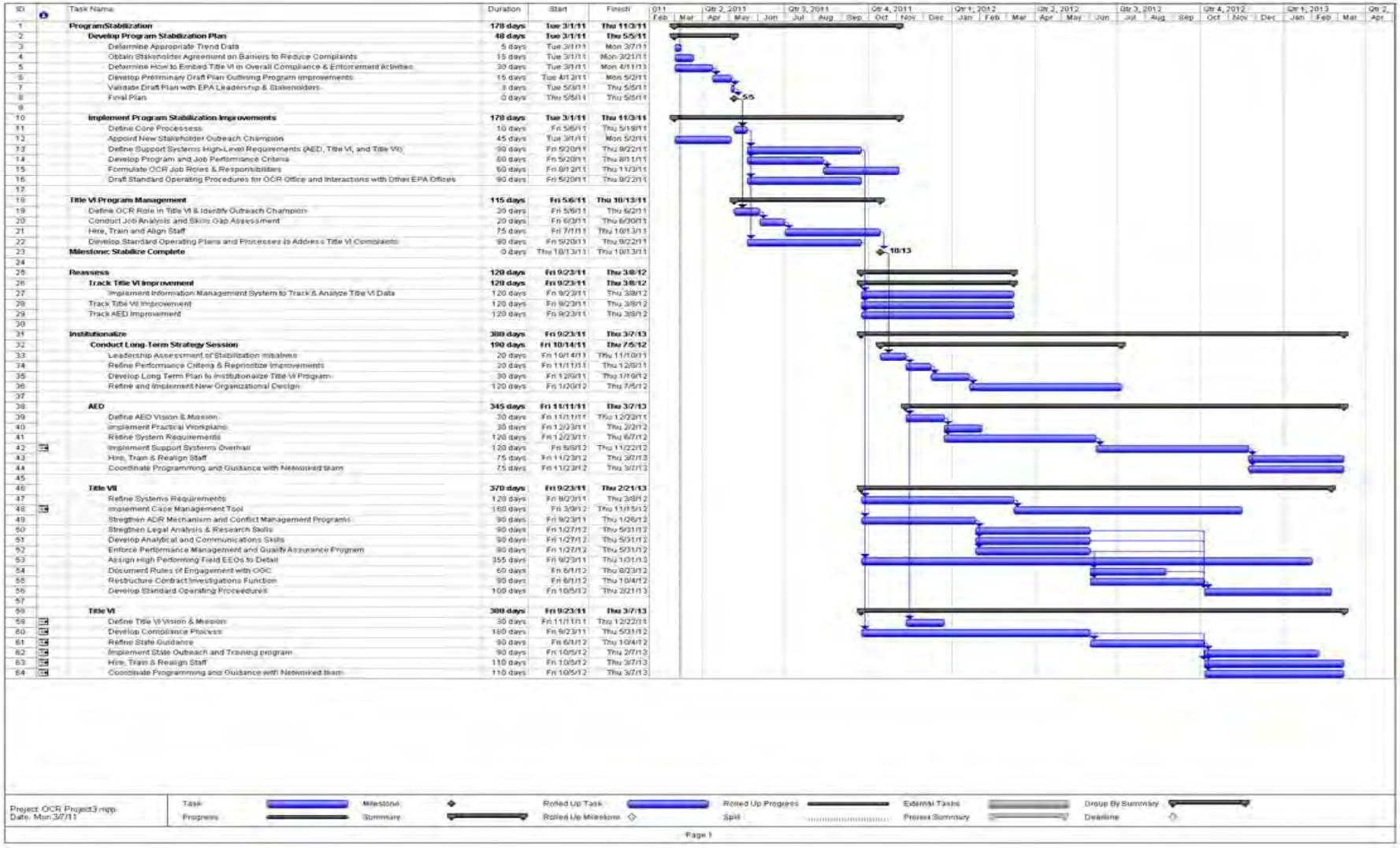
Should EPA have the resources, our Implementation Plan assumes the next series of transformation objectives will focus on process improvements in AED and Title VII, as well as improving the underlying support systems. Focusing on AED first, the majority of recommendations will be conducted beginning in November, 2011 and carry through to March 2013. The initial focus will be on developing practical work plans to improve its ability to coordinate affirmative employment across the Agency. In particular, these plans will focus on activities and outreach initiatives to improve inclusion and diversity in the workplace. This will also include better alignment and leveraging EEO Officers in the field to both promote Affirmative Employment and Diversity (AED) sponsored initiatives as well as improve their ability to gather information about potential barriers. Like the Title VI program, however, one of the most critical and time consuming activities will be staff development and/or realignment for Title VII and AED.

Title VII has the most recommendations in the Institutionalize Phase, as reflected in the project plan. Beginning in September 2011, the majority of Title VII efforts will focus on improving several key processes, including: strengthening the Alternative Dispute Resolution mechanism and conflict resolution programs; determining opportunities to improve staff legal research and analysis skills; and restructuring the Contracts Investigations function. We also recommend bringing experienced Equal Employment Opportunity (EEO) officials into the Title VII program to improve overall program interaction with regional offices. Once these process improvements are complete, they will be documented into a new set of Standard Operation Procedures (SOPs).

Finally, our recommendations discuss implementation of three major systems improvements, including predictive analytics to support Title VI, improved case management support for Title VII (which is already underway), and a general overall of the AED system. We have scheduled these systems improvements for the latter half of the overall effort as business requirements become clear. As discussed above, OCR has to focus on a number of critical process and human capital improvements at the outset, so there is no way to address these systems improvements earlier in the implementation plan. The risk, however, is that the plan calls for the systems improvements in AED, Title VI, Title VII to occur simultaneously. One systems upgrade, no matter how small, is a time and resource consuming initiative. Three upgrades in a near simultaneous schedule would be difficult to manage.

As such, we would believe that OCR should consider spacing these upgrades out over the course of 18-24 months so they can occur sequentially. This sequential systems development approach will also allow OCR to further refine the business and technical systems requirements, as well as explore additional technology alternatives both within the Agency and outside in order to determine the most cost-effective and least risky solutions.

Figure 5-1. Implementation Plan

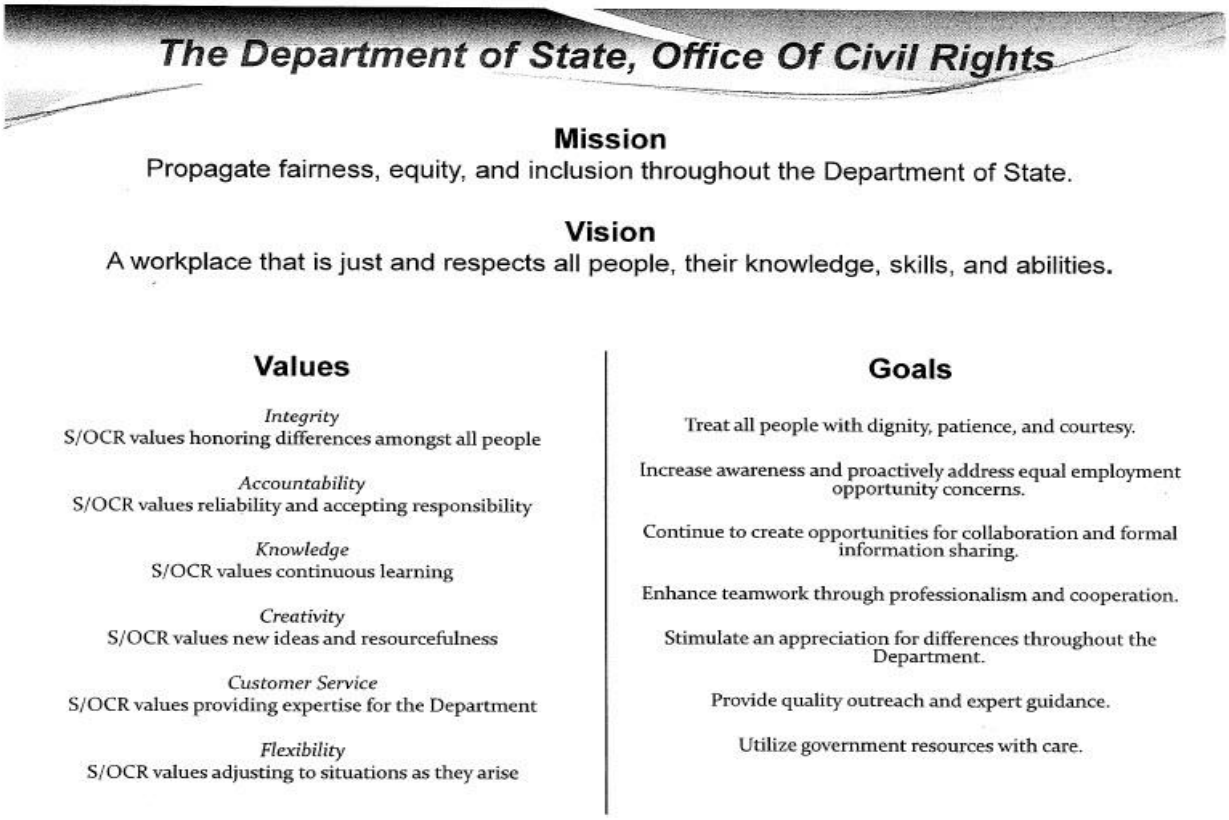


6 Appendices

6.1 Appendix A: Leading Practices Analysis

See enclosed PowerPoint presentation

Requested Department of State, Office of Civil Rights mission, vision, values and goals



The Department of State, Office Of Civil Rights

Mission

Propagate fairness, equity, and inclusion throughout the Department of State.

Vision

A workplace that is just and respects all people, their knowledge, skills, and abilities.

Values

Integrity
S/OCR values honoring differences amongst all people

Accountability
S/OCR values reliability and accepting responsibility

Knowledge
S/OCR values continuous learning

Creativity
S/OCR values new ideas and resourcefulness

Customer Service
S/OCR values providing expertise for the Department

Flexibility
S/OCR values adjusting to situations as they arise

Goals

Treat all people with dignity, patience, and courtesy.

Increase awareness and proactively address equal employment opportunity concerns.

Continue to create opportunities for collaboration and formal information sharing.

Enhance teamwork through professionalism and cooperation.

Stimulate an appreciation for differences throughout the Department.

Provide quality outreach and expert guidance.

Utilize government resources with care.

6.2 Appendix B: Case Studies/Additional Leading Practices

See enclosed PowerPoint presentation

6.3 Appendix C: Web-based Survey Results

See enclosed PowerPoint presentation

6.4 Appendix D: Title VI Complaints and Title VII Workload Analysis

See enclosed PowerPoint presentation

6.5 Appendix E: Information Sources

See enclosed PowerPoint presentation

6.6 Appendix F: Roles and Responsibilities

Strategic Advisors

The Human Resource Council (HRC) is a cadre of Senior Executive Service (SES) Environmental Protection Agency (EPA) employees who volunteer to provide strategic guidance and direction in setting future human resource goals and strategies. OCR provides periodic reports to the HRC regarding the Agency's demographic trends and high priority civil rights issues. The benefit of this relationship is access to SES staff overseeing both program and regional administration who can collaborate with the Office of Civil Rights (OCR) to link civil rights objectives to broader Agency goals. The HRC provides key operational insights to civil rights leadership and, vice versa, OCR receives important feedback regarding civil rights performance across EPA programs and regions.

The Office of Environmental Justice (OEJ) maintains an ad hoc reporting relationship with the External Complaints and Compliance (Title VI) program to provide an alternative venue for cases which do not fit within Title VI guidelines but could still be addressed by other EPA program offices. OEJ and the Title VI program also collaborate in developing briefing materials for the White House Initiative on Environmental Justice and to assess whether Title VI processes can be replicated for managing Environmental Justice cases.

The Office of Diversity, Outreach, and Collaboration (ODOC) is a newly established Associate Assistant Administrative level function whose role is to design a cross-cutting and strategic approach to diversity management. ODOC has developed a conceptual framework for an executive dashboard reporting workforce demographics which overlaps with the Affirmative Employment and Diversity's responsibilities. Cultivating this relationship could provide OCR with subject matter expertise and visibility into diversity management.

Operating Partners

The Civil Rights Law and Finance Office (CRFLO) provides legal expertise to assist both Title VI and employment complaints (predominantly Title VII) case managers with complex legal analysis. The relationship has expanded and contracted over the years and presently CRFLO provides quality assurance for documentation developed throughout the lifecycle of case management for both external (Title VI) and internal (Title VII) complaints. CRFLO is a dedicated resource for civil rights related cases and structurally separate from the Employment Law division which represents Agency management.

The Office of Human Resources (OHR) as well as its network of field staff, known as Human Resource Officers (HROs) is the primary partner for all EEO related civil rights programs – including those managed by the Affirmative Employment and Diversity (AED) and Employment Complaints Resolution programs. OHR and the HROs are stakeholders in capturing and reporting workforce data and ensuring affirmative employment and non-discrimination policies are integrated into EPA's talent management practices at Headquarters and with front-line managers at the field level.

The Office of Grants and Debarment (OGD) interfaces with the External Complaints and Compliance (Title VI) program to ensure all requests for federal funds include a pre-award declaration of compliance with federal non-discrimination requirements. OGD reports statistical data on grant applications which the Title VI program uses for ad hoc reporting to Agency leadership and biennial reporting to the Department of Justice. The Title VI program and OGD also coordinate changes to the database of organizations which have existing civil rights disputes or unresolved infractions and are barred from doing business with EPA.

Field offices at the regions and laboratories perform core civil rights responsibilities for AED, Title VI, and Title VII programs while also periodically interfacing with Headquarters OCR to communicate local civil rights challenges and accomplishments.

6.7 Appendix G: Abbreviations Glossary

AA: Associate/Assistant Administrator

ADR: Alternative Dispute Resolution

AED: Affirmative Employment and Diversity

ARA: Associate Regional Administrator

CRC: Civil Rights Center (Department of Labor)

CRFLO: Civil Rights and Finance Law Office

CRT: Complaints Resolution Team

DEQ: Department of Environmental Quality (State level)

DOJ: Department of Justice

DOL: Department of Labor

EEO: Equal Employment Opportunity

EEOC: Equal Employment Opportunity Commission

EES: Equal Employment Specialists

EPA: Environmental Protection Agency

FAD: Final Agency Decision

FHEO: Federal Housing and Equal Opportunity (HUD)

FHWA: Federal Highway Administration

HQ: Headquarters

HRO: Human Resources Officer

HUD: Department of Housing and Urban Development

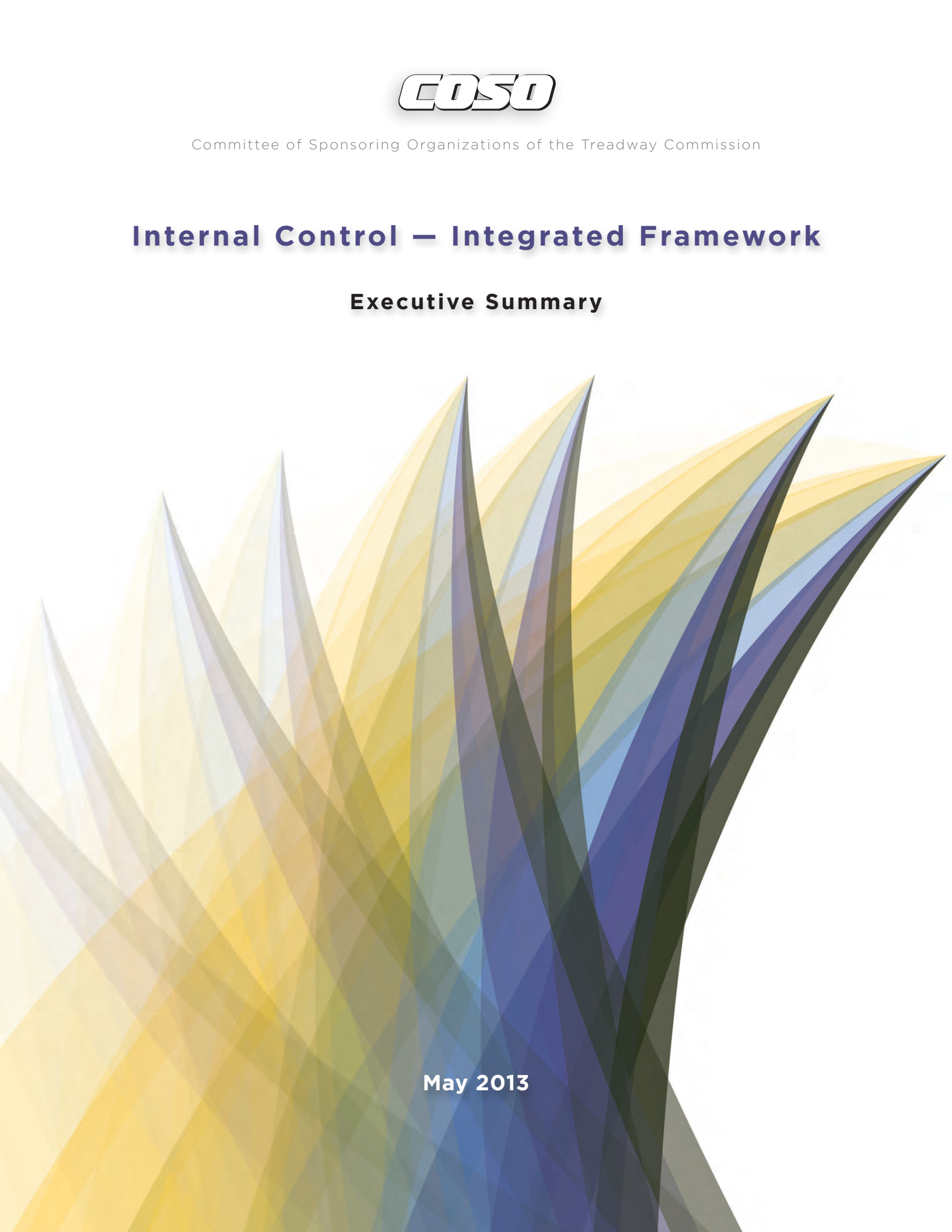
IR: Investigative Reports

KSA: Knowledge, Skills, and Abilities

MAI: Minority Academic Institution

MD-110: Management Directive Federal Sector Complaint Processing Manual

MD-715:	Management Directive EEO Reporting Requirements for Federal Agencies
MOU:	Memorandum of Understanding
NIH:	National Institutes of Health
OA:	Office of the Administrator
OCR:	Office of Civil Rights
ODEO:	Office of Diversity and Equal Opportunity (NASA)
ODOC:	Office of Diversity, Outreach, and Collaboration
OECA:	Office of Enforcement and Compliance Assurance
OEJ:	Office of Environmental Justice
OEODM:	Office of Equal Opportunity and Diversity Management (NIH)
OGC:	Office of General Counsel
OGD:	Office of Grants and Debarment
OHR:	Office of Human Resources
ORD:	Office of Research and Development
OSB:	Office of Small Business
PMO:	Program Management Officer
QA:	Quality Assurance
RA EEO:	Regional Administrator, Equal Employment Opportunity field office
RACI:	Responsibility Assignment Matrix
SEPM:	Special Emphasis Program Manager
SOO:	Statement of Objectives
SOP:	Standard Operating Procedure
USPS:	U.S. Postal Service
WHI:	White House Initiative



Committee of Sponsoring Organizations of the Treadway Commission

Internal Control — Integrated Framework

Executive Summary

May 2013

ISBN 978-1-93735-238-7

Committee of Sponsoring Organizations of the Treadway Commission

Internal Control — Integrated Framework

Executive Summary

May 2013

This project was commissioned by COSO, which is dedicated to providing thought leadership through the development of comprehensive frameworks and guidance on internal control, enterprise risk management, and fraud deterrence designed to improve organizational performance and oversight and to reduce the extent of fraud in organizations. COSO is a private sector initiative, jointly sponsored and funded by:

- American Accounting Association (AAA)
- American Institute of Certified Public Accountants (AICPA)
- Financial Executives International (FEI)
- Institute of Management Accountants (IMA)
- The Institute of Internal Auditors (IIA)

Committee of Sponsoring Organizations of the Treadway Commission

Board Members

David L. Landsittel
COSO Chair

Mark S. Beasley
Douglas F. Prawitt
American Accounting Association

Richard F. Chambers
The Institute of Internal Auditors

Charles E. Landes
American Institute of Certified Public Accountants

Marie N. Hollein
Financial Executives International

Sandra Richtermeyer
Jeffrey C. Thomson
Institute of Management Accountants

PwC—Author

Principal Contributors

Miles E.A. Everson
Engagement Leader
New York, USA

Stephen E. Soske
Project Lead Partner
Boston, USA

Frank J. Martens
Project Lead Director
Vancouver, Canada

Cara M. Beston
Partner
San Jose, USA

Charles E. Harris
Partner
Florham Park, USA

J. Aaron Garcia
Director
San Diego, USA

Catherine I. Jourdan
Director
Paris, France

Jay A. Posklensky
Director
Florham Park, USA

Sallie Jo Perraglia
Manager
New York, USA

Advisory Council

Sponsoring Organizations Representatives

Audrey A. Gramling
Bellarmine University
Fr. Raymond J. Treece Endowed Chair

Steven E. Jameson
Community Trust Bank
Executive Vice President and Chief Internal Audit & Risk Officer

J. Stephen McNally
Campbell Soup Company
Finance Director/Controller

Ray Purcell
Pfizer
Director of Financial Controls

William D. Schneider Sr.
AT&T
Director of Accounting

Members at Large

Jennifer Burns
Deloitte
Partner

James DeLoach
Protiviti
Managing Director

Trent Gazzaway
Grant Thornton
Partner

Cees Klumper
The Global Fund to Fight AIDS, Tuberculosis and Malaria
Chief Risk Officer

Thomas Montminy
PwC
Partner

Alan Paulus
Ernst & Young LLP
Partner

Thomas Ray
Baruch College

Dr. Larry E. Rittenberg
University of Wisconsin
Emeritus Professor of Accounting
Chair Emeritus COSO

Sharon Todd
KPMG
Partner

Kenneth L. Vander Wal
ISACA
International President 2011–2012

Regulatory Observers and Other Observers

James Dalkin
Government Accountability Office
Director in the Financial Management and Assurance Team

Harrison E. Greene Jr.
Federal Deposit Insurance Corporation
Assistant Chief Accountant

Christian Peo
Securities and Exchange Commission
Professional Accounting Fellow (Through June 2012)

Amy Steele
Securities and Exchange Commission
Associate Chief Accountant (Commencing July 2012)

Vincent Tophoff
International Federation of Accountants
Senior Technical Manager

Keith Wilson
Public Company Accounting Oversight Board
Deputy Chief Auditor

Foreword

In 1992 the Committee of Sponsoring Organizations of the Treadway Commission (COSO) released its *Internal Control—Integrated Framework* (the original framework). The original framework has gained broad acceptance and is widely used around the world. It is recognized as a leading framework for designing, implementing, and conducting internal control and assessing the effectiveness of internal control.

In the twenty years since the inception of the original framework, business and operating environments have changed dramatically, becoming increasingly complex, technologically driven, and global. At the same time, stakeholders are more engaged, seeking greater transparency and accountability for the integrity of systems of internal control that support business decisions and governance of the organization.

COSO is pleased to present the updated *Internal Control—Integrated Framework* (*Framework*). COSO believes the *Framework* will enable organizations to effectively and efficiently develop and maintain systems of internal control that can enhance the likelihood of achieving the entity's objectives and adapt to changes in the business and operating environments.

The experienced reader will find much that is familiar in the *Framework*, which builds on what has proven useful in the original version. It retains the core definition of internal control and the five components of internal control. The requirement to consider the five components to assess the effectiveness of a system of internal control remains unchanged fundamentally. Also, the *Framework* continues to emphasize the importance of management judgment in designing, implementing, and conducting internal control, and in assessing the effectiveness of a system of internal control.

At the same time, the *Framework* includes enhancements and clarifications that are intended to ease use and application. One of the more significant enhancements is the formalization of fundamental concepts that were introduced in the original framework. In the updated *Framework*, these concepts are now principles, which are associated with the five components, and which provide clarity for the user in designing and implementing systems of internal control and for understanding requirements for effective internal control.

The *Framework* has been enhanced by expanding the financial reporting category of objectives to include other important forms of reporting, such as non-financial and internal reporting. Also, the *Framework* reflects considerations of many changes in the business and operating environments over the past several decades, including:

- Expectations for governance oversight
- Globalization of markets and operations
- Changes and greater complexities of business
- Demands and complexities in laws, rules, regulations, and standards
- Expectations for competencies and accountabilities
- Use of, and reliance on, evolving technologies
- Expectations relating to preventing and detecting fraud

This *Executive Summary*, provides a high-level overview intended for the board of directors, chief executive officer, and other senior management. The *Framework and Appendices* publication sets out the *Framework*, defining internal control, describing requirements for effective internal control including components and relevant principles, and providing direction for all levels of management to use in designing, implementing, and conducting internal control and in assessing its effectiveness. Appendices within the *Framework and Appendices* provide additional reference, but are not considered a part of the *Framework*. The *Illustrative Tools for Assessing Effectiveness of a System of Internal Control*, provides templates and scenarios that may be useful in applying the *Framework*.

In addition to the *Framework*, *Internal Control over External Financial Reporting: A Compendium of Approaches and Examples* has been published concurrently to provide practical approaches and examples that illustrate how the components and principles set forth in the *Framework* can be applied in preparing external financial statements.

COSO previously issued *Guidance on Monitoring Internal Control Systems* to help organizations understand and apply monitoring activities within a system of internal control. While this guidance was prepared to assist in applying the original framework, COSO believes this guidance has similar applicability to the updated *Framework*.

COSO may, in the future, issue other documents to provide assistance in applying the *Framework*. However, neither the *Internal Control over External Financial Reporting: A Compendium of Approaches and Examples, Guidance on Monitoring Internal Control Systems*, nor any other past or future guidance takes precedence over the *Framework*.

Among other publications published by COSO is the *Enterprise Risk Management—Integrated Framework* (*ERM Framework*). The *ERM Framework* and the *Framework* are intended to be complementary, and neither supersedes the other. Yet, while these frameworks are distinct and provide a different focus, they do overlap. The *ERM Framework* encompasses internal control, with several portions of the text of the original *Internal Control–Integrated Framework* reproduced. Consequently, the *ERM Framework* remains viable and suitable for designing, implementing, conducting, and assessing enterprise risk management.

Finally, COSO would like to thank PwC and the Advisory Council for their contributions in developing the *Framework* and related documents. Their full consideration of input provided by many stakeholders and their insight were instrumental in ensuring that the core strengths of the original framework have been preserved, clarified, and strengthened.

David L. Landsittel
COSO Chair

Executive Summary

Internal control helps entities achieve important objectives and sustain and improve performance. COSO's *Internal Control—Integrated Framework (Framework)* enables organizations to effectively and efficiently develop systems of internal control that adapt to changing business and operating environments, mitigate risks to acceptable levels, and support sound decision making and governance of the organization.

Designing and implementing an effective system of internal control can be challenging; operating that system effectively and efficiently every day can be daunting. New and rapidly changing business models, greater use and dependence on technology, increasing regulatory requirements and scrutiny, globalization, and other challenges demand any system of internal control to be agile in adapting to changes in business, operating and regulatory environments.

An effective system of internal control demands more than rigorous adherence to policies and procedures: it requires the use of judgment. Management and boards of directors[1] use judgment to determine how much control is enough. Management and other personnel use judgment every day to select, develop, and deploy controls across the entity. Management and internal auditors, among other personnel, apply judgment as they monitor and assess the effectiveness of the system of internal control.

The *Framework* assists management, boards of directors, external stakeholders, and others interacting with the entity in their respective duties regarding internal control without being overly prescriptive. It does so by providing both understanding of what constitutes a system of internal control and insight into when internal control is being applied effectively.

For management and boards of directors, the *Framework* provides:

- A means to apply internal control to any type of entity, regardless of industry or legal structure, at the levels of entity, operating unit, or function
- A principles-based approach that provides flexibility and allows for judgment in designing, implementing, and conducting internal control—principles that can be applied at the entity, operating, and functional levels
- Requirements for an effective system of internal control by considering how components and principles are present and functioning and how components operate together
- A means to identify and analyze risks, and to develop and manage appropriate responses to risks within acceptable levels and with a greater focus on anti-fraud measures

1 The ***Framework*** uses the term "board of directors," which encompasses the governing body, including board, board of trustees, general partners, owner, or supervisory board.

- An opportunity to expand the application of internal control beyond financial reporting to other forms of reporting, operations, and compliance objectives
- An opportunity to eliminate ineffective, redundant, or inefficient controls that provide minimal value in reducing risks to the achievement of the entity's objectives

For external stakeholders of an entity and others that interact with the entity, application of this *Framework* provides:

- Greater confidence in the board of directors' oversight of internal control systems
- Greater confidence regarding the achievement of entity objectives
- Greater confidence in the organization's ability to identify, analyze, and respond to risk and changes in the business and operating environments
- Greater understanding of the requirement of an effective system of internal control
- Greater understanding that through the use of judgment, management may be able to eliminate ineffective, redundant, or inefficient controls

Internal control is not a serial process but a dynamic and integrated process. The *Framework* applies to all entities: large, mid-size, small, for-profit and not-for-profit, and government bodies. However, each organization may choose to implement internal control differently. For instance, a smaller entity's system of internal control may be less formal and less structured, yet still have effective internal control.

The remainder of this Executive Summary provides an overview of internal control, including a definition, categories of objective, description of the requisite components and associated principles, and requirement of an effective system of internal control. It also includes a discussion of limitations—the reasons why no system of internal control can be perfect. Finally, it offers considerations on how various parties may use the *Framework*.

Defining Internal Control

Internal control is defined as follows:

> *Internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.*

This definition reflects certain fundamental concepts. Internal control is:

- *Geared to the achievement of objectives* in one or more categories—operations, reporting, and compliance
- *A process* consisting of ongoing tasks and activities—a means to an end, not an end in itself
- *Effected by people*—not merely about policy and procedure manuals, systems, and forms, but about people and the actions they take at every level of an organization to affect internal control
- Able to *provide reasonable assurance*—but not absolute assurance, to an entity's senior management and board of directors
- *Adaptable to the entity structure*—flexible in application for the entire entity or for a particular subsidiary, division, operating unit, or business process

This definition is intentionally broad. It captures important concepts that are fundamental to how organizations design, implement, and conduct internal control, providing a basis for application across organizations that operate in different entity structures, industries, and geographic regions.

Objectives

The *Framework* provides for three categories of objectives, which allow organizations to focus on differing aspects of internal control:

- *Operations Objectives*—These pertain to effectiveness and efficiency of the entity's operations, including operational and financial performance goals, and safeguarding assets against loss.
- *Reporting Objectives*—These pertain to internal and external financial and non-financial reporting and may encompass reliability, timeliness, transparency, or other terms as set forth by regulators, recognized standard setters, or the entity's policies.
- *Compliance Objectives*—These pertain to adherence to laws and regulations to which the entity is subject.

Components of Internal Control

Internal control consists of five integrated components.

Control Environment

The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. The board of directors and senior management establish the tone at the top regarding the importance of internal control including expected standards of conduct. Management reinforces expectations at the various levels of the organization. The control environment comprises the integrity and ethical values of the organization; the parameters enabling the board of directors to carry out its governance oversight responsibilities; the organizational structure and assignment of authority and responsibility; the process for attracting, developing, and retaining competent individuals; and the rigor around performance measures, incentives, and rewards to drive accountability for performance. The resulting control environment has a pervasive impact on the overall system of internal control.

Risk Assessment

Every entity faces a variety of risks from external and internal sources. Risk is defined as the possibility that an event will occur and adversely affect the achievement of objectives. Risk assessment involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives. Risks to the achievement of these objectives from across the entity are considered relative to established risk tolerances. Thus, risk assessment forms the basis for determining how risks will be managed.

A precondition to risk assessment is the establishment of objectives, linked at different levels of the entity. Management specifies objectives within categories relating to operations, reporting, and compliance with sufficient clarity to be able to identify and analyze risks to those objectives. Management also considers the suitability of the objectives for the entity. Risk assessment also requires management to consider the impact of possible changes in the external environment and within its own business model that may render internal control ineffective.

Control Activities

Control activities are the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of the entity, at various stages within business processes, and over the technology environment. They may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews. Segregation of duties is typically built into the selection and development of control activities. Where segregation of duties is not practical, management selects and develops alternative control activities.

Information and Communication

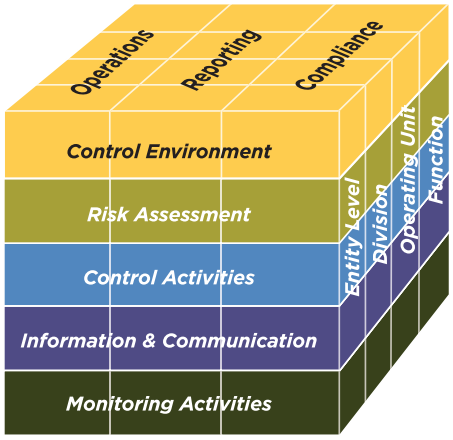
Information is necessary for the entity to carry out internal control responsibilities to support the achievement of its objectives. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of other components of internal control. Communication is the continual, iterative process of providing, sharing, and obtaining necessary information. Internal communication is the means by which information is disseminated throughout the organization, flowing up, down, and across the entity. It enables personnel to receive a clear message from senior management that control responsibilities must be taken seriously. External communication is twofold: it enables inbound communication of relevant external information, and it provides information to external parties in response to requirements and expectations.

Monitoring Activities

Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to effect the principles within each component, is present and functioning. Ongoing evaluations, built into business processes at different levels of the entity, provide timely information. Separate evaluations, conducted periodically, will vary in scope and frequency depending on assessment of risks, effectiveness of ongoing evaluations, and other management considerations. Findings are evaluated against criteria established by regulators, recognized standard-setting bodies or management and the board of directors, and deficiencies are communicated to management and the board of directors as appropriate.

Relationship of Objectives and Components

A direct relationship exists between *objectives*, which are what an entity strives to achieve, *components*, which represent what is required to achieve the objectives, and the *organizational structure* of the entity (the operating units, legal entities, and other). The relationship can be depicted in the form of a cube.



- The three categories of objectives—operations, reporting, and compliance—are represented by the columns.
- The five components are represented by the rows.
- An entity's organizational structure is represented by the third dimension.

Components and Principles

The *Framework* sets out seventeen principles representing the fundamental concepts associated with each component. Because these principles are drawn directly from the components, an entity can achieve effective internal control by applying all principles. All principles apply to operations, reporting, and compliance objectives. The principles supporting the components of internal control are listed below.

Control Environment

1. The organization[2] demonstrates a commitment to integrity and ethical values.
2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

2 For purposes of the *Framework*, the term "organization" is used to collectively capture the board, management, and other personnel, as reflected in the definition of internal control.

Risk Assessment

6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.

9. The organization identifies and assesses changes that could significantly impact the system of internal control.

Control Activities

10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

11. The organization selects and develops general control activities over technology to support the achievement of objectives.

12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

Information and Communication

13. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.

14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

15. The organization communicates with external parties regarding matters affecting the functioning of internal control.

Monitoring Activities

16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Effective Internal Control

The *Framework* sets forth the requirements for an effective system of internal control. An effective system provides reasonable assurance regarding achievement of an entity's objectives. An effective system of internal control reduces, to an acceptable level, the risk of not achieving an entity objective and may relate to one, two, or all three categories of objectives. It requires that:

- Each of the five components and relevant principles is present and functioning. "Present" refers to the determination that the components and relevant principles exist in the design and implementation of the system of internal control to achieve specified objectives. "Functioning" refers to the determination that the components and relevant principles continue to exist in the operations and conduct of the system of internal control to achieve specified objectives.
- The five components operate together in an integrated manner. "Operating together" refers to the determination that all five components collectively reduce, to an acceptable level, the risk of not achieving an objective. Components should not be considered discretely; instead, they operate together as an integrated system. Components are interdependent with a multitude of interrelationships and linkages among them, particularly the manner in which principles interact within and across components.

When a major deficiency exists with respect to the presence and functioning of a component or relevant principle, or with respect to the components operating together in an integrated manner, the organization cannot conclude that it has met the requirements for an effective system of internal control.

When a system of internal control is determined to be effective, senior management and the board of directors have reasonable assurance, relative to the application within the entity structure, that the organization:

- Achieves effective and efficient operations when external events are considered unlikely to have a significant impact on the achievement of objectives or where the organization can reasonably predict the nature and timing of external events and mitigate the impact to an acceptable level
- Understands the extent to which operations are managed effectively and efficiently when external events may have a significant impact on the achievement of objectives or where the organization can reasonably predict the nature and timing of external events and mitigate the impact to an acceptable level
- Prepares reports in conformity with applicable rules, regulations, and standards or with the entity's specified reporting objectives
- Complies with applicable laws, rules, regulations, and external standards

The *Framework* requires judgment in designing, implementing, and conducting internal control and assessing its effectiveness. The use of judgment, within the boundaries established by laws, rules, regulations, and standards, enhances management's ability to make better decisions about internal control, but cannot guarantee perfect outcomes.

Limitations

The *Framework* recognizes that while internal control provides reasonable assurance of achieving the entity's objectives, limitations do exist. Internal control cannot prevent bad judgment or decisions, or external events that can cause an organization to fail to achieve its operational goals. In other words, even an effective system of internal control can experience a failure. Limitations may result from the:

- Suitability of objectives established as a precondition to internal control
- Reality that human judgment in decision making can be faulty and subject to bias
- Breakdowns that can occur because of human failures such as simple errors
- Ability of management to override internal control
- Ability of management, other personnel, and/or third parties to circumvent controls through collusion
- External events beyond the organization's control

These limitations preclude the board and management from having absolute assurance of the achievement of the entity's objectives—that is, internal control provides reasonable but not absolute assurance. Notwithstanding these inherent limitations, management should be aware of them when selecting, developing, and deploying controls that minimize, to the extent practical, these limitations.

Using the *Internal Control—Integrated Framework*

How this report can be used depends on the roles of the interested parties:

- *The Board of Directors*—The board should discuss with senior management the state of the entity's system of internal control and provide oversight as needed. Senior management is accountable for internal control and to the board of directors, and the board needs to establish its policies and expectations of how members should provide oversight of the entity's internal control. The board should be apprised of the risks to the achievement of the entity's objectives, the assessments of internal control deficiencies, the management actions deployed to mitigate such risks and deficiencies, and how management assesses the effectiveness of the entity's system of internal control. The board should challenge management and ask the tough questions, as necessary, and seek input and support from internal auditors, external auditors, and others. Sub-committees of the board often can assist the board by addressing some of these oversight activities.
- *Senior Management*—Senior management should assess the entity's system of internal control in relation to the *Framework*, focusing on how the organization applies the seventeen principles in support of the components of internal control. Where management has applied the 1992 edition of the framework, it should first review the updates made to this version (as noted in Appendix F of the *Framework*), and consider implications of those updates to the entity's

system of internal control. Management may consider using the *Illustrative Tools* as part of this initial comparison and as an ongoing evaluation of the overall effectiveness of the entity's system of internal control.

- *Other Management and Personnel*—Managers and other personnel should review the changes made to this version and assess implications of those changes on the entity's system of internal control. In addition, they should consider how they are conducting their responsibilities in light of the *Framework* and discuss with more senior personnel ideas for strengthening internal control. More specifically, they should consider how existing controls affect the relevant principles within the five components of internal control.
- *Internal Auditors*—Internal auditors should review their internal audit plans and how they applied the 1992 edition of the framework. Internal auditors also should review in detail the changes made to this version and consider possible implications of those changes on audit plans, evaluations, and any reporting on the entity's system of internal control.
- *Independent Auditors*—In some jurisdictions, an independant auditor is engaged to audit or examine the effectiveness of the client's internal control over financial reporting in addition to auditing the entity's financial statements. Auditors can assess the entity's system of internal control in relation to the *Framework*, focusing on how the organization has selected, developed, and deployed controls that affect the principles within the components of internal control. Auditors, similar to management, may use the *Illustrative Tools* as part of this evaluation of the overall effectiveness of the entity's system of internal control.
- *Other Professional Organizations*—Other professional organizations providing guidance on operations, reporting, and compliance may consider their standards and guidance in comparison to the *Framework*. To the extent diversity in concepts and terminology is eliminated, all parties benefit.
- *Educators*—With the presumption that the *Framework* attains broad acceptance, its concepts and terms should find their way into university curricula.

Black's Law Dictionary (9th ed. 2009), **disparate treatment**

DISPARATE TREATMENT

disparate treatment. The practice, esp. in employment, of intentionally dealing with persons differently because of their race, sex, national origin, age, or disability. • To succeed on a **disparate**-**treatment** claim, the plaintiff must prove that the defendant acted with discriminatory intent or motive. [Cases: Civil Rights 1033, 1138.]

"Claims brought on behalf of a group of employees come in two varieties: claims of intentional discrimination (or **disparate treatment**) and claims of discriminatory impact (or **disparate** impact). The difference between these types of claims is significant, so much so that constitutional law only recognizes claims of **disparate treatment**, not **disparate** impact. Yet these two kinds of claims resemble one another, especially in the statistical evidence that the plaintiff must present in order to establish liability.... [C]lass claims of **disparate treatment** emphasize the historical perspective and its negative conception of equality as colorblindness, while class claims of **disparate** impact emphasize the remedial perspective and its goal of eliminating the effects of past discrimination." George Rutherglen, *Employment Discrimination Law* 56 (2001).

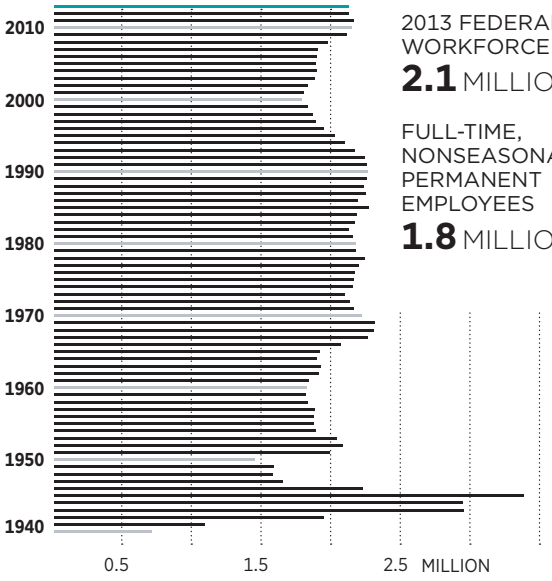
Bryan A. Garner, Editor in Chief

FED FIGURES 2014

Federal Departures

On the heels of budget cuts, pay freezes and hiring slow-downs, more than 114,000 people left the federal government in 2013, mostly through retirements. Additionally, the number of employees who voluntarily resigned from federal service increased every year since 2009. With the steady turnover, it is imperative for federal leaders to closely examine who they are losing and assess their short- and long-term needs. Who did government lose in 2013? Which agencies had the highest attrition rates and are people in specific occupations leaving at higher rates? To address these questions, the Partnership for Public Service analyzed recent separations data for full-time, nonseasonal, permanent civilian employees who left the federal government in fiscal 2013 in executive branch agencies, excluding the U.S. Postal Service.

SIZE OF THE FEDERAL WORKFORCE



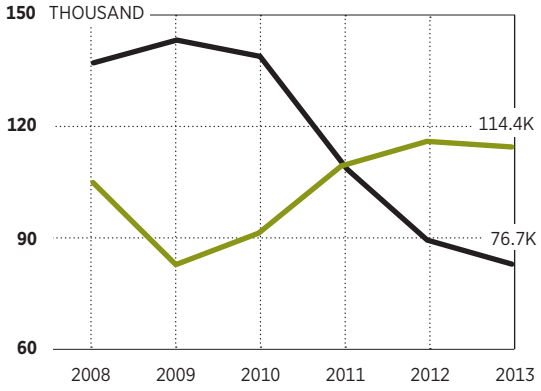
2013 FEDERAL WORKFORCE
2.1 MILLION

FULL-TIME, NONSEASONAL, PERMANENT EMPLOYEES
1.8 MILLION

RECENT HIRING AND DEPARTURES TRENDS

DEPARTURES
NEW HIRES

The number of employees annually leaving the federal government increased from a low of 83,317 in 2009 to 115,661 in 2012 and leveled off at 114,354 in 2013. At the same time, the number of new employees hired by the government declined every year since 2009.



TOTAL GOVERNMENT-WIDE DEPARTURES IN 2013
114,354

PERCENT OF THE TOTAL FEDERAL WORKFORCE
6.2%

PERCENT INCREASE IN DEPARTURES SINCE 2009
37.3%

RECENT DEPARTURE TRENDS BY FISCAL YEAR

RETIREMENT: Separation entitling employee to withdraw from retirement fund.

RESIGNATION: Voluntarily leaving one's position.

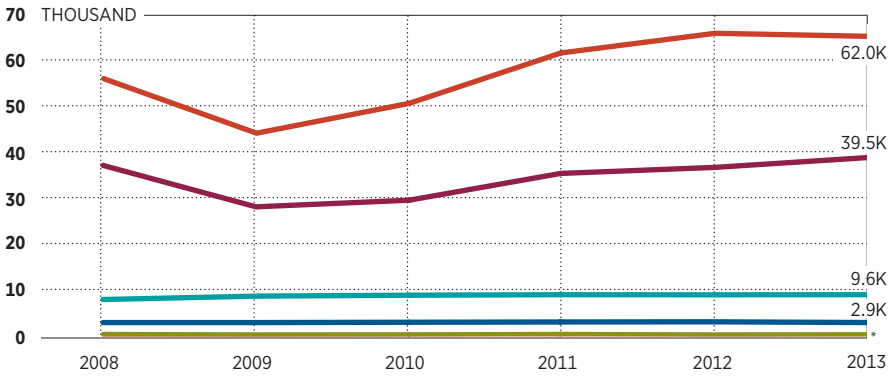
TERMINATION OR REMOVAL: Employee dismissal either based on misconduct, unsatisfactory performance or an expiration of appointment, work or funds.

REDUCTION IN FORCE (RIF): Separation resulting from lack of funds or elimination of position or agency.

OTHER SEPARATION: Departures that include resignations in lieu of termination and other agency-specific separations.

DEATH

Federal employees leave government service for a variety of reasons, including resignations, retirements, reductions in force, terminations or removal, and death. Retirements made up the largest classification of departures, accounting for 54.2 percent or 61,953 of all separations from federal service in 2013, while employees who resigned made up 34.5 percent of those who left.



*In 2013, there were 409 RIFs and 47 other separations.

TOP 10 OCCUPATIONAL GROUPS FOR FEDERAL DEPARTURES

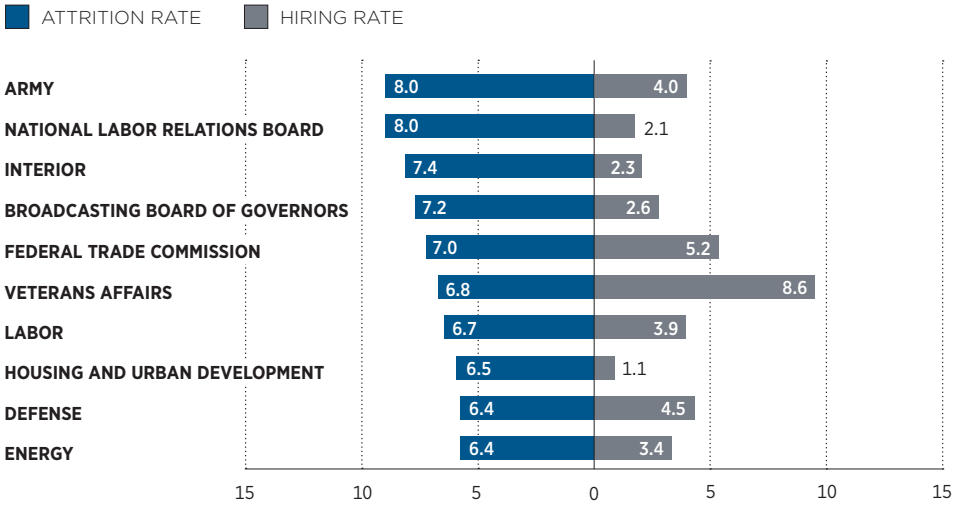
	ADMINISTRATION, OPERATIONS AND GENERAL MGMT.	MEDICAL, DENTAL AND PUBLIC HEALTH	INVESTIGATION AND INSPECTION	ACCOUNTING AND BUDGET
PERCENT OF DEPARTURES	**16.4**%	**15.2**%	**7.4**%	**5.7**%
EXITING EMPLOYEES IN **2013**	18,733	17,361	8,507	6,547
EXITING EMPLOYEES IN **2012**	20,429	15,923	7,993	7,207

A profile of recent federal departures

As government continues to lose more employees than it brings on board each year, who are we losing from federal service? The following pages offer a demographic profile of those employees who left in fiscal 2013 (October 1, 2012 through September 30, 2013). For years of service and veteran status, the most recent data available for departures was from fiscal 2012.

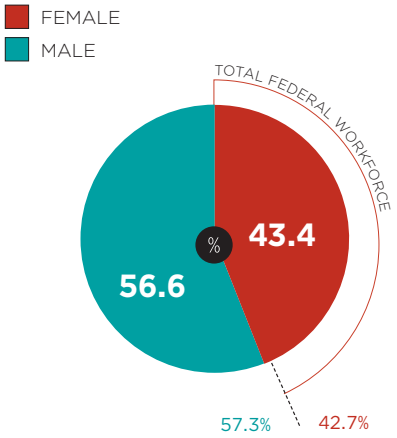
AGENCY ATTRITION RATES VERSUS AGENCY HIRING RATES

Attrition rates are calculated by dividing the number of departures throughout the fiscal year by the size of the workforce at the end of that fiscal year. Of all mid-size and large agencies—those with 1,000 or more employees—the Department of the Army and the National Labor Relations Board had the highest attrition rates during fiscal 2013. This is juxtaposed with agency hiring rates, which we calculated by dividing the number of hires throughout the fiscal year by the size of the workforce at the end of that fiscal year. The government-wide average attrition rate was 6.2 percent.



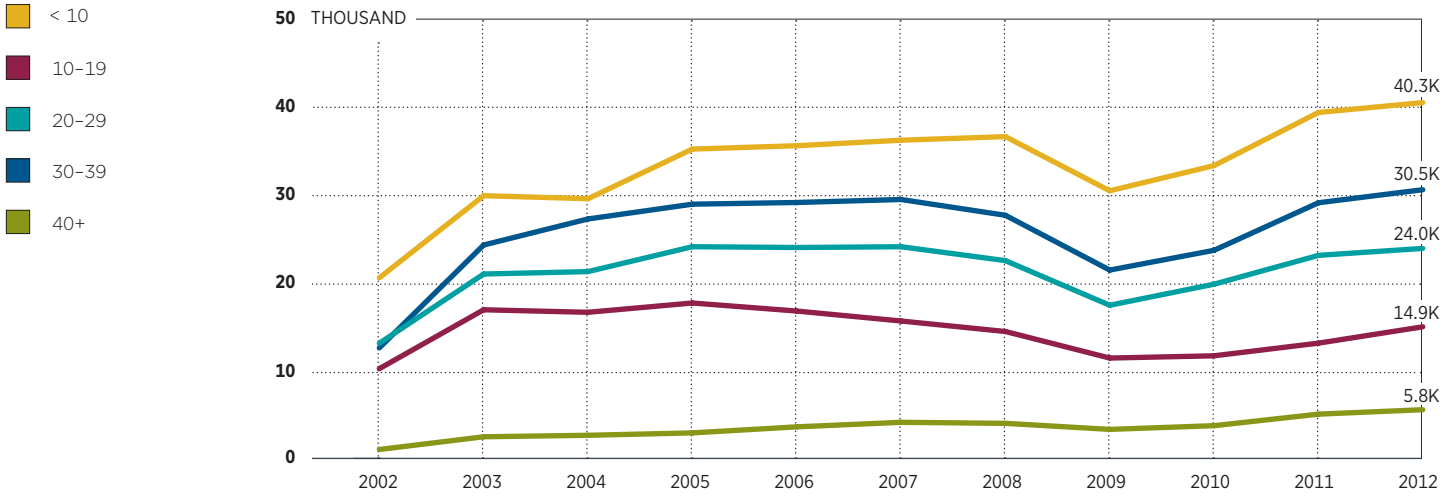
GENDER

Women accounted for 43.4 percent of all separations from federal service during fiscal 2013. This number closely mirrors the current makeup of the federal workforce, where 42.7 percent of federal employees in 2013 were women. This, along with recent hiring trends, continues to reinforce the gender gap between men and women in the federal workforce.



YEARS OF SERVICE

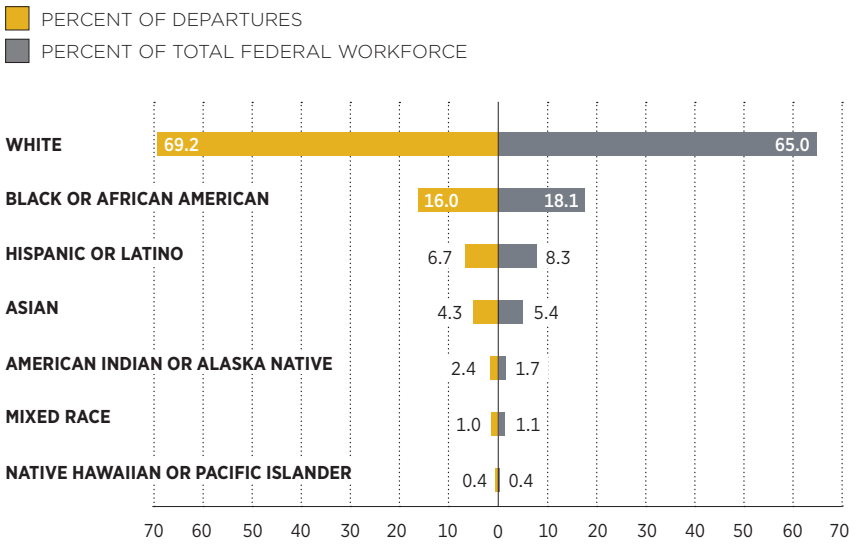
Those who served for fewer than 10 years made up the largest number of employees who left federal service every year from 2002 to 2012, accounting for approximately one-third of the departures during this time. Years of service refers to the number of years of federal civilian employment, including creditable military service. Complete departures data for years of service was not available for 2013.



ENGINEERING AND ARCHITECTURE	BUSINESS AND COMMERCE	OTHER OCCUPATIONS*	LEGAL AND CLAIMS SERVICES	SOCIAL SCIENCES AND PSYCHOLOGY	INFORMATION TECHNOLOGY
5.7%	**4.9%**	**4.7%**	**4.6%**	**4.1%**	**3.8%**
6,532	5,640	5,330	5,215	4,681	4,303
6,218	6,696	5,334	5,098	4,604	4,304

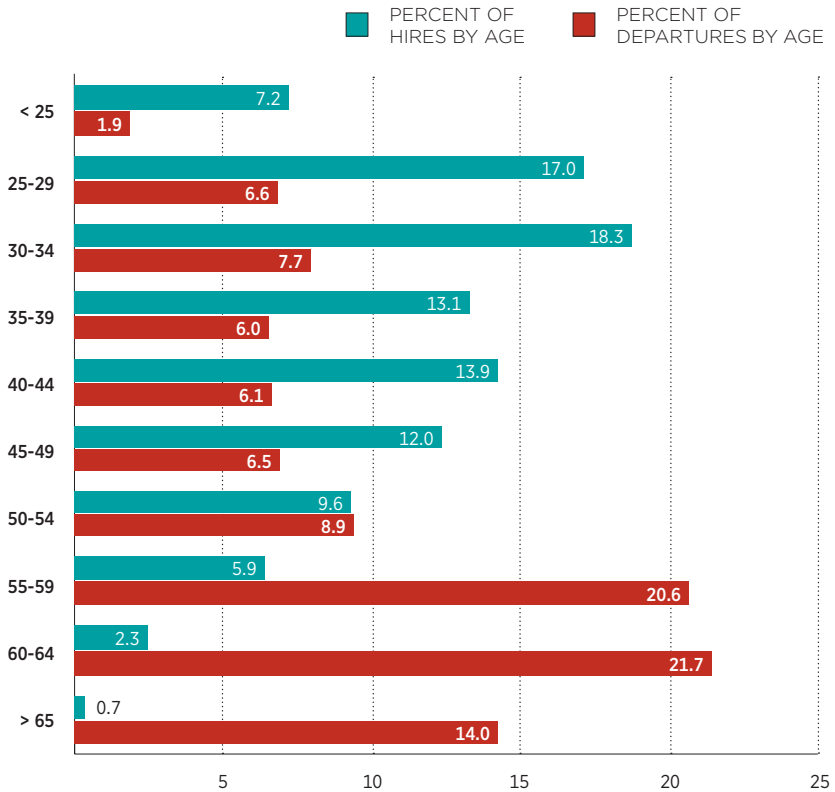
RACE AND ETHNICITY

In fiscal 2013, employees of a minority racial or ethnic group accounted for a smaller percentage of separations from federal service (30.8 percent) than they made up in the overall workforce (35.0 percent).



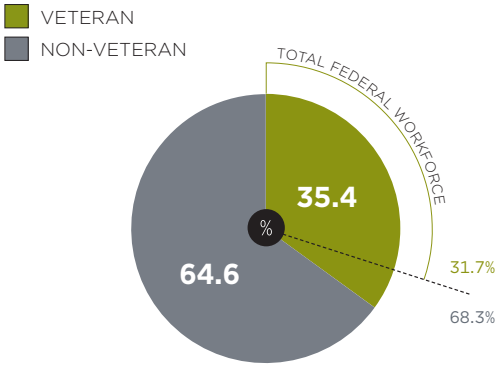
AGE

Employees under 30 accounted for 8.5 percent of departures, a sizable share since this group only represents 7.1 percent of the total federal workforce. Agencies will need to focus on retention strategies for this group of employees if they are to increase the representation of new, young talent in the federal workforce.

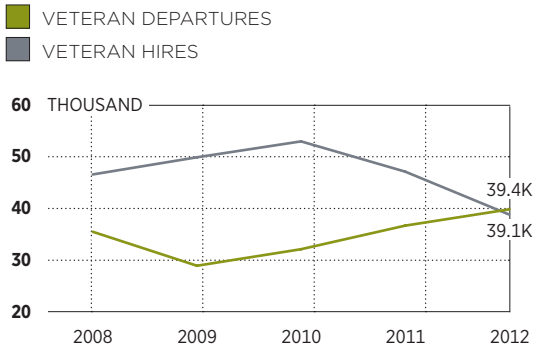


VETERAN STATUS

Veterans have accounted for slightly more than one-third of all federal employees who have left the government since 2008. Despite this turnover rate, the number of veterans in the federal workforce has increased from 446,826 veterans in 2008 to 572,239 veterans in 2012, the most recent year for which complete departures data for veterans is available. This coincided with a 2009 presidential executive order to increase veterans' employment.



VETERAN DEPARTURE TRENDS (2008–2012)



Data Sources: Unless otherwise noted below, all data are from FedScope (fedscope.opm.gov) for all full-time, nonseasonal, permanent employees who left federal service during fiscal 2013.

Race and Ethnicity: U.S. Office of Personnel Management analysis of full-time, nonseasonal, permanent employees who left federal service during fiscal 2013.

Veteran Status: U.S. Office of Personnel Management, *Employment of Veterans in the Federal Executive Branch: Fiscal Year 2012*, (Washington, D.C., 2012), 7, 17.

Veteran Departure Trends and Years of Service: Partnership for Public Service analysis of the Central Personnel Data File (now called the EHRI-SDM) for full-time, nonseasonal, permanent employees who left federal service during fiscal 2008-2012 and during 2002-2012, respectively.

Historical Federal Workforce Tables: "Executive Branch Civilian Employment Since 1940," U.S. Office of Personnel Management, http://1.usa.gov/1qUnFOQ (accessed Feb. 25, 2014).

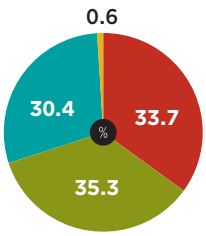
*Includes positions that are not included in other white-collar occupational groups either because the duties are unique or because they do not align with one particular group.

GS LEVEL

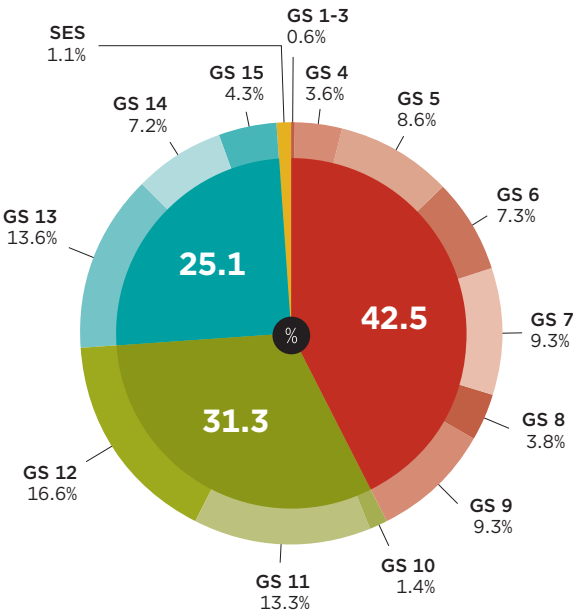
The General Schedule (GS) is a 15-level, government-wide pay and classification system used for the majority of the federal workforce. The largest number of employees who left federal service in 2013 were working at the GS-12 level, although entry-level employees made up a larger percentage of departures than they currently make up in the overall workforce—42.5 percent compared to 33.7 percent. Attrition rates were highest among the Senior Executive Service (SES) (11.3 percent) and among entry-level employees (7.6 percent).

ENTRY LEVEL
MID LEVEL
SENIOR LEVEL
SES

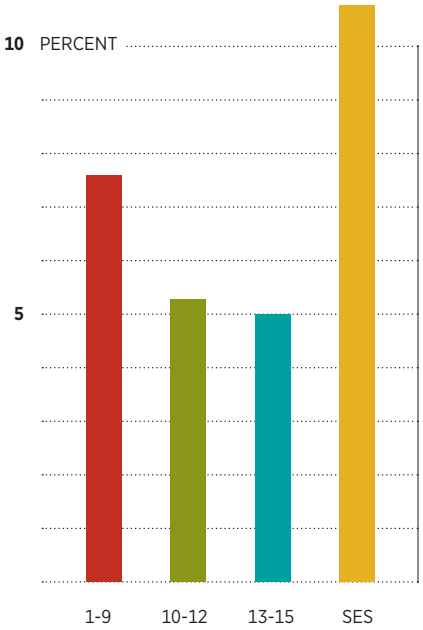
TOTAL FEDERAL WORKFORCE



PERCENT OF TOTAL WORKFORCE DEPARTURES BY GS LEVEL



ATTRITION RATE BY GS LEVEL (GROUPED)



In analyzing data for federal departures, the Partnership finds:

- The number of departing employees has increased for most years since fiscal 2009.
- Retirements accounted for more than half of all separations from federal service in 2013 (61,953), although the number of retirements decreased last year by 4,306.
- Resignations continued to increase in 2013, constituting 34.5 percent of all departures. The number of employees who resigned decreased in 2008 and 2009 during the worst years of the economic downturn, though more federal employees have quit each year since.
- Terminations or removals constituted only 8.4 percent of all departures in 2013. When placed in the context of government's 1.8 million employees, only 0.5 percent of the total workforce was terminated or removed in 2013.
- While entry-level employees only made up 33.7 percent of the federal workforce, they accounted for 42.5 percent of departures. In absolute numbers, the government hired roughly the same number of entry-level employees as it lost through departures in 2013, though the high turnover among entry-level talent poses challenges as agencies cultivate talent pipelines.

Predicting, preparing and managing these departures is critical to reshaping the federal workforce to meet evolving needs.

For more information and tips on how to examine turnover and retain employees, see "Beneath the Surface: Understanding Attrition at Your Agency and Why It Matters" and "Keeping Talent: Strategies for Retaining Valued Federal Employees."

For further information on the federal workforce or recent federal hiring trends, see the Partnership's "Federal Workforce" or "Federal Hiring" Fed Figures.

All are available at **ourpublicservice.org/publications.**

The Mission of INROADS is to develop and place talented underserved youth in business and industry, and prepare them for corporate and community leadership.

INROADS, Inc. 10 South Broadway, Suite 300 St Louis, Missouri 63102 Telephone: (314) 241-7488 Fax: (314) 241-9325
General Inquiries: info@INROADS.org - Applicant Inquiries: recruitment@INROADS.org

Students

Employers

Alumni

INROADS can be essential in meeting corporate strategic goals of hiring diverse leaders, future managers and high-performing, students.

Read more>>

Pat Collins
Sr. Manager for Diversity (retired)
Procter & Gamble North America

DonateNow

Frequently Asked Questions

GENERAL QUESTIONS ABOUT INROADS

See the menu at right for answers to questions related to the specific topics listed.

What is INROADS?

INROADS is the nation's largest non-profit source of paid internships for undergraduate, diverse youth. By providing the skills, support, and network students need to obtain an internship at a top company, INROADS prepares students to lead and contribute from Day 1. Learn more>>>

How does INROADS work?

INROADS knows talent. First, INROADS recruits the best and the brightest diverse college students. By understanding our corporate partners' needs and culture, while simultaneously coaching and training student applicants, we focus on getting the fit right, matching candidates who are ready to contribute on Day 1. Upon acceptance of an internship, INROADS Interns are provided on-going coaching with an advisor, a corporate mentor, access to our network and support such as free tutoring and scholarships, and most importantly, a unique skills development plan designed to increase the Intern's soft skills and overall understanding of how to become a high-performer. We save our clients time so they can focus on providing a supportive work environment with challenging work assignments. These successive year internships groom the Interns, not only for a full-time job with their corporate sponsor upon graduation, but also for fast advancement within that company. Learn more>>>

What is the INROADS goal?

The INROADS goal is achieved when a corporate sponsor hires its INROADS Intern immediately upon graduation. Over the past two years, 92% of INROADS Interns accepted offers for full time employment from their sponsoring companies. A large percentage of the remaining INROADS graduates accepted offers from other INROADS corporate sponsors.

Who is an INROADS Intern?

An INROADS Intern is an outstanding undergraduate college student pursuing a degree major in a field of study that will lead to a professional career in management. The student must maintain a B or better grade point average, and remain committed to the INROADS mission and goal. Learn more>>>

Who should apply for an INROADS Internship?

Talented undergraduate college students who have a 3.0 or higher GPA. Many INROADS Internships require a higher GPA. Interested students must pursue a college degree in business, accounting, actuarial science, engineering, computer and information sciences, sales, marketing

JEB HENSARLING, TX, CHAIRMAN

MAXINE WATERS, CA, RANKING MEMBER

United States House of Representatives
Committee on Financial Services
Washington, D.C. 20515

March 24, 2014

Acting Inspector General Fred Gibson
Federal Deposit Insurance Corporation
Office of Inspector General
3501 Fairfax Drive
Arlington, VA 22226

Dear Acting Inspector General Gibson:

We write to request that the Office of the Inspector General (OIG) for the Federal Deposit Insurance Corporation (FDIC) review the agency's internal operations to determine whether any personnel practices have created a discriminatory workplace or otherwise systematically disadvantaged minorities from obtaining senior management positions.

Section 342 of the Dodd-Frank Wall Street Reform and Consumer Protection Act established an Office of Minority and Women Inclusion (OMWI) at most of the federal financial regulatory agencies, responsible for matters relating to diversity in management, employment, and business activities. Despite this statutory mandate, the Government Accountability Office (GAO) concluded in a report released last year that management-level representation of minorities and women among federal financial agencies and Federal Reserve Banks has not changed substantially from 2007 through 2011. In fact, across all federal financial regulators, agency representation of minorities was as low as 6 percent and dropped as low as zero percent at one of the Reserve Banks. In light of these findings and the concerns raised by employee performance evaluations at the Consumer Financial Protection Bureau (CFPB), we believe the OIG should work in cooperation with Federal Deposit Insurance Corporation's OMWI Director to assess current personnel practices and make recommendations necessary to ensure full compliance with the law.

The 2013 GAO report, entitled "Trends and Practices in the Financial Industry and Agencies after the Recent Financial Crisis," documented the extremely poor representation of women and minorities in leadership positions within the financial services industry and among federal financial regulators. According to GAO, industry representation of minorities in 2011 was higher in lower-level management positions – approximately 20 percent – as compared to about 11 percent of senior-level manager positions.

While public attention is currently and justifiably focused on the CFPB, the most recent OMWI reports suggest the disparities impeding internal upward mobility for minorities may be endemic throughout all the agencies regulating the financial services industry. According to the Treasury Department's 2013 OMWI report, among its senior executive management, 86 percent are white men, compared to 7 percent Black men, 4 percent Hispanic men, and 3 percent Asian men. Among the agency's GS-15 employees, which serves as a pipeline to senior level management, white men are once again overrepresented at 86 percent, compared to 6 percent Black men, 2 percent Hispanic men, and 6 percent Asian men.

At the Federal Reserve, white men represent 50 percent of executive senior level managers, compared to just 28.7 percent represented by white women. Along ethnic categories, black and Hispanic men represent, respectively, roughly 5 percent and 1 percent of executive senior level managers. Black women represent roughly 6 percent and Hispanic women represent nearly 2 percent of senior managers.

According to the most recent information from the GAO, at the National Credit Union Administration (NCUA), whites represent 88 percent of senior level management positions, compared to 4 percent represented by blacks and 4 percent by Hispanics. At the Office of the Comptroller of the Currency (OCC), whites represent 82 percent of senior level managers, compared to 9 percent black and 5 percent Hispanic. Whites represent 89 percent of senior level management positions at the Securities and Exchange Commission, compared to 2 percent black and 5 percent Hispanic. Minorities appear to fair best at the Federal Housing Finance Agency, where whites represent 76 percent of senior level management positions, compared to 16 percent black and 8 percent Hispanic. However, more comprehensive analysis is still needed from the agency to fully assess the racial and gender employment of minorities in senior positions beyond the GAO's limited information.

Accordingly, we request that the OIG examine any employee complaints, formal or informal, related to personnel practices, workplace policies and the findings from any employee satisfaction surveys, whether conducted by the Federal Deposit Insurance Corporation or an outside entity. If the OIG identifies any individuals or groups of individuals who have exhibited discriminatory behaviors or patterns of unfair or unequal treatment, we ask that the OIG provide recommendations about appropriate actions, including remedial training or removal from employment with the agency. Furthermore, we request that the OIG assess the agency's OMWI operations, and ensure corrective actions are taken within the agency with regard to employee compensation, rating systems, retention, and promotion of women and minorities.

Sincerely,

JEB HENSARLING, TX, CHAIRMAN

MAXINE WATERS, CA, RANKING MEMBER

United States House of Representatives
Committee on Financial Services
Washington, D.C. 20515

March 24, 2014

Inspector General Eric M. Thorson
U.S. Department of the Treasury
Office of Inspector General
1500 Pennsylvania Avenue, N.W.
Room 4436,
Washington, DC 20220

Dear Inspector General Thorson:

We write to request that the Office of the Inspector General (OIG) for the U.S. Treasury Department review the agency's internal operations to determine whether any personnel practices have created a discriminatory workplace or otherwise systematically disadvantaged minorities from obtaining senior management positions.

Section 342 of the Dodd-Frank Wall Street Reform and Consumer Protection Act established an Office of Minority and Women Inclusion (OMWI) at most of the federal financial regulatory agencies, responsible for matters relating to diversity in management, employment, and business activities. Despite this statutory mandate, the Government Accountability Office (GAO) concluded in a report released last year that management-level representation of minorities and women among federal financial agencies and Federal Reserve Banks has not changed substantially from 2007 through 2011. In fact, across all federal financial regulators, agency representation of minorities was as low as 6 percent and dropped as low as zero percent at one of the Reserve Banks. In light of these findings and the concerns raised by employee performance evaluations at the Consumer Financial Protection Bureau (CFPB), we believe the OIG should work in cooperation with Treasury's OMWI Director to assess current personnel practices and make recommendations necessary to ensure full compliance with the law.

The 2013 GAO report, entitled "Trends and Practices in the Financial Industry and Agencies after the Recent Financial Crisis," documented the extremely poor representation of women and minorities in leadership positions within the financial services industry and among federal financial regulators. According to GAO, industry representation of minorities in 2011 was higher in lower-level management positions – approximately 20 percent – as compared to about 11 percent of senior-level manager positions.

While public attention is currently and justifiably focused on the CFPB, the most recent OMWI reports suggest the disparities impeding internal upward mobility for minorities may be endemic throughout all the agencies regulating the financial services industry. According to the Treasury Department's 2013 OMWI report, among its senior executive management, 86 percent are white men, compared to 7 percent Black men, 4 percent Hispanic men, and 3 percent Asian men. Among the agency's GS-15 employees, which serves as a pipeline to senior level management, white men are once again overrepresented at 86 percent, compared to 6 percent Black men, 2 percent Hispanic men, and 6 percent Asian men.

At the Federal Reserve, white men represent 50 percent of executive senior level managers, compared to just 28.7 percent represented by white women. Along ethnic categories, black and Hispanic men represent, respectively, roughly 5 percent and 1 percent of executive senior level managers. Black women represent roughly 6 percent and Hispanic women represent nearly 2 percent of senior managers.

According to the most recent information from the GAO, at the National Credit Union Administration (NCUA), whites represent 88 percent of senior level management positions, compared to 4 percent represented by blacks and 4 percent by Hispanics. At the Office of the Comptroller of the Currency (OCC), whites represent 82 percent of senior level managers, compared to 9 percent black and 5 percent Hispanic. Whites represent 89 percent of senior level management positions at the Securities and Exchange Commission, compared to 2 percent black and 5 percent Hispanic. Minorities appear to fair best at the Federal Housing Finance Agency, where whites represent 76 percent of senior level management positions, compared to 16 percent black and 8 percent Hispanic. However, more comprehensive analysis is still needed from the agency to fully assess the racial and gender employment of minorities in senior positions beyond the GAO's limited information.

Accordingly, we request that the OIG examine any employee complaints, formal or informal, related to personnel practices, workplace policies and the findings from any employee satisfaction surveys, whether conducted by the Treasury or an outside entity. If the OIG identifies any individuals or groups of individuals who have exhibited discriminatory behaviors or patterns of unfair or unequal treatment, we ask that the OIG provide recommendations about appropriate actions, including remedial training or removal from employment with the agency. Furthermore, we request that the OIG assess the agency's OMWI operations, and ensure corrective actions are taken within the agency with regard to employee compensation, rating systems, retention, and promotion of women and minorities.

Sincerely,

JEB HENSARLING, TX, CHAIRMAN

MAXINE WATERS, CA, RANKING MEMBER

United States House of Representatives
Committee on Financial Services
Washington, D.C. 20515

March 24, 2014

Acting Inspector General Michael P. Stephens
Federal Housing Finance Agency
Office of Inspector General
400 7th Street, S.W.
Washington, DC 20024

Dear Acting Inspector General Stephens:

We write to request that the Office of the Inspector General (OIG) for the Federal Housing Finance Agency (FHFA) review the agency's internal operations to determine whether any personnel practices have created a discriminatory workplace or otherwise systematically disadvantaged minorities from obtaining senior management positions.

Section 342 of the Dodd-Frank Wall Street Reform and Consumer Protection Act established an Office of Minority and Women Inclusion (OMWI) at most of the federal financial regulatory agencies, responsible for matters relating to diversity in management, employment, and business activities. Despite this statutory mandate, the Government Accountability Office (GAO) concluded in a report released last year that management-level representation of minorities and women among federal financial agencies and Federal Reserve Banks has not changed substantially from 2007 through 2011. In fact, across all federal financial regulators, agency representation of minorities was as low as 6 percent and dropped as low as zero percent at one of the Reserve Banks. In light of these findings and the concerns raised by employee performance evaluations at the Consumer Financial Protection Bureau (CFPB), we believe the OIG should work in cooperation with Federal Housing Finance Agency's OMWI Director to assess current personnel practices and make recommendations necessary to ensure full compliance with the law.

The 2013 GAO report, entitled "Trends and Practices in the Financial Industry and Agencies after the Recent Financial Crisis," documented the extremely poor representation of women and minorities in leadership positions within the financial services industry and among federal financial regulators. According to GAO, industry representation of minorities in 2011 was higher in lower-level management positions – approximately 20 percent – as compared to about 11 percent of senior-level manager positions.

While public attention is currently and justifiably focused on the CFPB, the most recent OMWI reports suggest the disparities impeding internal upward mobility for minorities may be endemic throughout all the agencies regulating the financial services industry. According to the Treasury Department's 2013 OMWI report, among its senior executive management, 86 percent are white men, compared to 7 percent Black men, 4 percent Hispanic men, and 3 percent Asian men. Among the agency's GS-15 employees, which serves as a pipeline to senior level management, white men are once again overrepresented at 86 percent, compared to 6 percent Black men, 2 percent Hispanic men, and 6 percent Asian men.

At the Federal Reserve, white men represent 50 percent of executive senior level managers, compared to just 28.7 percent represented by white women. Along ethnic categories, black and Hispanic men represent, respectively, roughly 5 percent and 1 percent of executive senior level managers. Black women represent roughly 6 percent and Hispanic women represent nearly 2 percent of senior managers.

According to the most recent information from the GAO, at the National Credit Union Administration (NCUA), whites represent 88 percent of senior level management positions, compared to 4 percent represented by blacks and 4 percent by Hispanics. At the Office of the Comptroller of the Currency (OCC), whites represent 82 percent of senior level managers, compared to 9 percent black and 5 percent Hispanic. Whites represent 89 percent of senior level management positions at the Securities and Exchange Commission, compared to 2 percent black and 5 percent Hispanic. Minorities appear to fair best at the Federal Housing Finance Agency, where whites represent 76 percent of senior level management positions, compared to 16 percent black and 8 percent Hispanic. However, more comprehensive analysis is still needed from the agency to fully assess the racial and gender employment of minorities in senior positions beyond the GAO's limited information.

Accordingly, we request that the OIG examine any employee complaints, formal or informal, related to personnel practices, workplace policies and the findings from any employee satisfaction surveys, whether conducted by the Federal Housing Finance Agency or an outside entity. If the OIG identifies any individuals or groups of individuals who have exhibited discriminatory behaviors or patterns of unfair or unequal treatment, we ask that the OIG provide recommendations about appropriate actions, including remedial training or removal from employment with the agency. Furthermore, we request that the OIG assess the agency's OMWI operations, and ensure corrective actions are taken within the agency with regard to employee compensation, rating systems, retention, and promotion of women and minorities.

Sincerely,

JEB HENSARLING, TX, CHAIRMAN

MAXINE WATERS, CA, RANKING MEMBER

United States House of Representatives
Committee on Financial Services
Washington, D.C. 20515

March 24, 2014

Inspector General James Hagen
National Credit Union Administration
Office of Inspector General
P. O. Box 25705
Alexandria, VA 22313-5705

Dear Inspector General Hagen:

We write to request that the Office of the Inspector General (OIG) for the National Credit Union Administration (NCUA) review the agency's internal operations to determine whether any personnel practices have created a discriminatory workplace or otherwise systematically disadvantaged minorities from obtaining senior management positions.

Section 342 of the Dodd-Frank Wall Street Reform and Consumer Protection Act established an Office of Minority and Women Inclusion (OMWI) at most of the federal financial regulatory agencies, responsible for matters relating to diversity in management, employment, and business activities. Despite this statutory mandate, the Government Accountability Office (GAO) concluded in a report released last year that management-level representation of minorities and women among federal financial agencies and Federal Reserve Banks has not changed substantially from 2007 through 2011. In fact, across all federal financial regulators, agency representation of minorities was as low as 6 percent and dropped as low as zero percent at one of the Reserve Banks. In light of these findings and the concerns raised by employee performance evaluations at the Consumer Financial Protection Bureau (CFPB), we believe the OIG should work in cooperation with National Credit Union Administration's OMWI Director to assess current personnel practices and make recommendations necessary to ensure full compliance with the law.

The 2013 GAO report, entitled "Trends and Practices in the Financial Industry and Agencies after the Recent Financial Crisis," documented the extremely poor representation of women and minorities in leadership positions within the financial services industry and among federal financial regulators. According to GAO, industry representation of minorities in 2011 was higher in lower-level management positions – approximately 20 percent – as compared to about 11 percent of senior-level manager positions.

While public attention is currently and justifiably focused on the CFPB, the most recent OMWI reports suggest the disparities impeding internal upward mobility for minorities may be endemic throughout all the agencies regulating the financial services industry. According to the Treasury Department's OMWI report, among its senior executive management, 86 percent are white men, compared to 7 percent Black men, 4 percent Hispanic men, and 3 percent Asian men. Among the agency's GS-15 employees, which serves as a pipeline to senior level management, white men are once again overrepresented at 86 percent, compared to 6 percent Black men, 2 percent Hispanic men, and 6 percent Asian men.

At the Federal Reserve, white men represent 50 percent of executive senior level managers, compared to just 28.7 percent represented by white women. Along ethnic categories, black and Hispanic men represent, respectively, roughly 5 percent and 1 percent of executive senior level managers. Black women represent roughly 6 percent and Hispanic women represent nearly 2 percent of senior managers.

According to the most recent information from the GAO, at the National Credit Union Administration (NCUA), whites represent 88 percent of senior level management positions, compared to 4 percent represented by blacks and 4 percent by Hispanics. At the Office of the Comptroller of the Currency (OCC), whites represent 82 percent of senior level managers, compared to 9 percent black and 5 percent Hispanic. Whites represent 89 percent of senior level management positions at the Securities and Exchange Commission, compared to 2 percent black and 5 percent Hispanic. Minorities appear to fair best at the Federal Housing Finance Agency, where whites represent 76 percent of senior level management positions, compared to 16 percent black and 8 percent Hispanic. However, more comprehensive analysis is still needed from the agency to fully assess the racial and gender employment of minorities in senior positions beyond the GAO's limited information.

Accordingly, we request that the OIG examine any employee complaints, formal or informal, related to personnel practices, workplace policies and the findings from any employee satisfaction surveys, whether conducted by the National Credit Union Administration or an outside entity. If the OIG identifies any individuals or groups of individuals who have exhibited discriminatory behaviors or patterns of unfair or unequal treatment, we ask that the OIG provide recommendations about appropriate actions, including remedial training or removal from employment with the agency. Furthermore, we request that the OIG assess the agency's OMWI operations, and ensure corrective actions are taken within the agency with regard to employee compensation, rating systems, retention, and promotion of women and minorities.

Sincerely,

JEB HENSARLING, TX, CHAIRMAN

United States House of Representatives
Committee on Financial Services
Washington, D.C. 20515

MAXINE WATERS, CA, RANKING MEMBER

March 24, 2014

Inspector General Mark Bialek
Board of Governors of the Federal Reserve System
Office of Inspector General
20th and C Streets N.W.
Mail Stop 300
Washington, DC 20551

Dear Inspector General Bialek:

We write to request that the Office of the Inspector General (OIG) for the Board of Governors of the Federal Reserve System (FRS) review the agency's internal operations to determine whether any personnel practices have created a discriminatory workplace or otherwise systematically disadvantaged minorities from obtaining senior management positions.

Section 342 of the Dodd-Frank Wall Street Reform and Consumer Protection Act established an Office of Minority and Women Inclusion (OMWI) at most of the federal financial regulatory agencies, responsible for matters relating to diversity in management, employment, and business activities. Despite this statutory mandate, the Government Accountability Office (GAO) concluded in a report released last year that management-level representation of minorities and women among federal financial agencies and Federal Reserve Banks has not changed substantially from 2007 through 2011. In fact, across all federal financial regulators, agency representation of minorities was as low as 6 percent and dropped as low as zero percent at one of the Reserve Banks. In light of these findings and the concerns raised by employee performance evaluations at the Consumer Financial Protection Bureau (CFPB), we believe the OIG should work in cooperation with Federal Reserve System's OMWI Director to assess current personnel practices and make recommendations necessary to ensure full compliance with the law.

The 2013 GAO report, entitled "Trends and Practices in the Financial Industry and Agencies after the Recent Financial Crisis," documented the extremely poor representation of women and minorities in leadership positions within the financial services industry and among federal financial regulators. According to GAO, industry representation of minorities in 2011 was higher in lower-level management positions – approximately 20 percent – as compared to about 11 percent of senior-level manager positions.

While public attention is currently and justifiably focused on the CFPB, the most recent OMWI reports suggest the disparities impeding internal upward mobility for minorities may be endemic throughout all the agencies regulating the financial services industry. According to the Treasury Department's 2013 OMWI report, among its senior executive management, 86 percent are white men, compared to 7 percent Black men, 4 percent Hispanic men, and 3 percent Asian men. Among the agency's GS-15 employees, which serves as a pipeline to senior level management, white men are once again overrepresented at 86 percent, compared to 6 percent Black men, 2 percent Hispanic men, and 6 percent Asian men.

At the Federal Reserve, white men represent 50 percent of executive senior level managers, compared to just 28.7 percent represented by white women. Along ethnic categories, black and Hispanic men represent, respectively, roughly 5 percent and 1 percent of executive senior level managers. Black women represent roughly 6 percent and Hispanic women represent nearly 2 percent of senior managers.

According to the most recent information from the GAO, at the National Credit Union Administration (NCUA), whites represent 88 percent of senior level management positions, compared to 4 percent represented by blacks and 4 percent by Hispanics. At the Office of the Comptroller of the Currency (OCC), whites represent 82 percent of senior level managers, compared to 9 percent black and 5 percent Hispanic. Whites represent 89 percent of senior level management positions at the Securities and Exchange Commission, compared to 2 percent black and 5 percent Hispanic. Minorities appear to fair best at the Federal Housing Finance Agency, where whites represent 76 percent of senior level management positions, compared to 16 percent black and 8 percent Hispanic. However, more comprehensive analysis is still needed from the agency to fully assess the racial and gender employment of minorities in senior positions beyond the GAO's limited information.

Accordingly, we request that the OIG examine any employee complaints, formal or informal, related to personnel practices, workplace policies and the findings from any employee satisfaction surveys, whether conducted by the Federal Reserve System or an outside entity. If the OIG identifies any individuals or groups of individuals who have exhibited discriminatory behaviors or patterns of unfair or unequal treatment, we ask that the OIG provide recommendations about appropriate actions, including remedial training or removal from employment with the agency. Furthermore, we request that the OIG assess the agency's OMWI operations, and ensure corrective actions are taken within the agency with regard to employee compensation, rating systems, retention, and promotion of women and minorities.

Sincerely,

JEB HENSARLING, TX, CHAIRMAN

MAXINE WATERS, CA, RANKING MEMBER

United States House of Representatives
Committee on Financial Services
Washington, D.C. 20515

March 24, 2014

Inspector General Carl W. Hoecker
U.S. Securities and Exchange Commission
Office of Inspector General
100 F Street, N.E.
Washington, DC 20549-2977

Dear Inspector General Hoecker:

We write to request that the Office of the Inspector General (OIG) for the U.S. Securities and Exchange Commission (SEC) review the agency's internal operations to determine whether any personnel practices have created a discriminatory workplace or otherwise systematically disadvantaged minorities from obtaining senior management positions.

Section 342 of the Dodd-Frank Wall Street Reform and Consumer Protection Act established an Office of Minority and Women Inclusion (OMWI) at most of the federal financial regulatory agencies, responsible for matters relating to diversity in management, employment, and business activities. Despite this statutory mandate, the Government Accountability Office (GAO) concluded in a report released last year that management-level representation of minorities and women among federal financial agencies and Federal Reserve Banks has not changed substantially from 2007 through 2011. In fact, across all federal financial regulators, agency representation of minorities was as low as 6 percent and dropped as low as zero percent at one of the Reserve Banks. In light of these findings and the concerns raised by employee performance evaluations at the Consumer Financial Protection Bureau (CFPB), we believe the OIG should work in cooperation with U.S. Securities and Exchange Commission's OMWI Director to assess current personnel practices and make recommendations necessary to ensure full compliance with the law.

The 2013 GAO report, entitled "Trends and Practices in the Financial Industry and Agencies after the Recent Financial Crisis," documented the extremely poor representation of women and minorities in leadership positions within the financial services industry and among federal financial regulators. According to GAO, industry representation of minorities in 2011 was higher in lower-level management positions – approximately 20 percent – as compared to about 11 percent of senior-level manager positions.

While public attention is currently and justifiably focused on the CFPB, the most recent OMWI reports suggest the disparities impeding internal upward mobility for minorities may be endemic throughout all the agencies regulating the financial services industry. According to the Treasury Department's OMWI report, among its senior executive management, 86 percent are white men, compared to 7 percent Black men, 4 percent Hispanic men, and 3 percent Asian men. Among the agency's GS-15 employees, which serves as a pipeline to senior level management, white men are once again overrepresented at 86 percent, compared to 6 percent Black men, 2 percent Hispanic men, and 6 percent Asian men.

At the Federal Reserve, white men represent 50 percent of executive senior level managers, compared to just 28.7 percent represented by white women. Along ethnic categories, black and Hispanic men represent, respectively, roughly 5 percent and 1 percent of executive senior level managers. Black women represent roughly 6 percent and Hispanic women represent nearly 2 percent of senior managers.

According to the most recent information from the GAO, at the National Credit Union Administration (NCUA), whites represent 88 percent of senior level management positions, compared to 4 percent represented by blacks and 4 percent by Hispanics. At the Office of the Comptroller of the Currency (OCC), whites represent 82 percent of senior level managers, compared to 9 percent black and 5 percent Hispanic. Whites represent 89 percent of senior level management positions at the Securities and Exchange Commission, compared to 2 percent black and 5 percent Hispanic. Minorities appear to fair best at the Federal Housing Finance Agency, where whites represent 76 percent of senior level management positions, compared to 16 percent black and 8 percent Hispanic. However, more comprehensive analysis is still needed from the agency to fully assess the racial and gender employment of minorities in senior positions beyond the GAO's limited information.

Accordingly, we request that the OIG examine any employee complaints, formal or informal, related to personnel practices, workplace policies and the findings from any employee satisfaction surveys, whether conducted by the U.S. Securities and Exchange Commission or an outside entity. If the OIG identifies any individuals or groups of individuals who have exhibited discriminatory behaviors or patterns of unfair or unequal treatment, we ask that the OIG provide recommendations about appropriate actions, including remedial training or removal from employment with the agency. Furthermore, we request that the OIG assess the agency's OMWI operations, and ensure corrective actions are taken within the agency with regard to employee compensation, rating systems, retention, and promotion of women and minorities.

Sincerely,

NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

http://dx.doi.org/10.6028/NIST.SP.800-53r4

National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

http://dx.doi.org/10.6028/NIST.SP.800-53r4

April 2013

INCLUDES UPDATES AS OF 01-15-2014: PAGE XVII

U.S. Department of Commerce
Rebecca M. Blank, Acting Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), *Securing Agency Information Systems*, as analyzed in Circular A-130, Appendix IV: *Analysis of Key Sections*. Supplemental information is provided in Circular A-130, Appendix III, *Security of Federal Automated Information Resources*.

National Institute of Standards and Technology Special Publication 800-53, Revision 4
Natl. Inst. Stand. Technol. Spec. Publ. 800-53, Rev. 4, 460 pages (April 2013)
http://dx.doi.org/10.6028/NIST.SP.800-53r4
CODEN: NSPUE2

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by Federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, Federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. All NIST Computer Security Division publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Electronic Mail: sec-cert@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

This publication provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors. The controls are customizable and implemented as part of an organization-wide process that manages information security and privacy risk. The controls address a diverse set of security and privacy requirements across the federal government and critical infrastructure, derived from legislation, Executive Orders, policies, directives, regulations, standards, and/or mission/business needs. The publication also describes how to develop specialized sets of controls, or overlays, tailored for specific types of missions/business functions, technologies, or environments of operation. Finally, the catalog of security controls addresses security from both a functionality perspective (the strength of security functions and mechanisms provided) and an assurance perspective (the measures of confidence in the implemented security capability). Addressing both security functionality and security assurance ensures that information technology products and the information systems built from those products using sound systems and security engineering principles are sufficiently trustworthy.

Keywords

Assurance; computer security; FIPS Publication 199; FIPS Publication 200, FISMA; Privacy Act; Risk Management Framework; security controls; security requirements.

Acknowledgements

This publication was developed by the *Joint Task Force Transformation Initiative* Interagency Working Group with representatives from the Civil, Defense, and Intelligence Communities in an ongoing effort to produce a unified information security framework for the federal government. The National Institute of Standards and Technology wishes to acknowledge and thank the senior leaders from the Departments of Commerce and Defense, the Office of the Director of National Intelligence, the Committee on National Security Systems, and the members of the interagency technical working group whose dedicated efforts contributed significantly to the publication. The senior leaders, interagency working group members, and their organizational affiliations include:

Department of Defense

Teresa M. Takai
DoD Chief Information Officer

Robert J. Carey
Principal Deputy DoD Chief Information Officer

Richard Hale
Deputy Chief Information Officer for Cybersecurity

Dominic Cussatt
Deputy Director, Cybersecurity Policy

Office of the Director of National Intelligence

Adolpho Tarasiuk Jr.
Assistant DNI and Intelligence Community Chief Information Officer

Charlene Leubecker
Deputy Intelligence Community Chief Information Officer

Catherine A. Henson
Director, Data Management

Greg Hall
Chief, Risk Management and Information Security Programs Division

National Institute of Standards and Technology

Charles H. Romine
Director, Information Technology Laboratory

Donna Dodson
Cybersecurity Advisor, Information Technology Laboratory

Donna Dodson
Chief, Computer Security Division

Ron Ross
FISMA Implementation Project Leader

Committee on National Security Systems

Teresa M. Takai
Chair, CNSS

Richard Spires
Co-Chair, CNSS

Dominic Cussatt
CNSS Subcommittee Tri-Chair

Jeffrey Wilk
CNSS Subcommittee Tri-Chair

Richard Tannich
CNSS Subcommittee Tri-Chair

Joint Task Force Transformation Initiative Interagency Working Group

Ron Ross *NIST, JTF Leader*	Gary Stoneburner *Johns Hopkins APL*	Richard Graubart *The MITRE Corporation*	Kelley Dempsey *NIST*
Esten Porter *The MITRE Corporation*	Bennett Hodge *Booz Allen Hamilton*	Karen Quigg *The MITRE Corporation*	Christian Enloe *NIST*
Kevin Stine *NIST*	Jennifer Fabius *The MITRE Corporation*	Daniel Faigin *The Aerospace Corporation*	Arnold Johnson *NIST*
Lisa Kaiser *DHS*	Pam Miller *The MITRE Corporation*	Sandra Miravalle *The MITRE Corporation*	Victoria Pillitteri *NIST*

In addition to the above acknowledgments, a special note of thanks goes to Peggy Himes and Elizabeth Lennon of NIST for their superb technical editing and administrative support. The authors also wish to recognize Marshall Abrams, Nadya Bartol, Frank Belz, Deb Bodeau, Dawn Cappelli, Corinne Castanza, Matt Coose, George Dinolt, Kurt Eleam, Jennifer Guild, Cynthia Irvine, Cass Kelly, Steve LaFountain, Steve Lipner, Tom Macklin, Tim McChesney, Michael

McEvilley, John Mildner, Joji Montelibano, George Moore, LouAnna Notargiacomo, Dorian Pappas, Roger Schell, Carol Woody, and the research staff from the NIST Computer Security Division for their exceptional contributions in helping to improve the content of the publication. And finally, the authors also gratefully acknowledge and appreciate the significant contributions from individuals, working groups, and organizations in the public and private sectors, both nationally and internationally, whose thoughtful and constructive comments improved the overall quality, thoroughness, and usefulness of this publication.

FIPS 200 AND SP 800-53

IMPLEMENTING INFORMATION SECURITY STANDARDS AND GUIDELINES

FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, is a mandatory federal standard developed by NIST in response to FISMA. To comply with the federal standard, organizations first determine the security category of their information system in accordance with FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, derive the information system impact level from the security category in accordance with FIPS 200, and then apply the appropriately tailored set of baseline security controls in NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*. Organizations have flexibility in applying the baseline security controls in accordance with the guidance provided in Special Publication 800-53. This allows organizations to tailor the relevant security control baseline so that it more closely aligns with their mission and business requirements and environments of operation.

FIPS 200 and NIST Special Publication 800-53, in combination, ensure that appropriate security requirements and security controls are applied to all federal information and information systems. An organizational assessment of risk validates the initial security control selection and determines if additional controls are needed to protect organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation. The resulting set of security controls establishes a level of security due diligence for the organization.

DEVELOPING COMMON INFORMATION SECURITY FOUNDATIONS

COLLABORATION AMONG PUBLIC AND PRIVATE SECTOR ENTITIES

In developing standards and guidelines required by FISMA, NIST consults with other federal agencies and the private sector to improve information security, avoid unnecessary and costly duplication of effort, and ensure that its publications are complementary with the standards and guidelines employed for the protection of national security systems. In addition to a comprehensive public review and vetting process, NIST is collaborating with the Office of the Director of National Intelligence (ODNI), the Department of Defense (DoD), and the Committee on National Security Systems (CNSS) to establish a unified information security framework for the federal government. A common foundation for information security will provide the Civil, Defense, and Intelligence sectors of the federal government and their contractors, more cost-effective and consistent ways to manage information security-related risk to organizational operations and assets, individuals, other organizations, and the Nation. The unified framework will also provide a strong basis for reciprocal acceptance of authorization decisions and facilitate information sharing. NIST is also working with many public and private sector entities to establish mappings and relationships between the security standards and guidelines developed by NIST and the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC).

SECURITY REQUIREMENTS

FROM THE PERSPECTIVE OF DIFFERENT COMMUNITIES OF INTEREST

The term *security requirement* is used by different communities and groups in different ways and may require additional explanation to establish the particular context for the various use cases. Security requirements can be stated at a very high level of abstraction, for example, in legislation, Executive Orders, directives, policies, standards, and mission/business needs statements. FISMA and FIPS Publication 200 articulate security requirements at such a level.

Acquisition personnel develop security requirements for contracting purposes that address the protections necessary to achieve mission/business needs. Systems/security engineers, system developers, and systems integrators develop the security design requirements for the information system, develop the system security architecture and the architecture-specific derived security requirements, and subsequently implement specific security functions at the hardware, software, and firmware component level.

Security requirements are also reflected in various nontechnical security controls that address such matters as policy and procedures at the management and operational elements within organizations, again at differing levels of detail. It is important to define the context for each use of the term security requirement so the respective communities (including individuals responsible for policy, architecture, acquisition, engineering, and mission/business protection) can clearly communicate their intent.

Organizations may define certain *security capabilities* needed to satisfy security requirements and provide appropriate mission and business protection. Security capabilities are typically defined by bringing together a specific set of safeguards/countermeasures (i.e., security controls) derived from the appropriately tailored baselines that together produce the needed capability.

TECHNOLOGY AND POLICY NEUTRALITY

CHARACTERISTICS OF SECURITY CONTROLS

The security controls in the catalog with few exceptions, have been designed to be policy- and technology-neutral. This means that security controls and control enhancements focus on the fundamental safeguards and countermeasures necessary to protect information during processing, while in storage, and during transmission. Therefore, it is beyond the scope of this publication to provide guidance on the application of security controls to specific technologies, environments of operation, communities of interest, or missions/business functions. Application-specific areas are addressed by the use of the tailoring process described in Chapter Three and the use of overlays described in Appendix I. It should also be noted that while the security controls are largely policy- and technology-neutral, that does not imply that the controls are policy- and technology-unaware. Understanding policy and technology is necessary so that the controls are meaningful and relevant when implemented.

In the few cases where specific technologies are called out in security controls (e.g., mobile, PKI, wireless, VOIP), organizations are cautioned that the need to provide adequate security goes well beyond the requirements in a single control associated with a particular technology. Many of the needed safeguards and countermeasures are obtained from the other security controls in the catalog allocated to the initial control baselines as starting points for the development of security plans and overlays using the tailoring process. There may also be some overlap in the protections articulated by the security controls within the different control families.

In addition to the customer-driven development of specialized security plans and overlays, NIST Special Publications and Interagency Reports may provide guidance on recommended security controls for specific technologies and sector-specific applications (e.g., Smart Grid, healthcare, Industrial Control Systems, and mobile).

Employing a technology- and policy-neutral security control catalog has the following benefits:

- It encourages organizations to focus on the *security capabilities* required for mission/business success and the protection of information, irrespective of the information technologies that are employed in organizational information systems.
- It encourages organizations to analyze each security control for its applicability to specific technologies, environments of operation, missions/business functions, and communities of interest.
- It encourages organizations to specify security policies as part of the tailoring process for security controls that have variable parameters.

The specialization of security plans using the tailoring guidance and overlays, together with a robust set of technology- and policy-neutral security controls, promotes cost-effective, risk-based information security for organizations—in any sector, for any technology, and in any operating environment.

INFORMATION SECURITY DUE DILIGENCE

MANAGING THE RISK TO ORGANIZATIONAL MISSIONS/BUSINESS FUNCTIONS

The security controls in NIST Special Publication 800-53 are designed to facilitate compliance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Compliance is *not* about adhering to static checklists or generating unnecessary FISMA reporting paperwork. Rather, compliance necessitates organizations executing *due diligence* with regard to information security and risk management. Information security due diligence includes using all appropriate information as part of an organization-wide risk management program to effectively use the tailoring guidance and inherent flexibility in NIST publications so that the selected security controls documented in organizational security plans meet the mission and business requirements of organizations. Using the risk management tools and techniques that are available to organizations is essential in developing, implementing, and maintaining the safeguards and countermeasures with the necessary and sufficient strength of mechanism to address the current threats to organizational operations and assets, individuals, other organizations, and the Nation. Employing effective risk-based processes, procedures, and technologies will help ensure that all federal information systems and organizations have the necessary resilience to support ongoing federal responsibilities, critical infrastructure applications, and continuity of government.

PRIVACY CONTROLS

PROVIDING PRIVACY PROTECTION FOR FEDERAL INFORMATION

Appendix J, *Privacy Control Catalog*, is a new addition to NIST Special Publication 800-53. It is intended to address the privacy needs of federal agencies. The Privacy Appendix:

- Provides a structured set of privacy controls, based on best practices, that help organizations comply with applicable federal laws, Executive Orders, directives, instructions, regulations, policies, standards, guidance, and organization-specific issuances;
- Establishes a linkage and relationship between privacy and security controls for purposes of enforcing respective privacy and security requirements which may overlap in concept and in implementation within federal information systems, programs, and organizations;
- Demonstrates the applicability of the NIST Risk Management Framework in the selection, implementation, assessment, and ongoing monitoring of privacy controls deployed in federal information systems, programs, and organizations; and
- Promotes closer cooperation between privacy and security officials within the federal government to help achieve the objectives of senior leaders/executives in enforcing the requirements in federal privacy legislation, policies, regulations, directives, standards, and guidance.

There is a strong similarity in the structure of the privacy controls in Appendix J and the security controls in Appendices F and G. For example, the control AR-1 (Governance and Privacy Program) requires organizations to develop privacy plans that can be implemented at the organizational or program level. These plans can also be used in conjunction with security plans to provide an opportunity for organizations to select the appropriate set of security and privacy controls in accordance with organizational mission/business requirements and the environments in which the organizations operate. Incorporating the same concepts used in managing information security risk, helps organizations implement privacy controls in a more cost-effective, risked-based manner while simultaneously protecting individual privacy and meeting compliance requirements. Standardized privacy controls provide a more disciplined and structured approach for satisfying federal privacy requirements and demonstrating compliance to those requirements.

CAUTIONARY NOTE

IMPLEMENTING CHANGES BASED ON REVISIONS TO SPECIAL PUBLICATION 800-53

When NIST publishes revisions to Special Publication 800-53, there are four primary types of changes made to the document: (i) security controls or control enhancements are added to or withdrawn from Appendices F and G and/or to the low, moderate, and high baselines; (ii) supplemental guidance is modified; (iii) material in the main chapters or appendices is modified; and (iv) language is clarified and/or updated throughout the document.

When modifying existing tailored security control baselines at Tier 3 in the risk management hierarchy (as described in Special Publication 800-39) and updating security controls at any tier as a result of Special Publication 800-53 revisions, organizations should take a measured, risk-based approach in accordance with organizational risk tolerance and current risk assessments. Unless otherwise directed by OMB policy, the following activities are recommended to implement changes to Special Publication 800-53:

- First, organizations determine if any added security controls/control enhancements are applicable to organizational information systems or environments of operation following tailoring guidelines in this publication.
- Next, organizations review changes to the supplemental guidance, guidance in the main chapters and appendices, and updated/clarified language throughout the publication to determine if changes apply to any organizational information systems and if any immediate actions are required.
- Finally, once organizations have determined the entirety of changes necessitated by the revisions to the publication, the changes are integrated into the established continuous monitoring process to the greatest extent possible. The implementation of new or modified security controls to address specific, active threats is always the highest priority for sequencing and implementing changes. Modifications such as changes to templates or minor language changes in policy or procedures are generally the lowest priority and are made in conjunction with established review cycles.

Table of Contents

Prologue

"*…Through the process of risk management, leaders must consider risk to US interests from adversaries using cyberspace to their advantage and from our own efforts to employ the global nature of cyberspace to achieve objectives in military, intelligence, and business operations… "*

"…For operational plans development, the combination of threats, vulnerabilities, and impacts must be evaluated in order to identify important trends and decide where effort should be applied to eliminate or reduce threat capabilities; eliminate or reduce vulnerabilities; and assess, coordinate, and deconflict all cyberspace operations…"

"…Leaders at all levels are accountable for ensuring readiness and security to the same degree as in any other domain…"

-- THE NATIONAL STRATEGY FOR CYBERSPACE OPERATIONS
OFFICE OF THE CHAIRMAN, JOINT CHIEFS OF STAFF, U.S. DEPARTMENT OF DEFENSE

Foreword

NIST Special Publication 800-53, Revision 4, represents the most comprehensive update to the security controls catalog since its inception in 2005. The publication was developed by NIST, the Department of Defense, the Intelligence Community, and the Committee on National Security Systems as part of the Joint Task Force, an interagency partnership formed in 2009. This update was motivated principally by the expanding threat space—characterized by the increasing sophistication of cyber attacks and the operations tempo of adversaries (i.e., the frequency of such attacks, the professionalism of the attackers, and the persistence of targeting by attackers). State-of-the-practice security controls and control enhancements have been developed and integrated into the catalog addressing such areas as: mobile and cloud computing; applications security; trustworthiness, assurance, and resiliency of information systems; insider threat; supply chain security; and the advanced persistent threat. In addition, Special Publication 800-53 has been expanded to include eight new families of privacy controls based on the internationally accepted Fair Information Practice Principles.

Special Publication 800-53, Revision 4, provides a more *holistic* approach to information security and risk management by providing organizations with the breadth and depth of security controls necessary to fundamentally strengthen their information systems and the environments in which those systems operate—contributing to systems that are more resilient in the face of cyber attacks and other threats. This "Build It Right" strategy is coupled with a variety of security controls for "Continuous Monitoring" to give organizations near real-time information that is essential for senior leaders making ongoing *risk-based* decisions affecting their critical missions and business functions.

To take advantage of the expanded set of security and privacy controls, and to give organizations greater flexibility and agility in defending their information systems, the concept of *overlays* was introduced in this revision. Overlays provide a structured approach to help organizations tailor security control baselines and develop specialized security plans that can be applied to specific missions/business functions, environments of operation, and/or technologies. This specialization approach is important as the number of threat-driven controls and control enhancements in the catalog increases and organizations develop risk management strategies to address their specific protection needs within defined risk tolerances.

Finally, there have been several new features added to this revision to facilitate ease of use by organizations. These include:

- Assumptions relating to security control baseline development;
- Expanded, updated, and streamlined tailoring guidance;
- Additional assignment and selection statement options for security and privacy controls;
- Descriptive names for security and privacy control enhancements;
- Consolidated tables for security controls and control enhancements by family with baseline allocations;
- Tables for security controls that support development, evaluation, and operational assurance; and
- Mapping tables for international security standard ISO/IEC 15408 (Common Criteria).

The security and privacy controls in Special Publication 800-53, Revision 4, have been designed to be largely policy/technology-neutral to facilitate flexibility in implementation. The controls are well positioned to support the integration of information security and privacy into organizational processes including enterprise architecture, systems engineering, system development life cycle, and acquisition/procurement. Successful integration of security and privacy controls into ongoing organizational processes will demonstrate a greater maturity of security and privacy programs and provide a tighter coupling of security and privacy investments to core organizational missions and business functions.

The Joint Task Force

Errata

The following changes have been incorporated into Special Publication 800-53, Revision 4.

DATE	TYPE	CHANGE	PAGE
05-07-2013	Editorial	Changed CA-9 Priority Code from P1 to P2 in Table D-2.	D-3
05-07-2013	Editorial	Changed CM-10 Priority Code from P1 to P2 in Table D-2.	D-4
05-07-2013	Editorial	Changed MA-6 Priority Code from P1 to P2 in Table D-2.	D-5
05-07-2013	Editorial	Changed MP-3 Priority Code from P1 to P2 in Table D-2.	D-5
05-07-2013	Editorial	Changed PE-5 Priority Code from P1 to P2 in Table D-2.	D-5
05-07-2013	Editorial	Changed PE-16 Priority Code from P1 to P2 in Table D-2.	D-5
05-07-2013	Editorial	Changed PE-17 Priority Code from P1 to P2 in Table D-2.	D-5
05-07-2013	Editorial	Changed PE-18 Priority Code from P2 to P3 in Table D-2.	D-5
05-07-2013	Editorial	Changed PL-4 Priority Code from P1 to P2 in Table D-2.	D-6
05-07-2013	Editorial	Changed PS-4 Priority Code from P2 to P1 in Table D-2.	D-6
05-07-2013	Editorial	Changed SA-11 Priority Code from P2 to P1 in Table D-2.	D-6
05-07-2013	Editorial	Changed SC-18 Priority Code from P1 to P2 in Table D-2.	D-7
05-07-2013	Editorial	Changed SI-8 Priority Code from P1 to P2 in Table D-2.	D-8
05-07-2013	Editorial	Deleted reference to SA-5 (6) in Table D-17.	D-32
05-07-2013	Editorial	Deleted CM-4 (3) from Table E-2.	E-4
05-07-2013	Editorial	Deleted CM-4 (3) from Table E-3.	E-5
05-07-2013	Editorial	Deleted reference to SA-5 (6).	F-161
05-07-2013	Editorial	Changed SI-16 Priority Code from P0 to P1.	F-233
01-15-2014	Editorial	Deleted “(both intentional and unintentional)” in line 5 in Abstract.	iii
01-15-2014	Editorial	Deleted “security and privacy” in line 5 in Abstract.	iii
01-15-2014	Editorial	Changed “an initial set of baseline security controls” to “the applicable security control baseline” in Section 2.1, RMF Step 2.	9
01-15-2014	Editorial	Deleted the following paragraph: “The security control enhancements section provides…in Appendix F.”	11
01-15-2014	Editorial	Changed “baseline security controls” to “the security control baselines” in Section 2.3, 2nd paragraph, line 6.	13
01-15-2014	Editorial	Changed “an initial set of security controls” to “the applicable security control baseline” in Section 3.1, paragraph 2, line 4.	28
01-15-2014	Editorial	Changed “security control baselines” to “baselines identified in Appendix D” in Section 3.1, paragraph 2, line 5.	28
01-15-2014	Editorial	Changed “an appropriate set of baseline controls” to “the appropriate security control baseline” in Section 3.1, paragraph 3, line 3.	29
01-15-2014	Editorial	Deleted “initial” before “security control baseline” and added “FIPS 200” before “impact level” in Section 3.1, paragraph 3, line 4.	29
01-15-2014	Editorial	Changed “sets of baseline security controls” to “security control baselines” in Section 3.1, paragraph 3, line 6.	29
01-15-2014	Editorial	Changed “initial set of baseline security controls” to “applicable security control baseline” in Section 3.2, paragraph 1, line 1.	30
01-15-2014	Editorial	Changed “initial set of baseline security controls” to “applicable security control baseline” in Section 3.2, paragraph 3, line 5.	31
01-15-2014	Editorial	Deleted “set of” before “security controls” in Section 3.2, Applying Scoping Considerations, Mobility paragraph, line 1.	33

DATE	TYPE	CHANGE	PAGE
01-15-2014	Editorial	Deleted “initial” before “set of” in Section 3.2, Applying Scoping Considerations, Mobility paragraph, line 2.	33
01-15-2014	Editorial	Changed “the baselines” to “each baseline” in Section 3.2, Applying Scoping Considerations, Mobility paragraph, line 3.	33
01-15-2014	Editorial	Changed “initial set of security controls” to “security control baseline” in Section 3.2, Applying Scoping Considerations, Mobility paragraph, line 5.	33
01-15-2014	Editorial	Added “specific” before “locations” in Section 3.2, Applying Scoping Considerations, Mobility paragraph, line 6.	33
01-15-2014	Editorial	Changed “initial” to “three” in Section 3.2, Applying Scoping Considerations, Mobility paragraph, line 8.	33
01-15-2014	Editorial	Changed “initial set of baseline security controls” to “applicable security control baseline” in Section 3.2, Selecting Compensating Security Controls, line 10.	36
01-15-2014	Editorial	Changed “a set of initial baseline security controls” to “security control baselines” in Section 3.3, line 1.	40
01-15-2014	Editorial	Added “.” after “C.F.R” in #3, Policies, Directives, Instructions, Regulations, and Memoranda.	A-1
01-15-2014	Editorial	Added “Revision 1 (Draft)” to NIST Special Publication 800-52 in References.	A-7
01-15-2014	Editorial	Added “Configuration,” to title of NIST Special Publication 800-52, Revision 1.	A-7
01-15-2014	Editorial	Changed date for NIST Special Publication 800-52, Revision 1 to September 2013.	A-7
01-15-2014	Editorial	Moved definition for Information Security Risk after Information Security Program Plan in Glossary.	B-11
01-15-2014	Editorial	Added AC-2 (11) to high baseline in Table D-2.	D-2
01-15-2014	Editorial	Changed AC-10 Priority Code from P2 to P3 in Table D-2.	D-2
01-15-2014	Editorial	Changed AC-14 Priority Code from P1 to P3 in Table D-2.	D-2
01-15-2014	Editorial	Changed AC-22 Priority Code from P2 to P3 in Table D-2.	D-2
01-15-2014	Editorial	Changed AU-10 Priority Code from P1 to P2 in Table D-2.	D-3
01-15-2014	Editorial	Changed CA-6 Priority Code from P3 to P2 in Table D-2.	D-3
01-15-2014	Editorial	Changed CA-7 Priority Code from P3 to P2 in Table D-2.	D-3
01-15-2014	Editorial	Changed CA-8 Priority Code from P1 to P2 in Table D-2.	D-3
01-15-2014	Editorial	Changed IA-6 Priority Code from P1 to P2 in Table D-2.	D-4
01-15-2014	Editorial	Changed IR-7 Priority Code from P3 to P2 in Table D-2.	D-5
01-15-2014	Editorial	Changed MA-3 Priority Code from P2 to P3 in Table D-2.	D-5
01-15-2014	Editorial	Changed MA-4 Priority Code from P1 to P2 in Table D-2.	D-5
01-15-2014	Editorial	Changed MA-5 Priority Code from P1 to P2 in Table D-2.	D-5
01-15-2014	Editorial	Deleted Program Management Controls from Table D-2.	D-8/9
01-15-2014	Editorial	Deleted the following sentence at end of paragraph: “There is no summary table provided for the Program Management (PM) family since PM controls are not associated with any particular security control baseline.”	D-9
01-15-2014	Editorial	Added AC-2 (12) and AC-2 (13) to high baseline in Table D-3.	D-10
01-15-2014	Editorial	Changed AC-17 (5) incorporated into reference from AC-17 to SI-4 in Table D-3.	D-12
01-15-2014	Editorial	Changed AC-17 (7) incorporated into reference from AC-3 to AC-3 (10) in Table D-3.	D-12
01-15-2014	Editorial	Changed AC-6 to AC-6 (9) in AU-2 (4) withdrawal notice in Table D-5.	D-15
01-15-2014	Editorial	Changed “Training” to “Scanning” in SA-19 (4) title in Table D-17.	D-34
01-15-2014	Editorial	Deleted SC-9 (1), SC-9 (2), SC-9 (3), and SC-9 (4) from Table D-18.	D-37
01-15-2014	Editorial	Added AC-2 and AC-5 to SC-14 and deleted SI-9 from SC-14 in Table D-18.	D-37

DATE	TYPE	CHANGE	PAGE
01-15-2014	Editorial	Deleted CA-3 (5) from Table E-2.	E-4
01-15-2014	Editorial	Added CM-3 (2) to Table E-2.	E-4
01-15-2014	Editorial	Added RA-5 (2) and RA-5 (5) to Table E-2.	E-4
01-15-2014	Editorial	Deleted CA-3 (5) from Table E-3.	E-5
01-15-2014	Editorial	Added CM-3 (2) to Table E-3.	E-5
01-15-2014	Editorial	Deleted bold text from RA-5 (2) and RA-5 (5) in Table E-3.	E-5
01-15-2014	Editorial	Added CM-8 (9) to Table E-4.	E-7
01-15-2014	Editorial	Added CP-4 (4) to Table E-4.	E-7
01-15-2014	Editorial	Added IR-3 (1) to Table E-4.	E-7
01-15-2014	Editorial	Added RA-5 (3) to Table E-4.	E-7
01-15-2014	Editorial	Deleted SA-4 (4) from Table E-4.	E-7
01-15-2014	Editorial	Changed SA-21 (1) from “enhancements” to “enhancement” in Table E-4.	E-7
01-15-2014	Editorial	Deleted SI-4 (8) from Table E-4.	E-7
01-15-2014	Editorial	Changed “risk management process” to “RMF” in Using the Catalog, line 4.	F-6
01-15-2014	Editorial	Changed “an appropriate set of security controls” to “the appropriate security control baselines” in Using the Catalog, line 5.	F-6
01-15-2014	Editorial	Deleted extraneous “,” from AC-2 g.	F-7
01-15-2014	Editorial	Added AC-2 (11) to high baseline.	F-10
01-15-2014	Substantive	Added the following text to AC-3 (2) Supplemental Guidance: “Dual authorization may also be known as two-person control.”	F-11
01-15-2014	Editorial	Changed “ucdmo.gov” to “None” in AC-4 References.	F-18
01-15-2014	Editorial	Added “.” after “C.F.R” in AT-2 References.	F-38
01-15-2014	Editorial	Changed AC-6 to AC-6 (9) in AU-2 (4) withdrawal notice.	F-42
01-15-2014	Editorial	Deleted “csrc.nist.gov/pcig/cig.html” and added “http://” to URL in AU-2 References.	F-42
01-15-2014	Editorial	Changed “identify” to “identity” in AU-6 (6) Supplemental Guidance.	F-46
01-15-2014	Substantive	Added the following text to AU-9 (5) Supplemental Guidance: “Dual authorization may also be known as two-person control.”	F-49
01-15-2014	Editorial	Added “Control Enhancements: None.” to AU-15.	F-53
01-15-2014	Editorial	Deleted extraneous “.” from CM-2 (7) Supplemental Guidance.	F-66
01-15-2014	Editorial	Added “)” after “board” in CM-3 g.	F-66
01-15-2014	Substantive	Added CA-7 to related controls list in CM-3.	F-66
01-15-2014	Substantive	Added the following text to CM-5 (4) Supplemental Guidance: “Dual authorization may also be known as two-person control.”	F-69
01-15-2014	Editorial	Added “http://” to URLs in CM-6 References.	F-71
01-15-2014	Editorial	Added “component” before “inventories” in CM-8 (5).	F-74
01-15-2014	Editorial	Changed “tsp.ncs.gov” to “http://www.dhs.gov/telecommunications-service-priority-tsp” in CP-8 References.	F-86
01-15-2014	Substantive	Added the following text to CP-9 (7) Supplemental Guidance: “Dual authorization may also be known as two-person control.”	F-87
01-15-2014	Editorial	Changed “HSPD 12” to “HSPD-12” and added “http://” to URL in IA-2 References.	F-93
01-15-2014	Editorial	Changed “encrypted representations of” to “cryptographically-protected” in IA-5 (1) (c).	F-96
01-15-2014	Editorial	Changed “Encrypted representations of” to “Cryptographically-protected” in IA-5 (1) Supplemental Guidance.	F-97

DATE	TYPE	CHANGE	PAGE
01-15-2014	Substantive	Added the following text to IA-5 (1) Supplemental Guidance: "To mitigate certain brute force attacks against passwords, organizations may also consider salting passwords."	F-97
01-15-2014	Editorial	Added "http://" to URL in IA-5 References.	F-99
01-15-2014	Editorial	Added "http://" to URL in IA-7 References.	F-99
01-15-2014	Editorial	Added "http://" to URL in IA-8 References.	F-101
01-15-2014	Editorial	Changed ":" to ";" after "800-61" and added "http://" to URL in IR-6 References.	F-108
01-15-2014	Substantive	Added the following text to MP-6 (7) Supplemental Guidance: "Dual authorization may also be known as two-person control."	F-124
01-15-2014	Editorial	Added "http://" to URL in MP-6 References.	F-124
01-15-2014	Editorial	Changed "DoDI" to "DoD Instruction" and added "http://" to URLs in PE-3 References.	F-130
01-15-2014	Editorial	Deleted "and supplementation" after "tailoring" in PL-2 a. 8.	F-140
01-15-2014	Editorial	Added "Special" before "Publication" in PL-4 References.	F-141
01-15-2014	Editorial	Added "Control Enhancements: None." to PL-7.	F-142
01-15-2014	Editorial	Deleted AT-5 and AC-19 (6) (8) (9) from PL-9 Supplemental Guidance.	F-144
01-15-2014	Editorial	Added "Control Enhancements: None." to PL-9.	F-144
01-15-2014	Editorial	Added "Special" before "Publication" in PL-9 References.	F-144
01-15-2014	Editorial	Changed "731.106(a)" to "731.106" in PS-2 References.	F-145
01-15-2014	Editorial	Changed "Publication" to "Publications" and added "http://" to URL in RA-3 References.	F-153
01-15-2014	Editorial	Added "http://" to URLs in RA-5 References.	F-155
01-15-2014	Editorial	Added "http://" to URLs in SA-4 References.	F-160
01-15-2014	Substantive	Added the following text to SA-11 (8) Supplemental Guidance: "To understand the scope of dynamic code analysis and hence the assurance provided, organizations may also consider conducting code coverage analysis (checking the degree to which the code has been tested using metrics such as percent of subroutines tested or percent of program statements called during execution of the test suite) and/or concordance analysis (checking for words that are out of place in software code such as non-English language words or derogatory terms)."	F-169
01-15-2014	Editorial	Added "http://" to URLs in SA-11 References.	F-169
01-15-2014	Editorial	Added "Control Enhancements: None." to SA-16.	F-177
01-15-2014	Editorial	Changed "Training" to "Scanning" in SA-19 (4) title.	F-181
01-15-2014	Editorial	Changed "physical" to "protected" in SC-8 Supplemental Guidance.	F-193
01-15-2014	Editorial	Changed "140-2" to "140" and added "http://" to URLs in SC-13 References.	F-196
01-15-2014	Editorial	Added "authentication" after "data origin" in SC-20, Part a.	F-199
01-15-2014	Editorial	Added "verification" after "integrity" in SC-20, Part a.	F-199
01-15-2014	Editorial	Added "Control Enhancements: None." to SC-35.	F-209
01-15-2014	Editorial	Deleted extraneous "References: None" from SI-7.	F-228

DATE	TYPE	CHANGE	PAGE
01-15-2014	Substantive	Added the following text as new third paragraph in Appendix G:: "Table G-1 provides a summary of the security controls in the program management family from Appendix G. Organizations can use the recommended *priority code* designation associated with each program management control to assist in making sequencing decisions for implementation (i.e., a Priority Code 1 [P1] control has a higher priority for implementation than a Priority Code 2 [P2] control; and a Priority Code 2 [P2] control has a higher priority for implementation than a Priority Code 3 [P3] control."	G-1/2
01-15-2014	Editorial	Added Table G-1 to Appendix G.	G-2
01-15-2014	Editorial	Added "http://" to URL in PM-5 References.	G-5
01-15-2014	Editorial	Deleted "Web: www.fsam.gov" from PM-7 References.	G-5
01-15-2014	Editorial	Added "http://" to URL in Footnote 124.	J-22

CHAPTER ONE

INTRODUCTION

THE NEED TO PROTECT INFORMATION AND INFORMATION SYSTEMS

The selection and implementation of *security controls* for information systems[1] and organizations are important tasks that can have major implications on the operations[2] and assets of organizations[3] as well as the welfare of individuals and the Nation. Security controls are the safeguards/countermeasures prescribed for information systems or organizations that are designed to: (i) protect the confidentiality, integrity, and availability of information that is processed, stored, and transmitted by those systems/organizations; and (ii) satisfy a set of defined security requirements.[4] There are several key questions that should be answered by organizations when addressing the information security considerations for information systems:

- What security controls are needed to satisfy the security requirements and to adequately mitigate risk incurred by using information and information systems in the execution of organizational missions and business functions?
- Have the security controls been implemented, or is there an implementation plan in place?
- What is the desired or required level of assurance that the selected security controls, as implemented, are effective in their application? [5]

The answers to these questions are not given in isolation but rather in the context of an effective *risk management process* for the organization that identifies, mitigates as deemed necessary, and monitors on an ongoing basis, risks[6] arising from its information and information systems. NIST Special Publication 800-39 provides guidance on managing information security risk at three distinct tiers—the organization level, mission/business process level, and information system level. The security controls defined in this publication and recommended for use by organizations to satisfy their information security requirements should be employed as part of a well-defined risk management process that supports organizational information security programs.[7]

[1] An information system is a discrete set of *information resources* organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information systems also include specialized systems such as industrial/process controls systems, telephone switching/private branch exchange (PBX) systems, and environmental control systems.

[2] Organizational operations include mission, functions, image, and reputation.

[3] The term *organization* describes an entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements).

[4] Security requirements are derived from mission/business needs, laws, Executive Orders, directives, regulations, policies, instructions, standards, guidance, and/or procedures to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by organizational information systems.

[5] Security control *effectiveness* addresses the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment or enforcing/mediating established security policies.

[6] Information security-related risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and consider the potential adverse impacts to organizational operations and assets, individuals, other organizations, and the Nation.

[7] The program management controls (Appendix G) complement the security controls for an information system (Appendix F) by focusing on the organization-wide information security requirements that are independent of any particular information system and are essential for managing information security programs.

It is of paramount importance that responsible officials understand the risks and other factors that could adversely affect organizational operations and assets, individuals, other organizations, and the Nation.[8] These officials must also understand the current status of their security programs and the security controls planned or in place to protect their information and information systems in order to make informed judgments and investments that mitigate risks to an acceptable level. The ultimate objective is to conduct the day-to-day operations of the organization and accomplish the organization's stated missions and business functions with what the OMB Circular A-130 defines as *adequate security*, or security commensurate with risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

1.1 PURPOSE AND APPLICABILITY

The purpose of this publication is to provide guidelines for selecting and specifying security controls for organizations and information systems supporting the executive agencies of the federal government to meet the requirements of FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. The guidelines apply to all components[9] of an information system that process, store, or transmit federal information. The guidelines have been developed to achieve more secure information systems and effective risk management within the federal government by:

- Facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems and organizations;
- Providing a stable, yet flexible catalog of security controls to meet current information protection needs and the demands of future protection needs based on changing threats, requirements, and technologies;
- Providing a recommendation for security controls for information systems categorized in accordance with FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*;
- Creating a foundation for the development of assessment methods and procedures for determining security control effectiveness; and
- Improving communication among organizations by providing a common lexicon that supports discussion of risk management concepts.

In addition to the security controls described above, this publication: (i) provides a set of information security program management (PM) controls that are typically implemented at the organization level and not directed at individual organizational information systems; (ii) provides a set of privacy controls based on international standards and best practices that help organizations enforce privacy requirements derived from federal legislation, directives, policies, regulations, and standards; and (iii) establishes a linkage and relationship between privacy and security controls for purposes of enforcing respective privacy and security requirements which may overlap in concept and in implementation within federal information systems, programs, and organizations. Standardized privacy controls provide a more disciplined and structured approach for satisfying federal privacy requirements and demonstrating compliance to those

[8] This includes risk to critical infrastructure/key resources described in Homeland Security Presidential Directive 7.

[9] Information system components include, for example, mainframes, workstations, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), input/output devices (e.g., scanners, copiers, printers), network components (e.g., firewalls, routers, gateways, voice and data switches, process controllers, wireless access points, network appliances, sensors), operating systems, virtual machines, middleware, and applications.

requirements. Incorporating the same concepts used in managing information security risk, helps organizations implement privacy controls in a more cost-effective, risked-based manner.

The guidelines in this special publication are applicable to all federal information systems[10] other than those systems designated as national security systems as defined in 44 U.S.C., Section 3542.[11] The guidelines have been broadly developed from a technical perspective to complement similar guidelines for national security systems and may be used for such systems with the approval of appropriate federal officials exercising policy authority over such systems.[12] State, local, and tribal governments, as well as private sector organizations are encouraged to consider using these guidelines, as appropriate.

1.2 TARGET AUDIENCE

This publication is intended to serve a diverse audience of information system and information security professionals including:

- Individuals with information system, security, and/or risk management and oversight responsibilities (e.g., authorizing officials, chief information officers, senior information security officers,[13] information system managers, information security managers);
- Individuals with information system development responsibilities (e.g., program managers, system designers and developers, information security engineers, systems integrators);
- Individuals with information security implementation and operational responsibilities (e.g., mission/business owners, information system owners, common control providers, information owners/stewards, system administrators, information system security officers);
- Individuals with information security assessment and monitoring responsibilities (e.g., auditors, Inspectors General, system evaluators, assessors, independent verifiers/validators, analysts, information system owners); and
- Commercial companies producing information technology products and systems, creating information security-related technologies, or providing information security services.

1.3 RELATIONSHIP TO OTHER SECURITY CONTROL PUBLICATIONS

To create a technically sound and broadly applicable set of security controls for information systems and organizations, a variety of sources were considered during the development of this special publication. The sources included security controls from the defense, audit, financial, healthcare, industrial/process control, and intelligence communities as well as controls defined by

[10] A *federal information system* is an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

[11] A *national security system* is any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency: (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, e.g., payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

[12] CNSS Instruction 1253 provides implementing guidance for *national security systems*.

[13] At the *agency* level, this position is known as the Senior Agency Information Security Officer. Organizations may also refer to this position as the *Senior Information Security Officer* or the *Chief Information Security Officer*.

national and international standards organizations. The objective of NIST Special Publication 800-53 is to provide a set of security controls that can satisfy the breadth and depth of security requirements[14] levied on organizations, mission/business processes, and information systems and that is consistent with and complementary to other established information security standards.

The catalog of security controls in Special Publication 800-53 can be effectively used to protect information and information systems from traditional and advanced persistent threats in varied operational, environmental, and technical scenarios. The controls can also be used to demonstrate compliance with a variety of governmental, organizational, or institutional security requirements. Organizations have the responsibility to select the appropriate security controls, to implement the controls correctly, and to demonstrate the effectiveness of the controls in satisfying established security requirements.[15] The security controls facilitate the development of assessment methods and procedures that can be used to demonstrate control effectiveness in a consistent/repeatable manner—thus contributing to the organization's confidence that security requirements continue to be satisfied on an ongoing basis. In addition, security controls can be used in developing *overlays* for specialized information systems, information technologies, environments of operation, or communities of interest (see Appendix I).

1.4 ORGANIZATIONAL RESPONSIBILITIES

Organizations use FIPS Publication 199 to categorize their information and information systems. Security categorization is accomplished as an organization-wide activity[16] with the involvement of senior-level organizational personnel including, for example, authorizing officials, chief information officers, senior information security officers, information owners and/or stewards, information system owners, and risk executive (function).[17] Information is categorized at Tier 1 (organization level) and at Tier 2 (mission/business process level). In accordance with FIPS Publication 200, organizations use the security categorization results from Tiers 1 and 2 to designate organizational information systems at Tier 3 (information system level) as low-impact, moderate-impact, or high-impact systems. For each organizational information system at Tier 3, the recommendation for security controls from the *baseline* controls defined in Appendix D is the starting point for the security control *tailoring* process. While the security control selection process is generally focused on information systems at Tier 3, the process is generally applicable across all three tiers of risk management.

FIPS Publication 199 security categorization associates information and the operation and use of information systems with the potential worst-case adverse impact on organizational operations and assets, individuals, other organizations, and the Nation.[18] Organizational assessments of risk, including the use of specific and credible threat information, vulnerability information, and the likelihood of such threats exploiting vulnerabilities to cause adverse impacts, guide and inform

[14] Security requirements are those requirements levied on an information system that are derived from laws, Executive Orders, directives, policies, instructions, regulations, standards, guidelines, or organizational (mission) needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

[15] NIST Special Publication 800-53A provides guidance on assessing the effectiveness of security controls.

[16] See FIPS Publication 200, Footnote 7.

[17] Organizations typically exercise managerial, operational, and financial control over their information systems and the security provided to those systems, including the authority and capability to implement or require the security controls deemed necessary to protect organizational operations and assets, individuals, other organizations, and the Nation.

[18] Considerations for potential national-level impacts and impacts to other organizations in categorizing organizational information systems derive from the USA PATRIOT Act and Homeland Security Presidential Directives (HSPDs).

the tailoring process and the final selection of security controls.[19] The final, agreed-upon set of security controls addressing specific organizational mission/business needs and tolerance for risk is documented with appropriate rationale in the security plan for the information system.[20] The use of security controls from Special Publication 800-53 (including the baseline controls as a starting point in the control selection process), facilitates a more consistent level of security for federal information systems and organizations, while simultaneously preserving the flexibility and agility organizations need to address an increasingly sophisticated and hostile threat space, specific organizational missions/business functions, rapidly changing technologies, and in some cases, unique environments of operation.

Achieving adequate information security for organizations, mission/business processes, and information systems is a multifaceted undertaking that requires:

- Clearly articulated security requirements and security specifications;
- Well-designed and well-built information technology products based on state-of-the-practice hardware, firmware, and software development processes;
- Sound systems/security engineering principles and practices to effectively integrate information technology products into organizational information systems;
- Sound security practices that are well documented and seamlessly integrated into the training requirements and daily routines of organizational personnel with security responsibilities;
- Continuous monitoring of organizations and information systems to determine the ongoing effectiveness of deployed security controls, changes in information systems and environments of operation, and compliance with legislation, directives, policies, and standards;[21] and
- Information security planning and system development life cycle management.[22]

From an engineering viewpoint, information security is just one of many required operational capabilities for information systems that support organizational mission/business processes—capabilities that must be funded by organizations throughout the system development life cycle in order to achieve mission/business success. It is important that organizations *realistically* assess the risk to organizational operations and assets, individuals, other organizations, and the Nation arising from mission/business processes and by placing information systems into operation or continuing operations. Realistic assessment of risk requires an understanding of threats to and vulnerabilities within organizations and the likelihood and potential adverse impacts of successful exploitations of such vulnerabilities by those threats.[23] Finally, information security requirements must be satisfied with the full knowledge and consideration of the risk management strategy of

[19] Risk assessments can be accomplished in a variety of ways depending on the specific needs of organizations. NIST Special Publication 800-30 provides guidance on the assessment of risk as part of an overall risk management process.

[20] Authorizing officials or designated representatives, by accepting the completed security plans, agree to the set of security controls proposed to meet the security requirements for organizations (including mission/business processes) and/or designated information systems.

[21] NIST Special Publication 800-137 provides guidance on continuous monitoring of organizational information systems and environments of operation.

[22] NIST Special Publication 800-64 provides guidance on the information security considerations in the system development life cycle.

[23] NIST Special Publication 800-30 provides guidance on the risk assessment process.

the organization, in light of the potential cost, schedule, and performance issues associated with the acquisition, deployment, and operation of organizational information systems.[24]

1.5 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- **Chapter Two** describes the fundamental concepts associated with security control selection and specification including: (i) multitiered risk management; (ii) the structure of security controls and how the controls are organized into families; (iii) security control baselines as starting points for the tailoring process; (iv) the use of common controls and inheritance of security capabilities; (v) external environments and service providers; (vi) assurance and trustworthiness; and (vii) revisions and extensions to security controls and control baselines.
- **Chapter Three** describes the process of selecting and specifying security controls for organizational information systems including: (i) selecting appropriate security control baselines; (ii) tailoring the baseline controls including developing specialized overlays; (iii) documenting the security control selection process; and (iv) applying the selection process to new and legacy systems.
- **Supporting appendices** provide essential security control selection and specification-related information including: (i) general references; [25] (ii) definitions and terms; (iii) acronyms; (iv) baseline security controls for low-impact, moderate-impact, and high-impact information systems; (v) guidance on assurance and trustworthiness in information systems; (vi) a catalog of security controls;[26] (vii) a catalog of information security program management controls; (viii) mappings to international information security standards; (ix) guidance for developing overlays by organizations or communities of interest; and (x) a catalog of privacy controls.

[24] In addition to information security requirements, organizations must also address privacy requirements that derive from federal legislation and policies. Organizations can employ the privacy controls in Appendix J in conjunction with the security controls in Appendix F to achieve comprehensive security and privacy protection.

[25] Unless otherwise stated, all references to NIST publications in this document (i.e., Federal Information Processing Standards and Special Publications) are to the most recent version of the publication.

[26] The security controls in Special Publication 800-53 are available online and can be downloaded in various formats from the NIST web site at: http://web.nvd.nist.gov/view/800-53/home.

CHAPTER TWO

THE FUNDAMENTALS

SECURITY CONTROL STRUCTURE, ORGANIZATION, BASELINES, AND ASSURANCE

This chapter presents the fundamental concepts associated with security control selection and specification including: (i) three-tiered risk management; (ii) the structure of security controls and the organization of the controls in the control catalog; (iii) security control baselines; (iv) the identification and use of common security controls; (v) security controls in external environments; (vi) security control assurance; and (vii) future revisions to the security controls, the control catalog, and baseline controls.

2.1 MULTITIERED RISK MANAGEMENT

The selection and specification of security controls for an information system is accomplished as part of an organization-wide information security program for the management of risk—that is, the risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation of information systems. Risk-based approaches to security control selection and specification consider effectiveness, efficiency, and constraints due to applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines. To integrate the risk management process throughout the organization and more effectively address mission/business concerns, a three-tiered approach is employed that addresses risk at the: (i) *organization* level; (ii) *mission/business process* level; and (iii) *information system* level. The risk management process is carried out across the three tiers with the overall objective of continuous improvement in the organization's risk-related activities and effective inter-tier and intra-tier communication among all stakeholders having a shared interest in the mission/business success of the organization. Figure 1 illustrates the three-tiered approach to risk management.

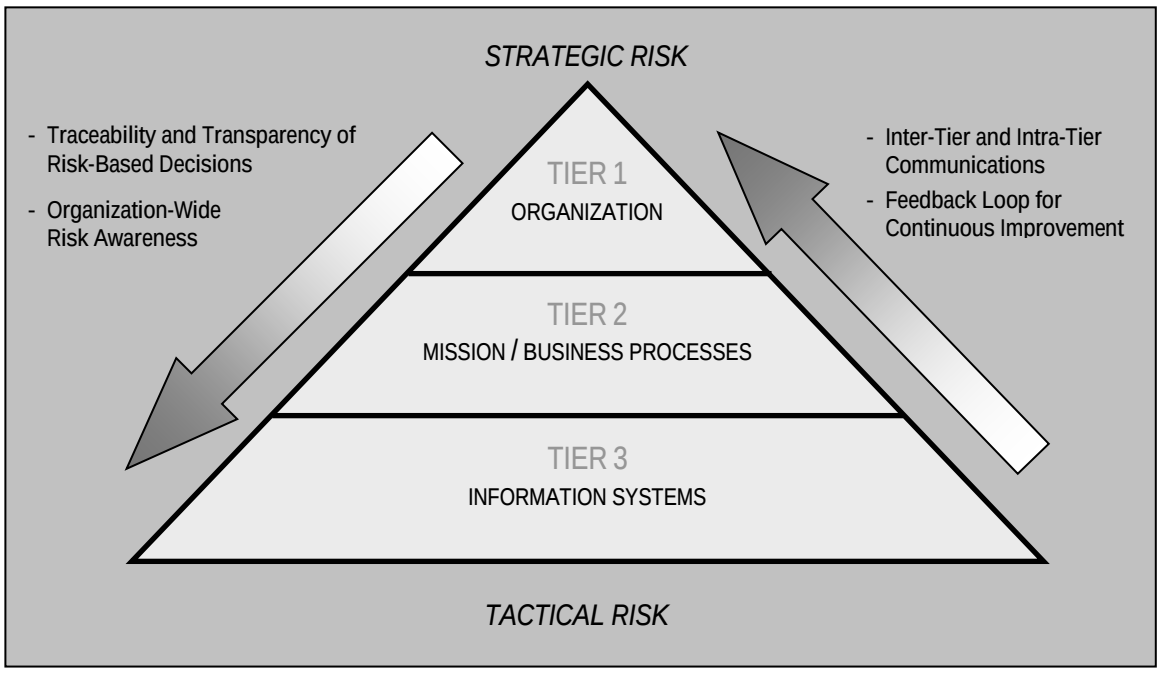


FIGURE 1: THREE-TIERED RISK MANAGEMENT APPROACH

Tier 1 provides a prioritization of organizational missions/business functions which in turn drives investment strategies and funding decisions—promoting cost-effective, efficient information technology solutions consistent with the strategic goals and objectives of the organization and measures of performance. Tier 2 includes: (i) defining the mission/business processes needed to support the organizational missions/business functions; (ii) determining the security categories of the information systems needed to execute the mission/business processes; (iii) incorporating information security requirements into the mission/business processes; and (iv) establishing an enterprise architecture (including an embedded information security architecture) to facilitate the allocation of security controls to organizational information systems and the environments in which those systems operate. The Risk Management Framework (RMF), depicted in Figure 2, is the primary means for addressing risk at Tier 3.[27] This publication focuses on Step 2 of the RMF, the security control selection process, in the context of the three tiers in the organizational risk management hierarchy.

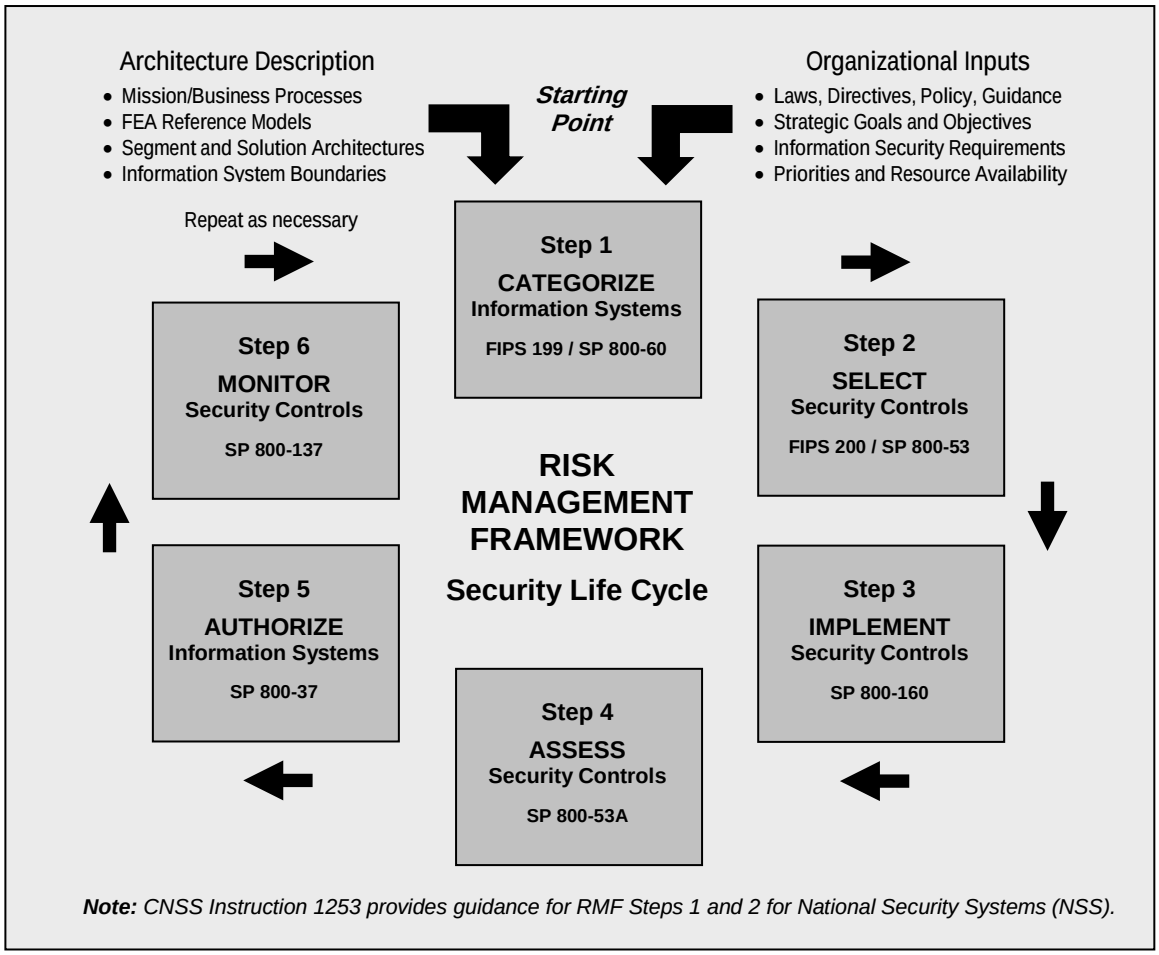


FIGURE 2: RISK MANAGEMENT FRAMEWORK

The RMF addresses the security concerns of organizations related to the design, development, implementation, operation, and disposal of information systems and the environments in which those systems operate. The RMF consists of the following six steps:

[27] NIST Special Publication 800-37 provides guidance on the implementation of the Risk Management Framework. A complete listing of all publications supporting the RMF and referenced in Figure 2 is provided in Appendix A.

Step 1: *Categorize* the information system based on a FIPS Publication 199 impact assessment;[28]

Step 2: *Select* the applicable security control baseline based on the results of the security categorization and apply tailoring guidance (including the potential use of overlays);

Step 3: *Implement* the security controls and document the design, development, and implementation details for the controls;

Step 4: *Assess* the security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system;[29]

Step 5: *Authorize* information system operation based on a determination of risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation and use of the information system and the decision that this risk is acceptable; and

Step 6: *Monitor* the security controls in the information system and environment of operation on an ongoing basis to determine control effectiveness, changes to the system/environment, and compliance to legislation, Executive Orders, directives, policies, regulations, and standards.

2.2 SECURITY CONTROL STRUCTURE

Security controls described in this publication have a well-defined organization and structure. For ease of use in the security control selection and specification process, controls are organized into eighteen *families*.[30] Each family contains security controls related to the general security topic of the family. A two-character identifier uniquely identifies security control families, for example, PS (Personnel Security). Security controls may involve aspects of policy, oversight, supervision, manual processes, actions by individuals, or automated mechanisms implemented by information systems/devices. Table 1 lists the security control families and the associated family identifiers in the security control catalog.[31]

TABLE 1: SECURITY CONTROL IDENTIFIERS AND FAMILY NAMES

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

[28] CNSS Instruction 1253 provides security categorization guidance for national security systems.

[29] NIST Special Publication 800-53A provides guidance on assessing the effectiveness of security controls.

[30] Of the eighteen security control families in NIST Special Publication 800-53, seventeen families are described in the security control catalog in Appendix F, and are closely aligned with the seventeen minimum security requirements for federal information and information systems in FIPS Publication 200. One additional family (Program Management [PM] family) provides controls for information security programs required by FISMA. This family, while not specifically referenced in FIPS Publication 200, provides security controls at the organization level rather than the information system level. See Appendix G for a description of and implementation guidance for the PM controls.

[31] *Privacy controls* listed in Appendix J, have an organization and structure similar to security controls, including the use of two-character identifiers for the eight privacy families.

The security control structure consists of the following components: (i) a *control* section; (ii) a *supplemental guidance* section; (iii) a *control enhancements* section; (iv) a *references* section; and (v) a *priority* and *baseline allocation* section. The following example from the Auditing and Accountability family illustrates the structure of a typical security control.

AU-3 CONTENT OF AUDIT RECORDS

Control: The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Supplemental Guidance: Audit record content that may be necessary to satisfy the requirement of this control includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the information system after the event occurred). Related controls: AU-2, AU-8, AU-12, SI-11.

Control Enhancements:

(1) *CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION*

The information system generates audit records containing the following additional information: [*Assignment: organization-defined additional, more detailed information*].

Supplemental Guidance: Detailed information that organizations may consider in audit records includes, for example, full-text recording of privileged commands or the individual identities of group account users. Organizations consider limiting the additional audit information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest.

(2) *CONTENT OF AUDIT RECORDS | CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT*

The information system provides centralized management and configuration of the content to be captured in audit records generated by [*Assignment: organization-defined information system components*].

Supplemental Guidance: This control enhancement requires that the content to be captured in audit records be configured from a central location (necessitating automation). Organizations coordinate the selection of required audit content to support the centralized management and configuration capability provided by the information system. Related controls: AU-6, AU-7.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AU-3	**MOD** AU-3 (1)	**HIGH** AU-3 (1) (2)

The control section prescribes specific security-related activities or actions to be carried out by organizations or by information systems. The term *information system* refers to those functions that generally involve the implementation of information technology (e.g., hardware, software, and firmware). Conversely, the term *organization* refers to activities that are generally process-driven or entity-driven—that is, the security control is generally implemented through human or procedural-based actions. Security controls that use the term organization may still require some degree of automation to be fulfilled. Similarly, security controls that use the term information system may have some elements that are process-driven or entity-driven. Using the terms organization and/or information system does not preclude the application of security controls at any of the tiers in the risk management hierarchy (i.e., organization level, mission/business process level, information system level), as appropriate.

For some security controls in the control catalog, a degree of flexibility is provided by allowing organizations to define values for certain parameters associated with the controls. This flexibility is achieved through the use of *assignment* and *selection* statements embedded within the security controls and control enhancements. Assignment and selection statements provide organizations with the capability to tailor security controls and control enhancements based on: (i) security requirements to support organizational missions/business functions and operational needs; (ii) risk assessments and organizational risk tolerance; and (iii) security requirements originating in federal laws, Executive Orders, directives, policies, regulations, standards, or guidelines.[32]

For example, organizations can specify additional information needed for audit records to support audit event processing. See the AU-3 (1) example above (i.e., [*Assignment: organization-defined additional, more detailed information*]). These assignments may include particular actions to be taken by information systems in the event of audit failures, the frequency of conducting system backups, restrictions on password use, or the distribution list for organizational policies and procedures.[33] Once specified,[34] the organization-defined values for assignment and selection statements become part of the security control, and the control implementation is assessed against the completed control statement. Assignment statements offer a high degree of flexibility by allowing organizations to specify parameter values, without requiring those values to be one of two or more specific predefined choices. In contrast, selection statements narrow the potential input values by providing a specific list of items from which organizations must choose.[35]

The supplemental guidance section provides non-prescriptive, additional information for a specific security control. Organizations can apply the supplemental guidance as appropriate, when defining, developing, and/or implementing security controls. The supplemental guidance can provide important considerations for implementing security controls in the context of operational environments, mission/business requirements, or assessments of risk and can also explain the purpose or meaning of particular controls. Security control enhancements may also contain supplemental guidance when the guidance is not applicable to the entire control but instead focused on a particular control enhancement. The supplemental guidance sections for security controls and control enhancements may contain a list of *related controls*. Related controls: (i) directly impact or support the implementation of a particular security control or control enhancement; (ii) address a closely related *security capability*; or (iii) are referenced in the supplemental guidance. Security control enhancements are by definition related to the base control. Related controls that are listed in the supplemental guidance for the base controls are not repeated in the supplemental guidance for the control enhancements. However, there may be related controls identified for control enhancements that are not listed in the base control.

The security control enhancements section provides statements of security capability to: (i) add functionality/specificity to a control; and/or (ii) increase the strength of a control. In both cases, control enhancements are used in information systems and environments of operation requiring

[32] In general, organization-defined *parameters* used in assignment and selection statements in the basic security controls apply also to all control enhancements associated with those controls.

[33] Organizations determine whether specific assignment or selection statements are completed at Tier 1 (organization level), Tier 2 (mission/business process level), Tier 3 (information system level), or a combination thereof.

[34] Organizations may choose to define specific values for security control parameters in policies, procedures, or guidance (which may be applicable to more than one information system) referencing the source documents in the security plan in lieu of explicitly completing the assignment/selection statements within the control as part of the plan.

[35] Security controls are generally designed to be *technology*- and *implementation*-independent, and therefore do not contain specific requirements in these areas. Organizations provide such requirements as deemed necessary in the security plan for the information system.

greater protection than provided by the base control due to the potential adverse organizational impacts or when organizations seek additions to the base control functionality/specificity based on organizational assessments of risk. Security control enhancements are numbered sequentially within each control so that the enhancements can be easily identified when selected to supplement the base control. Each security control enhancement has a short subtitle to indicate the intended security capability provided by the control enhancement. In the AU-3 example, if the first control enhancement is selected, the control designation becomes AU-3 (1). The numerical designation of a control enhancement is used only to identify the particular enhancement within the control. The designation is not indicative of either the strength of the control enhancement or any hierarchical relationship among the enhancements. Control enhancements are not intended to be selected independently (i.e., if a control enhancement is selected, then the corresponding base security control must also be selected). This intent is reflected in the baseline specifications in Appendix D and in the baseline allocation section under each control in Appendix F.

The references section includes a list of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines (e.g., OMB Circulars/Memoranda, Homeland Security Presidential Directives, FIPS Publications, and NIST Special Publications) that are relevant to a particular security control.[36] The references provide federal legislative and policy mandates as well as supporting information for the implementation of security controls and control enhancements. The references section also contains pertinent websites for organizations to use in obtaining additional information for security control implementation and assessment.

The priority and security control baseline allocation section provides: (i) the recommended priority codes used for sequencing decisions during security control implementation; and (ii) the initial allocation of security controls and control enhancements to the baselines. Organizations can use the *priority code* designation associated with each security control to assist in making sequencing decisions for control implementation (i.e., a Priority Code 1 [P1] control has a higher priority for implementation than a Priority Code 2 [P2] control, a Priority Code 2 [P2] control has a higher priority for implementation than a Priority Code 3 [P3] control, and a Priority Code 0 [P0] indicates the security control is not selected in any baseline). This recommended sequencing prioritization helps to ensure that the foundational security controls upon which other controls depend are implemented first, thus enabling organizations to deploy controls in a more structured and timely manner in accordance with available resources. The implementation of security controls by sequence priority code does not imply the achievement of any defined level of risk mitigation until *all* of the security controls in the security plan have been implemented. The priority codes are intended only for implementation sequencing, not for making security control selection decisions.

2.3 SECURITY CONTROL BASELINES

Organizations are required to adequately mitigate the risk arising from use of information and information systems in the execution of missions and business functions. A significant challenge for organizations is to determine the most cost-effective, appropriate set of security controls, which if implemented and determined to be effective, would mitigate risk while complying with security requirements defined by applicable federal laws, Executive Orders, regulations, policies, directives, or standards (e.g., FISMA, OMB Circular A-130, HSPD-12, FIPS Publication 200). There is no one correct set of security controls that addresses all organizational security concerns in all situations. Selecting the most appropriate set of security controls for a specific situation or

[36] Publications listed in the *references section* refer to the most recent versions of the publications. References are provided to assist organizations in applying the security controls and are not intended to be inclusive or complete.

information system to adequately mitigate risk is an important task that requires a fundamental understanding of organizational mission/business priorities, the mission and business functions the information systems will support, and the environments of operation where the systems will reside. With that understanding, organizations can demonstrate how to most effectively assure the confidentiality, integrity, and availability of organizational information and information systems in a manner that supports mission/business needs while demonstrating due diligence. Selecting, implementing, and maintaining an appropriate set of security controls to adequately protect the information systems employed by organizations requires strong collaboration with system owners to understand ongoing changes to missions/business functions, environments of operation, and how the systems are used.

To assist organizations in making the appropriate selection of security controls for information systems, the concept of *baseline* controls is introduced. Baseline controls are the starting point for the security control selection process described in this document and are chosen based on the security category and associated impact level of information systems determined in accordance with FIPS Publication 199 and FIPS Publication 200, respectively.[37] Appendix D provides a listing of the security control baselines. Three security control baselines have been identified corresponding to the low-impact, moderate-impact, and high-impact information systems using the high water mark defined in FIPS Publication 200 and used in Section 3.1 of this document to provide an initial set of security controls for each impact level.[38]

Appendix F provides a comprehensive catalog of security controls for information systems and organizations, arranged by control families. Chapter Three provides additional information on how to use FIPS Publication 199 security categories and FIPS Publication 200 system impact levels in applying the tailoring guidance to the baseline security controls to achieve adequate risk mitigation. Tailoring guidance, described in Section 3.2, helps organizations to customize the security control baselines selected using the results from organizational assessments of risk. Baseline tailoring actions include: (i) identifying and designating common controls; (ii) applying scoping considerations; (iii) selecting compensating controls; (iv) assigning specific values to security control parameters; (v) supplementing initial baselines with additional security controls or control enhancements; and (vi) providing additional information for control implementation.

Implementation Tip

There are security controls and control enhancements that appear in the security control catalog (Appendix F) that are found in only higher-impact baselines or are not used in any of the baselines. These additional security controls and control enhancements for information systems are available to organizations and can be used in tailoring security control baselines to achieve the needed level of protection in accordance with organizational assessments of risk. The set of security controls in the security plan must be sufficient to adequately mitigate risks to organizational operations and assets, individuals, other organizations, and the Nation based on the organizational risk tolerance.

[37] CNSS Instruction 1253 provides guidance on security control baselines for national security systems.

[38] The baseline security controls contained in Appendix D are not necessarily absolutes in that the guidance described in Section 3.2 provides organizations with the ability to tailor controls in accordance with the terms and conditions established by their authorizing officials and documented in their respective security plans.

2.4 SECURITY CONTROL DESIGNATIONS

There are three distinct types of designations related to the security controls in Appendix F that define: (i) the scope of applicability for the control; (ii) the shared nature of the control; and (iii) the responsibility for control development, implementation, assessment, and authorization. These designations include *common* controls, *system-specific* controls, and *hybrid* controls.

Common controls are security controls whose implementation results in a security capability that is *inheritable* by one or more organizational information systems. Security controls are deemed inheritable by information systems or information system components when the systems or components receive protection from the implemented controls but the controls are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the systems or components—entities internal or external to the organizations where the systems or components reside. Security capabilities provided by common controls can be inherited from many sources including, for example, organizations, organizational mission/business lines, sites, enclaves, environments of operation, or other information systems. Many of the controls needed to protect organizational information systems (e.g., security awareness training, incident response plans, physical access to facilities, rules of behavior) are excellent candidates for common control status. In addition, there can also be a variety of technology-based common controls (e.g., Public Key Infrastructure [PKI], authorized secure standard configurations for clients/servers, access control systems, boundary protection, cross-domain solutions). By centrally managing and documenting the development, implementation, assessment, authorization, and monitoring of common controls, security costs can be amortized across multiple information systems.

The organization assigns responsibility for common controls to appropriate organizational officials (i.e., common control providers) and coordinates the development, implementation, assessment, authorization, and monitoring of the controls.[39] The identification of common controls is most effectively accomplished as an organization-wide exercise with the active involvement of chief information officers, senior information security officers, the risk executive (function), authorizing officials, information owners/stewards, information system owners, and information system security officers. The organization-wide exercise considers the security categories of the information systems within the organization and the security controls necessary to adequately mitigate the risks arising from the use of those systems (see *baseline* security controls in Section 2.3).[40] Common control identification for the controls that impact multiple information systems, but not all systems across the organization could benefit from taking a similar approach. Key stakeholders collaborate to identify opportunities to effectively employ common controls at the mission/business line, site, or enclave level.

When common controls protect multiple organizational information systems of differing impact levels, the controls are implemented with regard to the highest impact level among the systems. If the common controls are not implemented at the highest impact level of the information systems, system owners will need to factor this situation into their assessments of risk and take appropriate risk mitigation actions (e.g., adding security controls or control enhancements, changing assigned values of security control parameters, implementing compensating controls, or changing certain aspects of mission/business processes). Implementing common controls that are less than

[39] The Chief Information Officer, Senior Information Security Officer, or other designated organizational officials at the senior leadership level assign responsibility for the development, implementation, assessment, authorization, and monitoring of common controls to appropriate entities (either internal or external to the organization).

[40] Each common control identified by the organization is reviewed for applicability to each specific organizational information system, typically by information system owners and authorizing officials.

effective or that provide insufficient security capability for higher-impact information systems can have a significant adverse impact on organizational missions or business functions.

Common controls are generally documented in the organization-wide *information security program plan* unless implemented as part of a specific information system, in which case the controls are documented in the security plan for that system.[41] Organizations have the flexibility to describe common controls in a single document or in multiple documents with references or pointers, as appropriate. In the case of multiple documents, the documents describing common controls are included as attachments to the information security program plan. If the information security program plan contains multiple documents, organizations specify in each document the organizational officials responsible for development, implementation, assessment, authorization, and monitoring of the respective common controls. For example, the organization may require that the Facilities Management Office develop, implement, assess, authorize, and continuously monitor physical and environmental protection controls from the PE family when such controls are not associated with a particular information system but instead, support multiple systems. When common controls are included in a separate security plan for an information system (e.g., security controls employed as part of an intrusion detection system providing boundary protection inherited by one or more organizational information systems), the information security program plan indicates which separate security plan contains a description of the common controls.

Implementation Tip

The selection of common controls is most effectively accomplished on an organization-wide basis with the involvement of senior leadership (i.e., mission/business owners, authorizing officials, chief information officers, senior information security officers, information system owners, information owners/stewards, risk executives). These individuals have the collective knowledge to understand organizational priorities, the importance of organizational operations and assets, and the importance of the information systems that support those operations/assets. The senior leaders are also in the best position to select the common controls for each security control baseline and assign specific responsibilities for developing, implementing, assessing, authorizing, and monitoring those controls.

Common controls, whether employed in organizational information systems or environments of operation, are authorized by senior officials with at least the same level of authority/responsibility for managing risk as the authorization officials for information systems inheriting the controls. Authorization results for common controls are shared with the appropriate information system owners and authorizing officials. A plan of action and milestones is developed and maintained for common controls that have been determined through independent assessments, to be less than effective. Information system owners dependent on common controls that are less than effective consider whether they are willing to accept the associated risk or if additional tailoring is required to address the weaknesses or deficiencies in the controls. Such risk-based decisions are influenced by available resources, the trust models employed by the organization, and the risk tolerance of authorizing officials and the organization.[42]

[41] Information security program plans are described in Appendix G. Organizations ensure that any security capabilities provided by common controls (i.e., security capabilities inheritable by other organizational entities) are described in sufficient detail to facilitate adequate understanding of the control implementation by inheriting entities.

[42] NIST Special Publication 800-39 provides guidance on trust models, including validated, direct historical, mediated, and mandated trust models.

Common controls are subject to the same assessment and monitoring requirements as system-specific controls employed in individual organizational information systems. Because common controls impact more than one system, a higher degree of confidence regarding the effectiveness of those controls may be required.

Security controls not designated as common controls are considered *system-specific* or *hybrid* controls. System-specific controls are the primary responsibility of information system owners and their respective authorizing officials. Organizations assign a *hybrid* status to security controls when one part of the control is common and another part of the control is system-specific. For example, an organization may choose to implement the Incident Response Policy and Procedures security control (IR-1) as a hybrid control with the policy portion of the control designated as common and the procedures portion of the control designated as system-specific. Hybrid controls may also serve as predefined templates for further control refinement. Organizations may choose, for example, to implement the Contingency Planning security control (CP-2) as a predefined template for a generalized contingency plan for all organizational information systems with information system owners tailoring the plan, where appropriate, for system-specific uses.

Partitioning security controls into common, hybrid, and system-specific controls can result in significant savings to organizations in implementation and assessment costs as well as a more consistent application of security controls organization-wide. While security control partitioning into common, hybrid, and system-specific controls is straightforward and intuitive conceptually, the actual application takes a significant amount of planning and coordination. At the information system level, determination of common, hybrid, or system-specific security controls follows the development of a tailored baseline. It is necessary to first determine what security capability is needed before organizations assign responsibility for how security controls are implemented, operated, and maintained.

Security plans for individual information systems identify which security controls required for those systems have been designated by organizations as common controls and which controls have been designated as system-specific or hybrid controls. Information system owners are responsible for any system-specific implementation details associated with common controls. These implementation details are identified and described in the security plans for the individual information systems. Senior information security officers for organizations coordinate with *common control providers* (e.g., facility/site managers, human resources managers, intrusion detection system owners) to ensure that the required controls are developed, implemented, and assessed for effectiveness. Collectively, the security plans for individual information systems and the organization-wide information security program plans provide complete coverage for all security controls employed within organizations.

The determination as to whether a security control is a common, hybrid, or system-specific is context-based. Security controls cannot be determined to be common, hybrid, or system-specific simply based on reviewing the language of the control. For example, a control may be system-specific for a particular information system, but at the same time that control could be a common control for another system, which would inherit the control from the first system. One indicator of whether a system-specific control may also be a common control for other information systems is to consider who or what depends on the functionality of that particular control. If a certain part of an information system or solution external to the system boundary depends on the control, then that control may be a candidate for common control identification.

Implementation Tip

- Organizations consider the *inherited risk* from the use of common controls. Security plans, security assessment reports, and plans of action and milestones for common controls (or a summary of such information) are made available to information system owners (for systems *inheriting* the controls) after the information is reviewed and approved by the senior official or executive responsible and accountable for the controls.
- Organizations ensure that common control providers keep control status information current since the controls typically support multiple organizational information systems. Security plans, security assessment reports, and plans of action and milestones for common controls are used by authorizing officials to make risk-based decisions in the security authorization process for their information systems and therefore, inherited risk from common controls is a significant factor in such risk-based decisions.
- Organizations ensure that common control providers have the capability to rapidly broadcast changes in the status of common controls that adversely affect the protections being provided by and expected of the common controls. Common control providers inform system owners when problems arise in the inherited common controls (e.g., when an assessment or reassessment of a common control indicates the control is flawed or deficient in some manner, or when a new threat or attack method arises that renders the common control less than effective in protecting against the new threat or attack method).
- Organizations are encouraged to employ automated management systems to maintain records of the specific common controls employed in each organizational information system to enhance the ability of common control providers to rapidly communicate with system owners.
- If common controls are provided to organizations by entities *external* to the organization (e.g., shared and/or external service providers), arrangements are made with the external/shared service providers by the organization to obtain information on the effectiveness of the deployed controls. Information obtained from external organizations regarding effectiveness of common controls is factored into authorization decisions.

2.5 EXTERNAL SERVICE PROVIDERS

Organizations are becoming increasingly reliant on information system services provided by external providers to conduct important missions and business functions. External information system services are computing and information technology services implemented outside of the traditional security authorization boundaries established by organizations for their information systems. Those traditional authorization boundaries linked to physical space and control of assets, are being extended (both physically and logically) with the growing use of external services. In this context, external services can be provided by: (i) entities within the organization but outside of the security authorization boundaries established for organizational information systems; (ii) entities outside of the organization either in the public sector (e.g., federal agencies) or private sector (e.g., commercial service providers); or (iii) some combination of the public and private sector options. External information system services include, for example, the use of service-oriented architectures (SOAs), cloud-based services (infrastructure, platform, software), or data center operations. External information system services may be used by, but are typically not part of, organizational information systems. In some situations, external information system services may completely replace or heavily augment the routine functionality of internal organizational information systems.

FISMA and OMB policies require that federal agencies using external service providers to process, store, or transmit federal information or operate information systems on behalf of the

federal government, assure that such use meets the same security requirements that federal agencies are required to meet. Security requirements for external service providers including the security controls for external information systems are expressed in contracts or other formal agreements.[43] Organizations are responsible and accountable for the information security risk incurred by the use of information system services provided by external providers. Such risk is addressed by incorporating the Risk Management Framework (RMF) as part of the terms and conditions of the contracts with external providers. Organizations can require external providers to implement all steps in the RMF except the security authorization step, which remains an inherent federal responsibility directly linked to managing the information security risk related to the use of external information system services.[44] Organizations can also require external providers to provide appropriate evidence to demonstrate that they have complied with the RMF in protecting federal information. However, federal agencies take direct responsibility for the overall security of such services by authorizing the information systems providing the services.

Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements, service-level agreements), licensing agreements, and/or supply chain exchanges. The growing use of external service providers and new relationships being forged with those providers present new and difficult challenges for organizations, especially in the area of information system security. These challenges include:

- Defining the types of external information system services provided to organizations;
- Describing how those external services are protected in accordance with the information security requirements of organizations; and
- Obtaining the necessary assurances that the risk to organizational operations and assets, individuals, other organizations, and the Nation arising from the use of the external services is acceptable.

The degree of confidence that the risk from using external services is at an acceptable level depends on the trust that organizations place in external service providers. In some cases, the level of trust is based on the amount of direct control organizations are able to exert on external service providers with regard to employment of security controls necessary for the protection of the service/information and the evidence brought forth as to the effectiveness of those controls.[45] The level of control is usually established by the terms and conditions of the contracts or service-level agreements with the external service providers and can range from extensive control (e.g., negotiating contracts or agreements that specify detailed security requirements for the providers) to very limited control (e.g., using contracts or service-level agreements to obtain commodity

[43] Organizations consult the Federal Risk and Authorization Management Program (FedRAMP) when acquiring cloud services from external providers. FedRAMP addresses required security controls and independent assessments for a variety of cloud services. Additional information is available at http://www.fedramp.gov.

[44] To effectively manage information security risk, organizations *authorize* information systems of external providers that are part of the information technologies or services (e.g., infrastructure, platform, or software) provided to the federal government. Security authorization requirements are expressed in the terms and conditions of contracts with external providers of those information technologies and services.

[45] The level of trust that organizations place in external service providers can vary widely, ranging from those who are highly trusted (e.g., business partners in a joint venture that share a common business model and common goals) to those who are less trusted and represent greater sources of risk (e.g., business partners in one endeavor who are also competitors in another market sector). NIST Special Publication 800-39 describes different trust models that can be employed by organizations when establishing relationships with external service providers.

services such as commercial telecommunications services).[46] In other cases, levels of trust are based on factors that convince organizations that required security controls have been employed and that determinations of control effectiveness exist. For example, separately authorized external information system services provided to organizations through well-established lines of business relationships may provide degrees of trust in such services within the tolerable risk range of the authorizing officials and organizations using the services.

The provision of services by external providers may result in certain services without explicit agreements between organizations and the providers. Whenever explicit agreements are feasible and practical (e.g., through contracts, service-level agreements), organizations develop such agreements and require the use of the security controls in Appendix F of this publication. When organizations are not in a position to require explicit agreements with external service providers (e.g., services are imposed on organizations, services are commodity services), organizations establish and document explicit assumptions about service capabilities with regard to security. In situations where organizations are procuring information system services through centralized acquisition vehicles (e.g., governmentwide contracts by the General Services Administration or other preferred and/or mandatory acquisition organizations), it may be more efficient and cost-effective for contract originators to establish and maintain stated levels of trust with external service providers (including the definition of required security controls and level of assurance with regard to the provision of such controls). Organizations subsequently acquiring information system services from centralized contracts can take advantage of the negotiated levels of trust established by the procurement originators and thus avoid costly repetition of activities necessary to establish such trust.[47] Centralized acquisition vehicles (e.g., contracts) may also require the active participation of organizations. For example, organizations may be required by provisions in contracts or agreements to install public key encryption-enabled client software recommended by external service providers.

Ultimately, the responsibility for adequately mitigating unacceptable risks arising from the use of external information system services remains with authorizing officials. Organizations require that appropriate *chains of trust* be established with external service providers when dealing with the many issues associated with information system security. Organizations establish and retain a level of trust that participating service providers in the potentially complex consumer-provider relationship provide adequate protection for the services rendered to organizations. The chain of trust can be complicated due to the number of entities participating in the consumer-provider relationship and the types of relationships between the parties. External service providers may also outsource selected services to other external entities, making the chain of trust more difficult and complicated to manage. Depending on the nature of the services, organizations may find it impossible to place significant trust in external providers. This situation is due not to any inherent untrustworthiness on the part of providers, but to the intrinsic level of risk in the services.[48]

[46] Commercial providers of commodity-type services typically organize their business models and services around the concept of shared resources and devices for a broad and diverse customer base. Therefore, unless organizations obtain fully dedicated services from commercial service providers, there may be a need for greater reliance on compensating security controls to provide the necessary protections for the information system that relies on those external services. Organizational assessments of risk and risk mitigation activities reflect this situation.

[47] For example, procurement originators could authorize information systems providing external services to the federal government under the specific terms and conditions of the contracts. Federal agencies requesting such services under the terms of the contracts would not be required to reauthorize the information systems when acquiring such services (unless the request included services outside the scope of the original contracts).

[48] There may also be risk in disallowing certain functionality because of security concerns. Security is merely one of multiple considerations in an overall risk determination.

Where a sufficient level of trust cannot be established in the external services and/or providers, organizations can: (i) mitigate the risk by employing compensating controls; (ii) accept the risk within the level of organizational risk tolerance; (iii) transfer risk by obtaining insurance to cover potential losses; or (iv) avoid risk by choosing not to obtain the services from certain providers (resulting in performance of missions/business operations with reduced levels of functionality or possibly no functionality at all).[49] For example, in the case of cloud-based information systems and/or services, organizations might require as a compensating control, that all information stored in the cloud be encrypted for added security of the information. Alternatively, organizations may require encrypting some of the information stored in the cloud (depending on the criticality or sensitivity of such information)—accepting additional risk but limiting the risk of not storing all information in an unencrypted form.

2.6 ASSURANCE AND TRUSTWORTHINESS

Assurance and trustworthiness of information systems, system components, and information system services are becoming an increasingly important part of the risk management strategies developed by organizations. Whether information systems are deployed to support, for example, the operations of the national air traffic control system, a major financial institution, a nuclear power plant providing electricity for a large city, or the military services and warfighters, the systems must be reliable, trustworthy, and resilient in the face of increasingly sophisticated and pervasive threats. To understand how organizations achieve trustworthy systems and the role assurance plays in the trustworthiness factor, it is important to first define the term *trust*. Trust, in general, is the *belief* that an entity will behave in a predictable manner while performing specific functions, in specific environments, and under specified conditions or circumstances. The entity may be a person, process, information system, system component, system-of-systems, or any combination thereof.

From an information security perspective, trust is the belief that a security-relevant entity will behave in a predictable manner when satisfying a defined set of security requirements under specified conditions/circumstances and while subjected to disruptions, human errors, component faults and failures, and purposeful attacks that may occur in the environment of operation. Trust is usually determined relative to a specific *security capability*[50] and can be decided relative to an individual system component or the entire information system. However, trust at the information system level is not achieved as a result of composing a security capability from a set of trusted system components—rather, trust at the system level is an inherently subjective determination that is derived from the complex interactions among entities (i.e., technical components, physical components, and individuals), taking into account the life cycle activities that govern, develop, operate, and sustain the system. In essence, to have trust in a security capability requires that there is a sufficient basis for trust, or *trustworthiness,* in the set of security-relevant entities that are to be composed to provide such capability.

Trustworthiness with respect to information systems, expresses the degree to which the systems can be expected to preserve with some degree of confidence, the confidentiality, integrity, and availability of the information that is being processed, stored, or transmitted by the systems across a range of threats. Trustworthy information systems are systems that are believed to be capable of operating within a defined risk tolerance despite the environmental disruptions, human errors,

[49] Alternative providers offering a higher basis for trust, usually at a higher cost, may be available.

[50] A *security capability* is a combination of mutually reinforcing security controls (i.e., safeguards/countermeasures) implemented by technical means (i.e., functionality in hardware, software, and firmware), physical means (i.e., physical devices and protective measures), and/or procedural means (i.e., procedures performed by individuals).

structural failures, and purposeful attacks that are expected to occur in the environments in which the systems operate—systems that have the trustworthiness to successfully carry out assigned missions/business functions under conditions of stress and uncertainty.[51]

Security Capability

Organizations can consider defining a set of security capabilities as a precursor to the security control selection process. The concept of *security capability* is a construct that recognizes that the protection of information being processed, stored, or transmitted by information systems, seldom derives from a single safeguard or countermeasure (i.e., security control). In most cases, such protection results from the selection and implementation of a set of mutually reinforcing security controls. For example, organizations may wish to define a security capability for secure remote authentication. This capability can be achieved by the selection and implementation of a set of security controls from Appendix F (e.g., IA-2 [1], IA-2 [2], IA-2 [8], IA-2 [9], and SC-8 [1]). Moreover, security capabilities can address a variety of areas that can include, for example, technical means, physical means, procedural means, or any combination thereof. Thus, in addition to the above functional capability for secure remote access, organizations may also need security capabilities that address physical means such as tamper detection on a cryptographic module or anomaly detection/analysis on an orbiting spacecraft.

As the number of security controls in Appendix F grows over time in response to an increasingly sophisticated threat space, it is important for organizations to have the ability to describe key security capabilities needed to protect core organizational missions/business functions, and to subsequently define a set of security controls that if properly designed, developed, and implemented, produce such capabilities. This simplifies how the protection problem is viewed conceptually. In essence, using the construct of security capability provides a shorthand method of grouping security controls that are employed for a common purpose or to achieve a common objective. This becomes an important consideration, for example, when assessing security controls for effectiveness.

Traditionally, assessments have been conducted on a control-by-control basis producing results that are characterized as pass (i.e., control satisfied) or fail (i.e., control not satisfied). However, the failure of a single control or in some cases, the failure of multiple controls, may not affect the overall security capability needed by an organization. Moreover, employing the broader construct of security capability allows an organization to assess the severity of vulnerabilities discovered in its information systems and determine if the failure of a particular security control (associated with a vulnerability) or the decision not to deploy a certain control, affects the overall capability needed for mission/business protection. It also facilitates conducting *root cause* analyses to determine if the failure of one security control can be traced to the failure of other controls based on the established relationships among controls. Ultimately, authorization decisions (i.e., risk acceptance decisions) are made based on the degree to which the desired security capabilities have been effectively achieved and are meeting the security requirements defined by an organization. These risk-based decisions are directly related to organizational risk tolerance that is defined as part of an organization's risk management strategy.

Two fundamental components affecting the trustworthiness of information systems are *security functionality* and *security assurance*. Security functionality is typically defined in terms of the security features, functions, mechanisms, services, procedures, and architectures implemented within organizational information systems or the environments in which those systems operate. Security assurance is the measure of confidence that the security functionality is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system—thus possessing the capability to accurately mediate and enforce established security policies. Security controls address both security functionality and

[51] While information is the primary area of concern, trustworthiness applies to the protections for all *assets* deemed critical by organizations. Furthermore, protections are provided by technology (i.e., hardware, software, firmware), physical elements (i.e., doors, locks, surveillance), and human elements (i.e., people, processes, procedures).

security assurance. Some controls focus primarily on security functionality (e.g., PE-3, Physical Access Control; IA-2, Identification and Authentication; SC-13, Cryptographic Protection; AC-2, Account Management). Other controls focus primarily on security assurance (e.g., CA-2, Security Assessment; SA-17, Developer Security Architecture and Design; CM-3, Configuration Change Control). Finally, certain security controls can support security functionality and assurance (e.g., RA-5, Vulnerability Scanning; SC-3, Security Function Isolation; AC-25, Reference Monitor). Security controls related to functionality are combined to develop a security capability with the assurance-related controls implemented to provide a degree of confidence in the capability within the organizational risk tolerance.

Assurance Evidence—From Developmental and Operational Activities

Organizations obtain security assurance by the *actions* taken by information system developers, implementers, operators, maintainers, and assessors. Actions by individuals and/or groups during the development/operation of information systems produce *security evidence* that contributes to the assurance, or measures of confidence, in the security functionality needed to deliver the security capability. The depth and coverage of these actions (as described in Appendix E) also contribute to the efficacy of the evidence and measures of confidence. The evidence produced by developers, implementers, operators, assessors, and maintainers during the system development life cycle (e.g., design/development artifacts, assessment results, warranties, and certificates of evaluation/validation) contributes to the understanding of the security controls implemented by organizations.

The *strength* of security functionality[52] plays an important part in being able to achieve the needed security capability and subsequently satisfying the security requirements of organizations. Information system developers can increase the strength of security functionality by employing as part of the hardware/software/firmware development process: (i) well-defined security policies and policy models; (ii) structured/rigorous design and development techniques; and (iii) sound system/security engineering principles. The artifacts generated by these development activities (e.g., functional specifications, high-level/low-level designs, implementation representations [source code and hardware schematics], the results from static/dynamic testing and code analysis) can provide important evidence that the information systems (including the components that compose those systems) will be more reliable and trustworthy. Security evidence can also be generated from security testing conducted by independent, accredited, third-party assessment organizations (e.g., Common Criteria Testing Laboratories, Cryptographic/Security Testing Laboratories, and other assessment activities by government and private sector organizations).[53]

In addition to the evidence produced in the development environment, organizations can produce evidence from the operational environment that contributes to the assurance of functionality and ultimately, security capability. Operational evidence includes, for example, flaw reports, records of remediation actions, the results of security incident reporting, and the results of organizational continuous monitoring activities. Such evidence helps to determine the effectiveness of deployed security controls, changes to information systems and environments of operation, and compliance with federal legislation, policies, directives, regulations, and standards. Security evidence,

[52] The *security strength* of an information system component (i.e., hardware, software, or firmware) is determined by the degree to which the security functionality implemented within that component is correct, complete, resistant to direct attacks (strength of mechanism), and resistant to bypass or tampering.

[53] For example, third-party assessment organizations assess cloud services and service providers in support of the Federal Risk and Authorization Management Program (FedRAMP). Common Criteria Testing Laboratories test and evaluate information technology products using ISO/IEC standard 15408. Cryptographic/Security Testing Laboratories test cryptographic modules using the FIPS 140-2 standard.

whether obtained from development or operational activities, provides a better understanding of security controls implemented and used by organizations. Together, the actions taken during the system development life cycle by developers, implementers, operators, maintainers, and assessors and the evidence produced as part of those actions, help organizations to determine the extent to which the security functionality within their information systems is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting stated security requirements and enforcing or mediating established security policies—thus providing greater confidence in the security capability.

The Compelling Argument for Assurance

Organizations specify assurance-related controls to define activities performed to generate relevant and credible evidence about the functionality and behavior of organizational information systems and to trace the evidence to the elements that provide such functionality/behavior. This evidence is used to obtain a degree of confidence that the systems satisfy stated security requirements—and do so while effectively supporting the organizational missions/business functions while being subjected to threats in the intended environments of operation.

With regard to the security evidence produced, the *depth* and *coverage* of such evidence can affect the level of assurance in the functionality implemented. Depth and coverage are attributes associated with assessment methods and the generation of security evidence. Assessment methods can be applied to developmental and operational assurance. For developmental assurance, depth is associated with the rigor, level of detail, and formality of the artifacts produced during the design and development of the hardware, software, and firmware components of information systems (e.g., functional specifications, high-level design, low-level design, source code). The level of detail available in development artifacts can affect the type of testing, evaluation, and analysis conducted during the system development life cycle (e.g., black-box testing, gray-box testing, white-box testing, static/dynamic analysis). For operational assurance, the depth attribute addresses the number and types of assurance-related security controls selected and implemented. In contrast, the coverage attribute is associated with the assessment methods employed during development and operations, addressing the scope and breadth of assessment objects included in the assessments (e.g., number/types of tests conducted on source code, number of software modules reviewed, number of network nodes/mobile devices scanned for vulnerabilities, number of individuals interviewed to check basic understanding of contingency responsibilities).[54]

Addressing assurance-related controls during acquisition and system development can help organizations to obtain sufficiently trustworthy information systems and components that are more reliable and less likely to fail. These controls include ensuring that developers employ sound systems security engineering principles and processes including, for example, providing a comprehensive security architecture, and enforcing strict configuration management and control of information system and software changes. Once information systems are deployed, assurance-related controls can help organizations to continue to have confidence in the trustworthiness of the systems. These controls include, for example, conducting integrity checks on software and firmware components, conducting penetration testing to find vulnerabilities in organizational

[54] NIST Special Publication 800-53A provides guidance on the generation of security evidence related to security assessments conducted during the system development life cycle.

information systems, monitoring established secure configuration settings, and developing policies/procedures that support the operation and use of the systems.

The concepts described above, including security requirements, security capability, security controls, security functionality, and security assurance, are brought together in a model for trustworthiness for information systems and system components. Figure 3 illustrates the key components in the model and the relationship among the components.

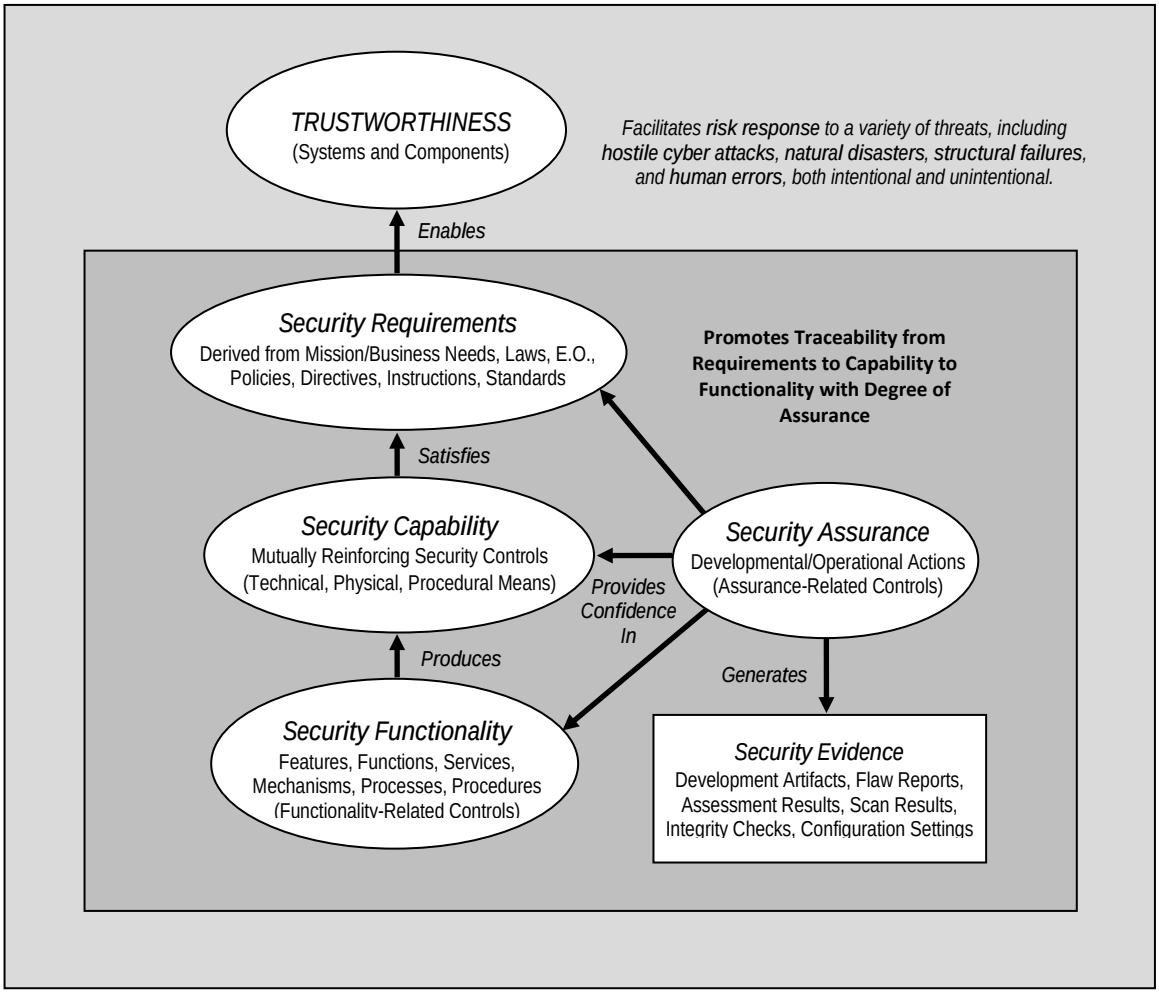


FIGURE 3: TRUSTWORTHINESS MODEL

Developmental and Operational Activities to Achieve High Assurance

Raising the bar on assurance can be difficult and costly for organizations—but sometimes essential for critical applications, missions, or business functions. Determining what parts of the organization's information technology infrastructure demand higher assurance of implemented security functionality is a Tier 1/Tier 2 risk management activity (see Figure 1 in Chapter Two). This type of activity occurs when organizations determine the *security requirements* necessary to protect organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation. Determining security requirements and the associated *security capabilities* needed to generate the appropriate protection is an integral part of the organizational risk management process described in NIST Special Publication 800-39—specifically, in the development of the *risk response strategy* following the risk framing and risk assessment steps (where organizations establish priorities, assumptions, constraints, risk tolerance and assess threats, vulnerabilities, mission/business impacts, and likelihood of threat occurrence). After the security requirements and security capabilities are determined at Tiers 1 and 2 (including the necessary assurance requirements to provide measures of confidence in the desired capabilities), those requirements/capabilities are reflected in the design of the enterprise architecture, the associated mission/business processes, and the organizational information systems that are needed to support those processes. Organizations can use the Risk Management Framework (RMF), described in NIST Special Publication 800-37, to ensure that the appropriate assurance levels are achieved for the information systems and system components deployed to carry out core missions and business functions. This is primarily a Tier 3 activity but can have some overlap with Tiers 1 and 2, for example, in the area of common control selection.

Trustworthy information systems are difficult to build from a software and systems development perspective. However, there are a number of design, architectural, and implementation principles that, if used, can result in more trustworthy systems. These core *security principles* include, for example, simplicity, modularity, layering, domain isolation, least privilege, least functionality, and resource isolation/encapsulation. Information technology products and systems exhibiting a higher degree of trustworthiness (i.e., products/systems having the requisite security functionality and security assurance) are expected to exhibit a lower rate of latent design/implementation flaws and a higher degree of penetration resistance against a range of threats including, for example, sophisticated cyber attacks, natural disasters, accidents, and intentional/unintentional errors.[55] The vulnerability and susceptibility of organizational missions/business functions and supporting information systems to known threats, the environments of operation where those systems are deployed, and the maximum acceptable level of information security risk, guide the degree of trustworthiness needed.

Appendix E describes the minimum assurance requirements for federal information systems and organizations and highlights the assurance-related controls in the security control baselines in Appendix D needed to ensure that the requirements are satisfied.[56]

[55] Organizations also rely to a great extent on security assurance from an operational perspective as illustrated by the assurance-related controls in Tables E-1 through E-3. Operational assurance is obtained by other than developmental actions including for example, defining and applying security configuration settings on information technology products, establishing policies and procedures, assessing security controls, and conducting a rigorous continuous monitoring program. In some situations, to achieve the necessary security capability with weak or deficient information technology, organizations compensate by increasing their operational assurance.

[56] CNSS Instruction 1253 designates security control baselines for national security systems. Therefore, the assurance-related controls in the baselines established for the national security community, if so designated, may differ from those controls designated for non-national security systems.

Why Assurance Matters

The importance of security assurance can be described by using the example of a light switch on a wall in the living room of your house. Individuals can observe that by simply turning the switch on and off, the switch appears to be performing according to its functional specification. This is analogous to conducting black-box testing of security functionality in an information system or system component. However, the more important questions might be—

- Does the light switch do anything else besides what it is supposed to do?
- What does the light switch look like from behind the wall?
- What types of components were used to construct the light switch and how was the switch assembled?
- Did the switch manufacturer follow industry best practices in the development process?

This example is analogous to the many developmental activities that address the quality of the security functionality in an information system or system component including, for example, design principles, coding techniques, code analysis, testing, and evaluation.

The security assurance requirements and associated assurance-related controls in Appendix E address the light switch problem from the *front of the wall perspective*, and potentially from the *behind the wall perspective*, depending on the measure of confidence needed about the component in question. For organizational missions/business functions that are less critical (i.e., low impact), lower levels of assurance might be appropriate. However, as missions/business functions become more important (i.e., moderate or high impact) and information systems and organizations become susceptible to advanced persistent threats by high-end adversaries, increased levels of assurance may be required. In addition, as organizations become more dependent on external information system services and providers, assurance becomes more important—providing greater insight and measures of confidence to organizations in understanding and verifying the security capability of external providers and the services provided to the federal government. Thus, when the potential impact to organizational operations and assets, individuals, other organizations, or the Nation is great, an increasing level of effort must be directed at what is happening behind the wall.

2.7 REVISIONS AND EXTENSIONS

The security controls listed in this publication represent the state-of-the-practice safeguards and countermeasures for federal information systems and organizations. The security controls[57] will be carefully reviewed and revised periodically to reflect:

- Experience gained from using the controls;
- New federal legislation, Executive Orders, directives, regulations, or policies;
- Changing security requirements;
- Emerging threats, vulnerabilities, and attack methods; and
- Availability of new technologies.

The security controls in the security control catalog are expected to change over time, as controls are withdrawn, revised, and added. The security controls defined in the low, moderate, and high baselines are also expected to change over time as the level of security and due diligence for mitigating risks within organizations changes. In addition to the need for change, the need for stability is addressed by requiring that proposed modifications to security controls go through a

[57] The privacy controls listed in Appendix J will also be updated on a regular basis using similar criteria.

rigorous public review process to obtain both public and private sector feedback and to build consensus for such change. This provides over time, a stable, flexible, and technically sound set of security controls for the federal government, contractors, and any other organizations using the security control catalog.

CHAPTER THREE

THE PROCESS

SELECTION AND SPECIFICATION OF SECURITY CONTROLS

This chapter describes the process of selecting and specifying security controls and control enhancements for organizational information systems to include: (i) selecting appropriate security control baselines; (ii) tailoring the baselines; (iii) documenting the security control selection process; and (iv) applying the control selection process to new development and legacy systems.

3.1 SELECTING SECURITY CONTROL BASELINES

In preparation for selecting and specifying the appropriate security controls for organizational information systems and their respective environments of operation, organizations first determine the criticality and sensitivity of the information to be processed, stored, or transmitted by those systems. This process, known as security categorization, is described in FIPS Publication 199.[58] The security categorization standard is based on a simple and well-established concept—that is, determining the potential adverse impact for organizational information systems. The results of security categorization help guide and inform the selection of appropriate security controls (i.e., safeguards and countermeasures) to adequately protect those information systems. The security controls selected for information systems are commensurate with the potential adverse impact on organizational operations and assets, individuals, other organizations, or the Nation if there is a loss of confidentiality, integrity, or availability. FIPS Publication 199 requires organizations to categorize information systems as low-impact, moderate-impact, or high-impact for the stated security objectives of confidentiality, integrity, and availability (**RMF Step 1**). The potential impact values assigned to the security objectives are the highest values (i.e., high water mark) from the security categories that have been determined for each type of information processed, stored, or transmitted by those information systems.[59] The generalized format for expressing the security category (SC) of an information system is:

$$\mathbf{SC}_{\text{information system}} = \{(\textbf{confidentiality}, \textit{impact}), (\textbf{integrity}, \textit{impact}), (\textbf{availability}, \textit{impact})\},$$

where the acceptable values for potential impact are low, moderate, or high.

Since the potential impact values for confidentiality, integrity, and availability may not always be the same for a particular information system, the high water mark concept (introduced in FIPS Publication 199) is used in FIPS Publication 200 to determine the impact level of the information system for the express purpose of selecting the applicable security control baseline from one of the three baselines identified in Appendix D.[60] Thus, a *low-impact* system is defined as an information system in which all three of the security objectives are low. A *moderate-impact* system is an information system in which at least one of the security objectives is moderate and

[58] CNSS Instruction 1253 provides security categorization guidance for national security systems.

[59] NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, provides guidance on the assignment of security categories to information systems.

[60] The high water mark concept is employed because there are significant dependencies among the security objectives of confidentiality, integrity, and availability. In most cases, a compromise in one security objective ultimately affects the other security objectives as well. Accordingly, security controls are not categorized by security objective. Rather, the security controls are grouped into baselines to provide a general protection capability for classes of information systems based on impact level.

no security objective is greater than moderate. Finally, a *high-impact* system is an information system in which at least one security objective is high.

Implementation Tip

To determine the impact level of an information system:

- First, determine the different types of information that are processed, stored, or transmitted by the information system. NIST Special Publication 800-60 provides common information types.
- Second, using the impact values in FIPS Publication 199 and the recommendations of NIST Special Publication 800-60, categorize the confidentiality, integrity, and availability of each information type.
- Third, determine the information system security categorization, that is, the highest impact value for each security objective (confidentiality, integrity, availability) from among the categorizations for the information types associated with the information system.
- Fourth, determine the overall impact level of the information system from the highest impact value among the three security objectives in the system security categorization.

Note: *For national security systems, organizations use CNSSI 1253 for security categorization*.

Once the impact level of the information system is determined, organizations begin the security control selection process (**RMF Step 2**). The first step in selecting and specifying security controls for the information system is to choose the appropriate security control baseline.[61] The selection of the security control baseline is based on the FIPS 200 impact level of the information system as determined by the security categorization process described above. The organization selects one of three security control baselines from Appendix D corresponding to the low-impact, moderate-impact, or high-impact rating of the information system.[62] Note that not all security controls are assigned to baselines, as indicated in Table D-2 by the phrase *not selected*. Similarly, as illustrated in Tables D-3 through D-19, not all control enhancements are assigned to baselines. Those control enhancements that are assigned to baselines are so indicated by an "**X"** in the low, moderate, or high columns. The use of the term *baseline* is intentional. The security controls and control enhancements in the baselines are a starting point from which controls/enhancements may be removed, added, or specialized based on the tailoring guidance in Section 3.2.

The security control baselines in Appendix D address the security needs of a broad and diverse set of constituencies (including individual users and organizations). Some *assumptions* that generally underlie the baselines in Appendix D include, for example: (i) the environments in which organizational information systems operate; (ii) the nature of operations conducted by organizations; (iii) the functionality employed within information systems; (iv) the types of threats facing organizations, missions/business processes, and information systems; and (v) the type of information processed, stored, or transmitted by information systems. Articulating the underlying assumptions is a key element in the initial *risk framing* step of the risk management process described in NIST Special Publication 800-39. Some of the assumptions that underlie the baselines in Appendix D include:

[61] The general security control selection process may be augmented or further detailed by additional sector-specific guidance as described in Section 3.3, *Creating Overlays*, and Appendix I, *template* for developing overlays.

[62] CNSS Instruction 1253 provides security control baselines for national security systems.

- Information systems are located in physical facilities;
- User data/information in organizational information systems is relatively persistent;[63]
- Information systems are multi-user (either serially or concurrently) in operation;
- Some user data/information in organizational information systems is not shareable with other users who have authorized access to the same systems;
- Information systems exist in networked environments;
- Information systems are general purpose in nature; and
- Organizations have the necessary structure, resources, and infrastructure to implement the controls.[64]

If one or more of these assumptions is not valid, then some of the security controls assigned to the initial baselines in Appendix D may not be applicable—a situation that can be readily addressed by applying the tailoring guidance in Section 3.2 and the results of organizational assessments of risk. Conversely, there are also some possible situations that are specifically not addressed in the baselines. These include:

- Insider threats exist within organizations;
- Classified data/information is processed, stored, or transmitted by information systems;
- Advanced persistent threats (APTs) exist within organizations;
- Selected data/information requires specialized protection based on federal legislation, directives, regulations, or policies; and
- Information systems need to communicate with other systems across different security domains.

If any of the above assumptions apply, then additional security controls from Appendix F would likely be needed to ensure adequate protection—a situation that can also be effectively addressed by applying the tailoring guidance in Section 3.2 (specifically, security control supplementation) and the results of organizational assessments of risk.

3.2 TAILORING BASELINE SECURITY CONTROLS

After selecting the applicable security control baseline from Appendix D, organizations initiate the tailoring process to modify appropriately and align the controls more closely with the specific conditions within the organization (i.e., conditions related to organizational missions/business functions, information systems, or environments of operation). The tailoring process includes:

- Identifying and designating common controls in initial security control baselines;
- Applying scoping considerations to the remaining baseline security controls;
- Selecting compensating security controls, if needed;

[63] Persistent data/information refers to data/information with utility for a relatively long duration (e.g., days, weeks).

[64] In general, federal departments and agencies will satisfy this assumption. The assumption becomes more of an issue for nonfederal entities such as municipalities, first responders, and small (business) contractors. Such entities may not be large enough or sufficiently resourced to have elements dedicated to providing the range of security capabilities that are assumed by the baselines. Organizations consider such factors in their risk-based decisions.

- Assigning specific values to organization-defined security control parameters via explicit assignment and selection statements;
- Supplementing baselines with additional security controls and control enhancements, if needed; and
- Providing additional specification information for control implementation, if needed.

The tailoring process, as an integral part of security control selection and specification, is part of a comprehensive organizational risk management process—framing, assessing, responding to, and monitoring information security risk. Organizations use risk management guidance to facilitate risk-based decision making regarding the applicability of security controls in the security control baselines. Ultimately, organizations use the tailoring process to achieve cost-effective, risk-based security that supports organizational mission/business needs. Tailoring activities are approved by authorizing officials in coordination with selected organizational officials (e.g., risk executive [function], chief information officers, senior information security officers, information system owners, common control providers) prior to implementing the security controls. Organizations have the flexibility to perform the tailoring process at the organization level for all information systems (either as a required tailored baseline or as the starting point for system-specific tailoring activities), in support of a particular line of business or mission/business process, at the individual information system level, or by using a combination of the above.[65]

Conversely, organizations do not remove security controls for operational convenience. Tailoring decisions regarding security controls should be defensible based on mission/business needs and accompanied by explicit risk-based determinations.[66] Tailoring decisions, including the specific rationale for those decisions, are documented in the security plans for organizational information systems. Every security control from the applicable security control baseline is accounted for either by the organization (e.g., common control provider) or by the information system owner. If certain security controls are tailored out, then the associated rationale is recorded in security plans (or references/pointers to other relevant documentation are provided) for the information systems and approved by the responsible organizational officials as part of the security plan approval process.[67]

Documenting significant risk management decisions in the security control selection process is imperative in order for authorizing officials to have the necessary information to make credible, risk-based decisions with regard to the authorization of information systems. Since information systems, environments of operation, and personnel associated with the system development life cycle are subject to change, providing the assumptions, constraints, and rationale supporting those important risk decisions allows for a better understanding in the future of the security state of the information systems or environments of operation at the time the original risk decisions were made and facilitates identifying changes, when previous risk decisions are revisited.

[65] See also Section 3.3, *Creating Overlays*, and Appendix I, *template* for developing overlays.

[66] Tailoring decisions can also be based on timing and applicability of selected security controls under certain defined conditions. That is, security controls may not apply in every situation or the parameter values for assignment statements may change under certain circumstances. Overlays can define these special situations, conditions, or timing-related considerations.

[67] The level of detail required in documenting tailoring decisions in the security control selection process is at the discretion of organizations and reflects the impact levels of the respective information systems implementing or inheriting the controls.

Identifying and Designating Common Controls

Common controls are controls that may be inherited by one or more organizational information systems. If an information system inherits a common control, then that system does not need to explicitly implement that control—that is, the security capability is being provided by another entity. Therefore, when the security controls in Appendix F call for an information system to implement or perform a particular security function, it should not be interpreted to mean that all systems that are part of larger, more complex systems or all components of a particular system need to implement the control or function. Organizational decisions on which security controls are designated as common controls may greatly affect the responsibilities of individual system owners with regard to the implementation of controls in a particular baseline. Common control selection can also affect the overall resource expenditures by organizations (i.e., the greater the number of common controls implemented, the greater potential cost savings).

Applying Scoping Considerations

Scoping considerations, when applied in conjunction with risk management guidance, provide organizations with a more granular foundation with which to make risk-based decisions.[68] The application of scoping considerations can eliminate unnecessary security controls from the initial security control baselines and help to ensure that organizations select *only* those controls that are needed to provide the appropriate level of protection for organizational information systems—protection based on the missions and business functions being supported by those systems and the environments in which the systems operate. Organizations may apply the scoping considerations described below to assist with making risk-based decisions regarding security control selection and specification—decisions that can potentially affect how the baseline security controls are applied and implemented by organizations:

- CONTROL ALLOCATION AND PLACEMENT CONSIDERATIONS—

  The term *information system* can refer to systems at multiple levels of abstraction ranging from system-of-systems to individual single-user systems. The growing complexity of many information systems requires careful analysis in the allocation/placement of security controls within the three tiers in the risk management hierarchy (organization level, mission/business process level, and information system level) without imposing any specific architectural views or solutions.[69] Security controls in the initial baselines represent an information system-wide set of controls that may not be applicable to every component in the system. Security controls are applicable only to information system components that provide or support the information security capability addressed by the controls.[70] Organizations make explicit risk-based decisions about where to apply or allocate specific security controls in organizational information systems in order to achieve the needed security capability and to satisfy security requirements.[71] An example of this type of allocation is applying the

[68] The scoping considerations listed in this section are exemplary and *not* intended to limit organizations in rendering risk-based decisions based on other organization-defined considerations with appropriate rationale.

[69] This is especially true with the advent of service-oriented architectures where specific services are provided to implement a single function.

[70] For example, auditing controls are typically applied to components of an information system that provide auditing capability (e.g., servers, etc.) and are not necessarily applied to every user-level workstation within the organization. Organizations should carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.

[71] As information technology advances, more powerful and diverse functionality can be found in smart phones, tablets, and other types of mobile devices. While tailor guidance may support not allocating a particular security control to a specific technology or device, any residual risk associated with the absence of that control must be addressed in risk assessments to adequately protect organizational operations and assets, individuals, other organizations, and the Nation.

requirement from AC-18 (1) (i.e., protecting wireless access to information systems using authentication/encryption) to all wireless access except for wireless access to visitor subnetworks which are not connected to other system components.

- OPERATIONAL/ENVIRONMENTAL-RELATED CONSIDERATIONS—

  Several of the security controls in the baselines are based on the assumption of the existence of certain operational/environmental factors. Where these factors are absent or significantly diverge from the baseline assumptions, it is justifiable to tailor the baseline. Some of the more common operational/environmental factors include:

  - *Mobility*

    The mobility of physical hosting environments can impact the security controls selected for organizational information systems. As noted above, the set of security controls assigned to each baseline in Appendix D assumes the operation of information systems in fixed facilities and nonmobile locations. If those information systems operate primarily in mobile environments, the security control baseline should be tailored appropriately to account for the differences in mobility and accessibility of the specific locations where the systems reside. For example, many of the security controls in the Physical and Environmental Protection (PE) family that are selected in all three baselines reflect the assumption that the information systems reside in physical facilities/complexes that require appropriate physical protections. Such controls would likely not provide added value for mobile environments such as ships, aircraft, automobiles, vans, or space-based systems.[72]

  - *Single-User Systems and Operations*

    For information systems that are designed to operate as single-user systems (e.g., smart phones), several of the security controls that address sharing among users may not be needed. A single-user system or device refers to a system/device that is only intended to be used by a single individual over time (i.e., exclusive use). Systems or devices that are shared by multiple users over time are not considered single-user. Security controls such as AC-10, Concurrent Session Control, SC-4, Information in Shared Resources, and AC-3, Access Enforcement[73] may not be required in single-user systems/operations and could reasonably be tailored out of the baseline at the discretion of organizations.

  - *Data Connectivity and Bandwidth*

    While many information systems are interconnected, there are some systems which for security or operational reasons, lack networking capabilities—that is, the systems are *air gapped* from the network. For nonnetworked systems, security controls such as AC-17, Remote Access, SC-8, Transmission Confidentiality and Integrity, and SC-7, Boundary Protection, are not applicable and may be tailored out of the security control baselines at the discretion of organizations. In addition to nonnetworked information systems, there are systems that have very limited or sporadic bandwidth (e.g., tactical systems that support warfighter or law enforcement missions). For such systems, the application of security controls would need to be examined carefully as the limited and/or sporadic bandwidth could impact the practicality of implementing those controls and the viability of adversaries staging cyber attacks over the limited bandwidth.

[72] The mobile nature of devices means that it is possible that, for some period of time, the devices may reside in fixed facilities or complexes in fixed locations. During that time, the PE controls would likely apply.

[73] Organizations consider whether individual users have administrator privileges before removing AC-3 from security control baselines.

- *Limited Functionality Systems or System Components*

  What constitutes an information system under the E-Government Act of 2002 is quite broad. Fax machines, printers, scanners, pagers, smart phones, tablets, E-readers, and digital cameras can all be categorized as information systems (or system components). These types of systems and components may lack the general processing capabilities assumed in the security control baselines. The nature of these constraints may limit the types of threats that these systems face, and hence the appropriateness of some of the security controls. Thus, a control such as SI-3, Malicious Code Protection (required in all control baselines) may not be practical for information systems or components that are not capable of executing code (e.g., text-only pagers). However, because there is often no clear delineation between these types of information systems or components (e.g., smart phones combine the digital capabilities of telephones, cameras, and computers), it is important that the application of security controls to limited functionality systems or components be done judiciously and always take into account the intended use of the systems, system capabilities, and the risk of compromise.

- *Information and System Non-Persistence*

  There is often an assumption that user information within organizational information systems is persistent for a considerable period of time. However, for some applications and environments of operation (e.g., tactical systems, industrial control systems), the persistence of user information is often very limited in duration. For information systems processing, storing, or transmitting such non-persistent information, several security controls in the Contingency Planning (CP) family such as CP-6, Alternate Storage Site, CP-7, Alternate Processing Site, and CP-9, Information System Backup, may not be practical and can be tailored out at the discretion of organizations. For similar reasons, controls such as MP-6, Media Sanitization, and SC-28, Protection of Information at Rest, are good candidates for removal through tailoring.[74] In addition to the non-persistence of information, the information systems/services may be non-persistent as well. This can be achieved by the use of virtualization techniques to establish non-persistent instantiations of operating systems and applications. Depending on the duration of the instantiations, some baseline controls might not be applicable.

- *Public Access*

  When public access to organizational information systems is allowed, security controls should be applied with discretion since some security controls from the specified control baselines (e.g., identification and authentication, personnel security controls) may not be applicable for public access. Thus, in the case of the general public accessing federal government websites (e.g., to download publically accessible information such as forms, emergency preparedness information), security controls such as AC-7, Unsuccessful Logon Attempts, AC-17, Remote Access, IA-2, Identification and Authentication, IA-4, Identifier Management, and IA-5, Authenticator Management, typically would not be relevant for validating access authorizations or privileges. However, many of these controls would still be needed for identifying and authenticating organizational personnel that maintain and support information systems providing such public access websites and services. Similarly, many of the security controls may still be required for users accessing nonpublic information systems through such public interfaces, for example, to access or change personal information.

[74] Organizations balance information persistence with the sensitivity of the information. Non-persistent information may still require sanitization after deletion. In addition, organizations consider the duration of information sensitivity—some information may be persistent, but only be sensitive for a limited time.

- SECURITY OBJECTIVE-RELATED CONSIDERATIONS—

  Security controls that support only one or two of the confidentiality, integrity, or availability security objectives may be downgraded to the corresponding control in a lower baseline (or modified or eliminated if not defined in a lower baseline) only if the downgrading action: (i) reflects the FIPS Publication 199 security category for the supported security objective(s) before moving to the FIPS Publication 200 impact level (i.e., high water mark);[75] (ii) is supported by an organizational assessment of risk; and (iii) does not adversely affect the level of protection for the security-relevant information within the information system.[76] For example, if an information system is categorized as moderate impact using the high water mark concept because confidentiality and/or integrity are moderate but availability is low, there are several controls that only support the availability security objective and that potentially could be downgraded to low baseline requirements—that is, it may be appropriate *not* to implement CP-2 (1) because the control enhancement supports only availability and is selected in the moderate baseline but not in the low baseline. The following security controls and control enhancements are potential candidates for downgrading:[77]

  - *Confidentiality:* AC-21, MA-3 (3), MP-3, MP-4, MP-5, MP-5 (4), MP-6 (1), MP-6 (2), PE-4, PE-5, SC-4, SC-8, SC-8 (1);
  - *Integrity:* CM-5, CM-5 (1), CM-5 (3), SC-8, SC-8 (1), SI-7, SI-7 (1), SI-7 (5), SI-10; and
  - *Availability:* CP-2 (1), CP-2 (2), CP-2 (3), CP-2 (4), CP-2 (5), CP-2 (8), CP-3 (1), CP-4 (1), CP-4 (2), CP-6, CP-6 (1), CP-6 (2), CP-6 (3), CP-7, CP-7 (1), CP-7 (2), CP-7 (3), CP-7 (4), CP-8, CP-8 (1), CP-8 (2), CP-8 (3), CP-8 (4), CP-9 (1), CP-9 (2), CP-9 (3), CP-9 (5), CP-10 (2), CP-10 (4), MA-6, PE-9, PE-10, PE-11, PE-11 (1), PE-13 (1), PE-13 (2), PE-13 (3), PE-15 (1).

- TECHNOLOGY-RELATED CONSIDERATIONS—

  Security controls that refer to specific technologies (e.g., wireless, cryptography, public key infrastructure) are applicable only if those technologies are employed or are required to be employed within organizational information systems. Security controls that can be explicitly or implicitly supported by automated mechanisms do not require the development of such mechanisms if the mechanisms do not already exist or are not readily available in commercial or government off-the-shelf products. If automated mechanisms are not readily available,

[75] When applying the high water mark in Section 3.1, some of the original FIPS Publication 199 confidentiality, integrity, or availability security objectives may have been upgraded to a higher security control baseline. As part of this process, security controls that uniquely support the confidentiality, integrity, or availability security objectives may have been upgraded unnecessarily. Consequently, it is recommended that organizations consider appropriate and allowable downgrading actions to ensure cost-effective, risk-based application of security controls.

[76] Information that is security-relevant at the information system level (e.g., password files, network routing tables, cryptographic key management information) is distinguished from user-level information within the same system. Certain security controls are used to support the security objectives of confidentiality and integrity for both user-level and system-level information. Caution should be exercised in downgrading confidentiality or integrity-related security controls to ensure that downgrading actions do not result in insufficient protection for the security-relevant information within the information system. Security-relevant information must be protected at the high water mark in order to achieve a similar level of protection for any of the security objectives related to user-level information.

[77] Downgrading actions apply only to the moderate and high baselines. Security controls that are uniquely attributable to confidentiality, integrity, or availability that would ordinarily be considered as potential candidates for downgrading (e.g., AC-16, AU-10, IA-7, PE-12, PE-14, SC-5, SC-13, SC-16) are eliminated from consideration because the controls are either selected for use in all baselines and have no enhancements that could be downgraded, or the controls are optional and not selected for use in any baseline. Organizations should exercise caution when downgrading security controls that do not appear in the list in Section 3.2 to ensure that downgrading actions do not affect security objectives other than the objectives targeted for downgrading.

cost-effective, or technically feasible, compensating security controls, implemented through nonautomated mechanisms or procedures, are used to satisfy specified security controls or control enhancements (see terms and conditions for applying compensating controls below).

- MISSION REQUIREMENTS-RELATED CONSIDERATIONS—

  Some security controls may not be applicable (or appropriate) if implementing those controls has the potential to degrade, debilitate, or otherwise hamper critical organizational missions and/or business functions. For example, if the mission requires that an uninterrupted display of mission-critical information be available at an operator console (e.g., air traffic controller console), the implementation of AC-11, Session Lock, or SC-10, Network Disconnect, may not be appropriate.

Selecting Compensating Security Controls

Organizations may find it necessary on occasion to employ compensating security controls. Compensating controls are alternative security controls employed by organizations in lieu of specific controls in the low, moderate, or high baselines described in Appendix D—controls that provide equivalent or comparable protection for organizational information systems and the information processed, stored, or transmitted by those systems.[78] This may occur, for example, when organizations are unable to effectively implement specific security controls in the baselines or when, due to the specific nature of the information systems or environments of operation, the controls in the baselines are not a cost-effective means of obtaining the needed risk mitigation. Compensating controls are typically selected after applying the scoping considerations in the tailoring guidance to the applicable security control baseline. Compensating controls may be employed by organizations under the following conditions:

- Organizations select compensating controls from Appendix F; if appropriate compensating controls are not available, organizations adopt suitable compensating controls from other sources;[79]
- Organizations provide supporting rationale for how compensating controls provide equivalent security capabilities for organizational information systems and why the baseline security controls could not be employed; and
- Organizations assess and accept the risk associated with implementing compensating controls in organizational information systems.

Assigning Security Control Parameter Values

Security controls and control enhancements containing embedded parameters (i.e., assignment and selection statements) give organizations the flexibility to define certain portions of controls and enhancements to support specific organizational requirements. After the initial application of scoping considerations and the selection of compensating controls, organizations review the security controls and control enhancements for assignment/selection statements and determine appropriate organization-defined values for the identified parameters. Parameter values may be prescribed by applicable federal laws, Executive Orders, directives, regulations, policies, or standards. Once organizations define the parameter values for security controls and control

[78] More than one compensating control may be required to provide the equivalent protection for a particular security control in Appendix F. For example, organizations with significant staff limitations may compensate for the separation of duty security control by strengthening the audit, accountability, and personnel security controls.

[79] Organizations should make every attempt to select compensating controls from the security control catalog in Appendix F. Organization-defined compensating controls are employed *only* when organizations determine that the security control catalog does not contain suitable compensating controls.

enhancements, the assignments and selections become a part of the control and enhancement.[80] Organizations may choose to specify the values for security control parameters before selecting compensating controls since the specification of the parameters completes the control definitions and may affect compensating control requirements. There can also be significant benefits in collaborating on the development of parameter values. For organizations that work together on a frequent basis, it may be useful for those organizations to develop a mutually agreeable set of uniform values for security control parameters. Doing so may assist organizations in achieving a greater degree of reciprocity when depending upon the information systems and/or services offered by other organizations.

Supplementing Security Control Baselines

The final determination of the appropriate set of security controls necessary to provide adequate security for organizational information systems and the environments in which those systems operate is a function of the assessment of risk and what is required to sufficiently mitigate the risks to organizational operations and assets, individuals, other organizations, and the Nation.[81] In many cases, additional security controls or control enhancements (beyond those controls and enhancements contained in the baselines in Appendix D) will be required to address specific threats to and vulnerabilities in organizations, mission/business processes, and/or information systems and to satisfy the requirements of applicable federal laws, Executive Orders, directives, policies, standards, or regulations.[82] The risk assessment in the security control selection process provides essential information in determining the necessity and sufficiency of the security controls and control enhancements in the initial baselines. Organizations are encouraged to make maximum use of Appendix F to facilitate the process of supplementing the initial baselines with additional security controls and/or control enhancements.[83]

Situations Requiring Potential Baseline Supplementation

Organizations may be subject to conditions that, from an operational, environmental, or threat perspective, warrant the selection and implementation of additional (supplemental) controls to achieve adequate protection of organizational missions/business functions and the information systems supporting those missions/functions. Examples of conditions and additional controls that might be required are provided below.

- ADVANCED PERSISTENT THREAT

  Security control baselines do not assume that the current threat environment is one where adversaries have achieved a significant foothold and presence within organizations and organizational information systems—that is, organizations are dealing with an advanced persistent threat (APT). Adversaries continue to attack organizational information systems and the information technology infrastructure and are successful in some aspects of such attacks. To more fully address the advanced persistent threat, concepts such as insider threat

[80] CNSS Instruction 1253 provides assignment of minimum values for organization-defined variables applicable to national security systems. Parameter values can also be defined as part of overlays described in Section 3.4.

[81] Considerations for potential national-level impacts and impacts to other organizations in categorizing organizational information systems derive from the USA PATRIOT Act and Homeland Security Presidential Directives.

[82] In previous versions of Special Publication 800-53, tailoring referred only to the removal of security controls from baselines and supplementation referred only to the addition of controls to baselines. In this document, the term tailoring has been redefined to include both the addition of security controls to baselines (i.e., tailoring up) and the removal of controls from baselines (i.e., tailoring down).

[83] Security controls and control enhancements selected to supplement baselines are allocated to appropriate information system components in the same manner as the control allocations carried out by organizations in the initial baselines.

protection (CM-5 (4)), heterogeneity (SC-29), deception (SC-26 and SC-30), non-persistence (SC-25 and SC-34), and segmentation (SC-7 (13)) can be considered.

- CROSS-DOMAIN SERVICES

  Security control baselines do not assume that information systems have to operate across multiple security domains. The baselines assume a flat view of information flows (i.e., the same security policies in different domains when information moves across authorization boundaries). To address cross-domain services and transactions, some subset of the AC-4 security control enhancements can be considered to ensure adequate protection of information when transferred between information systems with different security policies.

- MOBILITY

  The use of mobile devices might result in the need for additional security controls and control enhancements not selected in the initial baselines. For example, AC-7 (2), which requires the purging/wiping of information after an organization-defined number of unsuccessful logon attempts, or MP-6 (8), which requires the capability for remote purging/wiping, could be selected in order to address the threat of theft or loss of mobile devices.

- CLASSIFIED INFORMATION

  In some environments, classified and sensitive information[84] may be resident on national security systems without all users having the necessary authorizations to access all of the information. In those situations, additional security controls are required to ensure that information requiring strict separation is not accessed by unauthorized users. More stringent access controls include, for example, AC-3 (3) and AC-16. When classified information is being processed, stored, or transmitted on information systems that are jointly owned by multiple entities (e.g., coalition partners in military alliances), more restrictive controls for maintenance personnel may be required including, for example, MA-5 (4).

Processes for Identifying Additional Needed Security Controls

Organizations can employ a *requirements definition* approach or a *gap analysis* approach in selecting security controls and control enhancements to supplement initial baselines. In the requirements definition approach, organizations obtain specific and credible threat[85] information (or make reasonable assumptions) about the activities of adversaries with certain capabilities or attack potential (e.g., skill levels, expertise, available resources). To effectively withstand cyber attacks from adversaries with the stated capabilities or attack potential, organizations strive to achieve a certain level of defensive capability or cyber preparedness. Organizations can select additional security controls and control enhancements from Appendix F to obtain such defensive capability or level of preparedness. In contrast to the requirements definition approach, the gap analysis approach begins with an organizational assessment of its current defensive capability or level of cyber preparedness. From that initial capability assessment, organizations determine the types of threats they can reasonably expect to counter. If the current organizational defensive capabilities or levels of cyber preparedness are insufficient, the gap analysis determines the required capabilities and levels of preparedness. Organizations subsequently define the security controls and control enhancements from Appendix F needed to achieve the desired capabilities or cyber-preparedness levels. Both of the approaches described above require timely and accurate

[84] The example is illustrative only. CNSS Instruction 1253 provides specific guidance regarding security controls required for national security systems.

[85] While this example focuses on threats to information systems from purposeful attacks, the threat space of concern to organizations also includes environmental disruptions and human errors.

threat information. It is essential that organizations work with the appropriate threat identification component to obtain such information.

During the tailoring process, organizations consider reevaluating the priority codes from the security control baselines to determine if any changes to those priorities are appropriate. This is especially important when adding security controls that are not included in any of the baselines, because those controls have priority codes of P0. The reevaluation of priority codes can be based on organizational assessments of risk or design/developmental decisions related to the security architecture or the systems and security engineering process that may require certain sequencing in security control implementation.

Enhancing Information Security without Changing Control Selection

There may be situations in which organizations cannot apply sufficient security controls within their information systems to adequately reduce or mitigate risk (e.g., when using certain types of information technologies or employing certain computing paradigms). Therefore, alternative strategies are needed to prevent organizational missions/business functions from being adversely affected— strategies that consider the mission and business risks resulting from an aggressive use of information technology. Restrictions on the types of technologies used and how organizational information systems are employed provide an alternative method to reduce or mitigate risk that may be used in conjunction with, or instead of, supplemental security controls. Restrictions on the use of information systems and specific information technologies may be, in some situations, the only practical or reasonable actions organizations can take in order to have the capability to carry out assigned missions/business functions in the face of determined adversaries. Examples of use restrictions include:

- Limiting the information that information systems can process, store, or transmit or the manner in which organizational missions/business functions are automated;
- Prohibiting external access to organizational information by removing selected information system components from networks (i.e., air gapping); and
- Prohibiting moderate- or high-impact information on organizational information system components to which the public has access, unless an explicit risk determination is made authorizing such access.

Providing Additional Specification Information for Control Implementation

Since security controls are statements of security capability at higher levels of abstraction, the controls may lack sufficient information for successful implementation. Therefore, additional detail may be necessary to fully define the intent of a given security control for implementation purposes and to ensure that the security requirements related to that control are satisfied. For example, additional information may be provided as part of the process of moving from control to specification requirement, and may involve *refinement* of implementation details, *refinement* of scope, or *iteration* to apply the same control differently to different scopes. Organizations ensure that if existing security control information (e.g., selection and assignment statements) is not sufficient to fully define the intended application of the control, such information is provided. Organizations have the flexibility to determine whether additional detail is included as a part of the control statement, in supplemental guidance, or in a separate control addendum section. When providing additional detail, organizations are cautioned not to change the intent of the security control or modify the original language in the control. The additional implementation information can be documented either in security plans or systems and security engineering plans. The type of

additional detail that might be necessary to fully specify a security control for implementation purposes is provided in the SI-7 (6) example below:

SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

(6) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CRYPTOGRAPHIC PROTECTION*

The information system implements cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.

Supplemental Guidance: Cryptographic mechanisms used for the protection of integrity include, for example, digital signatures and the computation and application of signed hashes using asymmetric cryptography, protecting the confidentiality of the key used to generate the hash, and using the public key to verify the hash information. Related control: SC-13.

Additional implementation detail for SI-7 (6):

Digital signatures are applied to all traffic for which non-repudiation is required employing SHA-256 or another approved NIST algorithm demonstrably of at least the same strength of mechanism.

3.3 CREATING OVERLAYS

The previous sections described the process of tailoring security control baselines to achieve a more focused and relevant security capability for organizations. In certain situations, it may be beneficial for organizations to apply tailoring guidance to the baselines to develop a set of security controls for community-wide use or to address specialized requirements, technologies, or unique missions/environments of operation.[86] For example, the federal government may decide to establish a governmentwide set of security controls and implementation guidance for: (i) public key infrastructure (PKI) systems that could be uniformly applied to all PKI systems implemented within federal agencies; (ii) cloud-based information systems that are uniformly applied to all federal agencies procuring or implementing cloud services; or (iii) industrial control systems (ICSs) at federal facilities producing electric power or controlling environmental systems in federal facilities. Alternatively, to address particular communities of interest with specialized requirements, the Department of Defense, for example, may decide to establish a set of security controls and implementation guidance for its tactical operations and environments by applying the tailoring guidance to the standard security control baselines for national security systems to achieve more specialized solutions. In each of the above examples, tailored baselines can be developed for each information technology area or for the unique circumstances/environments and promulgated to large communities of interest—thus achieving standardized security capabilities, consistency of implementation, and cost-effective security solutions.

To address the need for developing community-wide and specialized sets of security controls for information systems and organizations, the concept of *overlay* is introduced. An overlay is a fully specified set of security controls, control enhancements, and supplemental guidance derived from the application of tailoring guidance in Section 3.2 to security control baselines in Appendix D.[87] Overlays complement the initial security control baselines by: (i) providing the opportunity to add or eliminate controls; (ii) providing security control applicability and interpretations for specific information technologies, computing paradigms, environments of operation, types of information systems, types of missions/operations, operating modes, industry sectors, and statutory/regulatory requirements; (iii) establishing community-wide parameter values for assignment and/or selection statements in security controls and control enhancements; and (iv) extending the supplemental guidance for security controls, where necessary. Organizations typically use the overlay concept

[86] This type of tailoring can be conducted at the federal level or by individual organizations.

[87] CNSS Instruction 1253 provides tailoring guidance and security control baselines for national security systems.

when there is divergence from the basic assumptions used to create the initial security control baselines (see Section 3.1). If organizations are not divergent from the basic assumptions for the initial baselines, there is likely no need to create an overlay. Alternatively, the baselines may be missing key assumptions which would justify creating an overlay with additional assumptions.

The full range of tailoring activities can be employed by organizations to provide a disciplined and structured approach for developing tailored baselines supporting the areas described above. Overlays provide an opportunity to build consensus across communities of interest and develop security plans for organizational information systems that have broad-based support for very specific circumstances, situations, and/or conditions. Categories of overlays that may be useful include, for example:

- Communities of interest, industry sectors, or coalitions/partnerships (e.g., healthcare, law enforcement, intelligence, financial, transportation, energy, allied collaboration/sharing);
- Information technologies/computing paradigms (e.g., cloud/mobile, PKI, Smart Grid, cross-domain solutions);
- Environments of operation (e.g., space, tactical);
- Types of information systems and operating modes (e.g., industrial/process control systems, weapons systems, single-user systems, standalone systems);
- Types of missions/operations (e.g., counterterrorism, first responders, research, development, test, and evaluation); and
- Statutory/regulatory requirements (e.g., Foreign Intelligence Surveillance Act, Health Insurance Portability and Accountability Act, Privacy Act).

Organizations can effectively use the risk management concepts defined in NIST Special Publication 800-39 when developing overlays. The successful development of overlays requires the involvement of: (i) information security professionals who understand the specific subject area that is the focus of the overlay development effort; and (ii) subject matter experts in the overlay area who understand the security controls in Appendix F and the initial baselines in Appendix D. The format and structure for developing overlays is provided in Appendix I.

Multiple overlays can be applied to a single security control baseline. The tailored baselines that result from the overlay development process may be more or less stringent than the original security control baselines. Risk assessments provide information necessary to determine if the risk from implementing the tailored baselines falls within the risk tolerance of the organizations or communities of interest developing the overlays. If multiple overlays are employed, it is possible that there could be a conflict between the overlays. If the use of multiple overlays results in conflicts between the application or removal of security controls, the authorizing official (or designee), in coordination with the mission/business owner and/or information owner/steward, can resolve the conflict. In general, overlays are intended to reduce the need for ad hoc tailoring of baselines by organizations through the selection of a set of controls and control enhancements that more closely correspond to common circumstances, situations, and/or conditions. However, the use of overlays does not preclude organizations from performing further tailoring to reflect organization-specific needs, assumptions, or constraints. Tailoring of overlays is accomplished within the constraints defined within the overlay and may require the concurrence/approval of the authorizing official or other organization-designated individuals. For example, an overlay created for an industrial control system (ICS) may require tailoring for applicability to a specific type of ICS and its environment of operation. But it is anticipated that the use of overlays would greatly reduce the number and extent of organization-specific ad hoc tailoring.

3.4 DOCUMENTING THE CONTROL SELECTION PROCESS

Organizations document the relevant decisions taken during the security control selection process, providing a sound rationale for those decisions. This documentation is essential when examining the security considerations for organizational information systems with respect to the potential mission/business impact. The resulting set of security controls and the supporting rationale for the selection decisions (including any information system use restrictions required by organizations) are documented in the security plans. Documenting significant risk management decisions in the security control selection process is imperative so that authorizing officials can have access to the necessary information to make informed authorization decisions for organizational information systems.[88] Without such information, the understanding, assumptions, constraints, and rationale supporting those risk management decisions will, in all likelihood, not be available when the state of the information systems or environments of operation change, and the original risk decisions are revisited. Figure 4 summarizes the security control selection process, including the selection of initial baselines and the tailoring of the baselines by applying the guidance in Section 3.2.

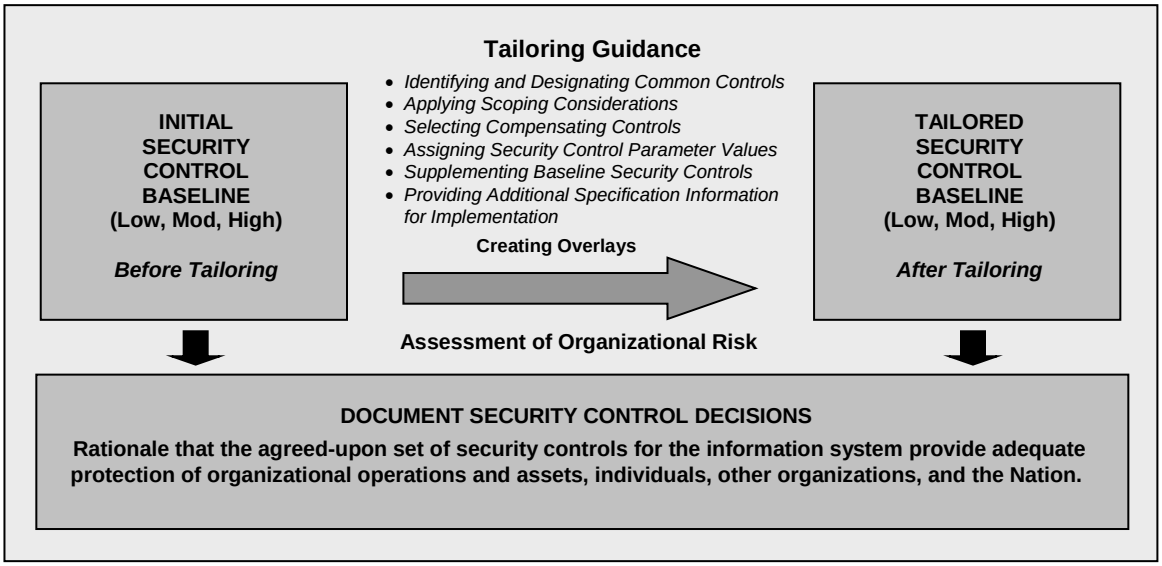


FIGURE 4: SECURITY CONTROL SELECTION PROCESS

Iterative and Dynamic Nature of Security Control Tailoring

The security control tailoring process described above, while appearing to be sequential in nature, can also have an iterative aspect. Organizations may choose to execute the tailoring steps in any order based on organizational needs and the information generated from risk assessments. For example, some organizations may establish the parameter values for security controls in the initial baselines prior to selecting compensating controls. Other organizations may delay completing assignment and selection statements in the controls until after the supplementation activities have been completed. Organizations may also discover that when fully specifying security controls for the intended environments of operation, there may be difficulties that arise which may trigger the need for additional (supplemental) controls. Finally, the security control tailoring process is not static—that is, organizations revisit the tailoring step as often as needed based on ongoing organizational assessments of risk.

[88] The security control selection process also applies to common control providers and the authorizing officials rendering authorization decisions for common controls deployed within organizations.

In addition to the iterative and dynamic nature of the security control tailoring process, there may also be side effects as controls are added and removed from the baselines. Security controls in Appendix F can have some degree of dependency and functional overlap with other controls. In many cases, security controls work together to achieve a security capability. Thus, removing a particular security control from a baseline during the tailoring process may have unintended side effects (and potentially adverse impacts) on the remaining controls. Alternatively, adding a new security control to a baseline during the tailoring process may eliminate or reduce the need for certain specific controls because the new control provides a better security capability than the capability provided by other controls. For example, if organizations implement SC-30 (2) using virtualization techniques to randomly/frequently deploy diverse and changing operating systems and applications, this approach could potentially limit the requirement to update the security configurations in CM-2 (2). Therefore, the addition or removal of security controls is viewed with regard to the totality of the information security needs of the organization and its information systems, and not simply with regard to the controls being added or removed.

Implementation Tip

In diverging from the security control baselines during the tailoring process, organizations consider some very important linkages between various controls and control enhancements. These linkages are captured in the selection of controls and enhancements in the baselines and are especially significant when developing overlays (described in Section 3.3 and Appendix I). In some instances, the linkages are such that it is not meaningful to include a security control or control enhancement without some other control or enhancement. The totality of the controls and enhancements provide a required *security capability*. Some linkages are obvious such as the linkage between Mandatory Access Control enhancement (AC-3 (3)) and Security Attributes (AC-16). But other linkages may be more subtle. This is especially true in the case where the linkage is between security functionality-related controls and security assurance-related controls as described in Appendix E. For example, it is not particularly meaningful to implement AC-3 (3) without also implementing a Reference Monitor (AC-25). Organizations are encouraged to pay careful attention to the *related controls* section of the *Supplemental Guidance* for the security controls to help in identifying such linkages.

Other Considerations

Organizational tailoring decisions are not carried out in a vacuum. While such decisions are rightly focused on information security considerations, it is important that the decisions be aligned with other risk factors that organizations address routinely. Risk factors such as cost, schedule, and performance are considered in the overall determination of which security controls to employ in organizational information systems and environments of operation. For example, in military command and control systems in which lives may be at stake, the adoption of security controls is balanced with operational necessity. With respect to the air traffic control system and consoles used by air traffic controllers, the need to access the consoles in real time to control the air space outweighs the security need for an AC-11, Session Lock. In short, the security control selection process (to include tailoring activities described in Section 3.2) should be integrated into the overall risk management process as described in NIST Special Publication 800-39.

Finally, organizations factor scalability into the security control selection process—that is, controls are scalable with regard to the extent/rigor of the implementation. Scalability is guided by the FIPS Publication 199 security categorizations and the associated FIPS Publication 200 impact levels of the information systems where the controls are to be applied. For example, contingency plans for high-impact information systems may contain significant amounts of

implementation detail and be quite lengthy. In contrast, contingency plans for low-impact systems may contain considerably less detail and be quite succinct. Organizations use discretion in applying the security controls to organizational information systems, giving consideration to the scalability factors in particular operational environments. Scaling controls to the appropriate system impact level facilitates a more cost-effective, risk-based approach to security control implementation—expending only the level of resources necessary to achieve sufficient risk mitigation and adequate security.

Implementation Tip

Maintaining a record of security control selection and control status can be addressed in one or multiple documents or security plans. If using multiple documents, consider providing references to the necessary information in the relevant documents rather than requiring duplication of information. Using references to relevant documentation reduces the amount of time and resources needed by organizations to generate such information. Other benefits include greater security awareness and understanding of the information system capabilities. Increased security awareness/understanding supports more effective integration of information security into organizational information systems.

3.5 NEW DEVELOPMENT AND LEGACY SYSTEMS

The security control selection process described in this section can be applied to organizational information systems from two different perspectives: (i) new development; and (ii) legacy. For new development systems, the security control selection process is applied from a *requirements definition* perspective since the systems do not yet exist and organizations are conducting initial security categorizations. The security controls included in the security plans for the information systems serve as a security specification and are expected to be incorporated into the systems during the development and implementation phases of the system development life cycle. In contrast, for legacy information systems, the security control selection process is applied from a *gap analysis* perspective when organizations are anticipating significant changes to the systems (e.g., during major upgrades, modifications, or outsourcing). Since the information systems already exist, organizations in all likelihood have completed the security categorization and security control selection processes resulting in the establishment of previously agreed-upon security controls in the respective security plans and the implementation of those controls within the information systems. Therefore, the gap analysis can be applied in the following manner:

- First, *reconfirm* or *update* as necessary, the security category and impact level for the information system based on the types of information that are *currently* being processed, stored, or transmitted by the system.
- Second, *review* the existing security plan that describes the security controls that are currently employed considering any updates to the security category and information system impact level as well as any changes to the organization, mission/business processes, the system, or the operational environment. Reassess the risk and revise the security plan as necessary, including documenting any additional security controls that *would* be needed by the system to ensure that the risk to organizational operations, organizational assets, individuals, other organizations, and the Nation, remains at an acceptable level.
- Third, *implement* the security controls described in the updated security plan, document in the plan of action and milestones any controls not implemented, and continue with the remaining steps in the Risk Management Framework in the same manner as a new development system.

Applying Gap Analyses to External Service Providers

The gap analysis perspective is also applied when interacting with external service providers. As described in Section 2.5, organizations are becoming increasingly reliant on external providers for information system services. Using the steps in the gap analysis described above, organizations can effectively use the acquisition process and appropriate contractual vehicles to require external providers to carry out the security categorization and security control selection steps in the RMF. The resulting information can help determine what security controls the external provider either has in place or intends to implement for the information system services that are to be provided. If a security control deficit exists, the responsibility for adequately mitigating unacceptable risks arising from the use of external information system services remains with authorizing officials. In such situations, organizations can reduce the organizational risk to an acceptable level by:

- Using the existing contractual vehicle to require the external provider to meet the additional security control requirements established by the organization;
- Negotiating with the provider for additional security controls if the existing contractual vehicle does not provide for such added requirements;
- Approving the use of compensating controls by the provider; or
- Employing alternative risk mitigation actions[89] within the organizational information system when a contract either does not exist or the contract does not provide the necessary leverage for organizations to obtain the needed security controls.

Implementation Tip

Many organizations operate and maintain complex information systems, often referred to as a system-of-systems. Enterprise architecture plays a key part in the security control selection process for these types of information systems. Organizations can address the complex system problem by dividing the system into two or more subsystems and applying the FIPS 199 security categorization and FIPS 200 impact level determination to each subsystem. Applying separate impact levels to each subsystem does not change the overall impact level of the information system; rather, it allows constituent subsystems to receive a separate allocation of security controls instead of deploying higher-impact controls across every subsystem. It is not valid to treat the subsystems as entirely independent entities, however, since the subsystems are interdependent and interconnected.

Organizations develop security architectures to allocate security controls among subsystems including monitoring and controlling communications at key internal boundaries within the system and provide system-wide controls that meet or exceed the highest information system impact level of the constituent subsystems inheriting security capabilities from those controls. Organizations also consider that replicated subsystems within complex systems may exhibit common vulnerabilities that can be exploited by common threat sources—thereby negating the redundancy that might be relied upon as a risk mitigation measure. The impact due to a security incident against one constituent subsystem might cascade and impact many subsystems at the same time.

[89] For example, local policies, procedures, and/or compensating controls could be established by organizations to serve as alternative mitigation actions for risks identified in a gap analysis.

APPENDIX A

REFERENCES

LAWS, POLICIES, DIRECTIVES, REGULATIONS, MEMORANDA, STANDARDS, AND GUIDELINES

LEGISLATION AND EXECUTIVE ORDERS

1. E-Government Act [includes FISMA] (P.L. 107-347), December 2002.
2. Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.
3. Paperwork Reduction Act (P.L. 104-13), May 1995.
4. USA PATRIOT Act (P.L. 107-56), October 2001.
5. Privacy Act of 1974 (P.L. 93-579), December 1974.
6. Freedom of Information Act (FOIA), 5 U.S.C. § 552, As Amended By Public Law No. 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996.
7. Health Insurance Portability and Accountability Act (P.L. 104-191), August 1996.
8. The Atomic Energy Act of 1954 (P.L. 83-703), August 1954.
9. Executive Order 13556, Controlled Unclassified Information, November 2010.
10. Executive Order 13587, Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, October 2011.

POLICIES, DIRECTIVES, INSTRUCTIONS, REGULATIONS, AND MEMORANDA

1. Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, November 2012.
2. Code of Federal Regulations, Title 5, *Administrative Personnel*, Section 731.106, *Designation of Public Trust Positions and Investigative Requirements* (5 C.F.R. 731.106).
3. Code of Federal Regulations, Part 5 Administrative Personnel, Subpart C—Employees Responsible for the Management or Use of Federal Computer Systems, Section 930.301 through 930.305 (5 C.F.R. 930.301-305).
4. Committee on National Security Systems Policy (CNSSP) No. 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products*, July 2003.
5. Committee on National Security Systems Policy (CNSSP) No. 12, *National Information Assurance Policy for Space Systems Used to Support National Security Missions*, March 2007.
6. Committee on National Security Systems (CNSS) Instruction 4009, *National Information Assurance Glossary*, April 2010.
7. Committee on National Security Systems (CNSS) Instruction 1253, Version 2, *Security Categorization and Control Selection for National Security Systems*, March 2012.
8. Committee on National Security Systems Directive (CNSSD) No. 504, *Directive on Protecting National Security Systems from Insider Threat*, January 2012.
9. Department of Homeland Security, *National Infrastructure Protection Plan (NIPP)*, 2009.

10. Intelligence Community Directive (ICD) 705, *Sensitive Compartmented Information Facilities*, May 2010.

11. Federal Continuity Directive 1 (FCD 1), *Federal Executive Branch National Continuity Program and Requirements*, February 2008.

12. Executive Office of the President of the United States and Federal CIO Council, *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance*, December 2011.

13. Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 2003.

14. Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 2004.

15. Homeland Security Presidential Directive 20 (National Security Presidential Directive 51), *National Continuity Policy*, May 2007.

16. Intelligence Community Directive Number 704, *Personnel Security Standards and Procedures Governing Eligibility For Access To Sensitive Compartmented Information And Other Controlled Access Program Information*, October 2008.

17. National Communications System (NCS) Directive 3-10, *Minimum Requirements for Continuity Communications Capabilities*, July 2007.

18. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7003, *Protective Distribution Systems (PDS)*, December 1996.

19. Office of Management and Budget Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.

20. Office of Management and Budget, Federal Enterprise Architecture Program Management Office, *FEA Consolidated Reference Model Document*, Version 2.3, October 2007.

21. Office of Management and Budget, *Federal Segment Architecture Methodology (FSAM)*, January 2009.

22. Office of Management and Budget Memorandum 01-05, *Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy*, December 2000.

23. Office of Management and Budget Memorandum 02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 2001.

24. Office of Management and Budget Memorandum 03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting*, August 2003.

25. Office of Management and Budget Memorandum 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 2003.

26. Office of Management and Budget Memorandum 04-04, *E-Authentication Guidance for Federal Agencies*, December 2003.

27. Office of Management and Budget Memorandum 04-26, *Personal Use Policies and File Sharing Technology*, September 2004.

28. Office of Management and Budget Memorandum 05-08, *Designation of Senior Agency Officials for Privacy*, February 2005.

29. Office of Management and Budget Memorandum 05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors*, August 2005.

30. Office of Management and Budget Memorandum 06-15, *Safeguarding Personally Identifiable Information*, May 2006.

31. Office of Management and Budget Memorandum 06-16, *Protection of Sensitive Information*, June 2006.

32. Office of Management and Budget Memorandum 06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 2006.

33. Office of Management and Budget Memorandum, *Recommendations for Identity Theft Related Data Breach Notification Guidance*, September 2006.

34. Office of Management and Budget Memorandum 07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*, March 2007.

35. Office of Management and Budget Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 2007.

36. Office of Management and Budget Memorandum 07-18, *Ensuring New Acquisitions Include Common Security Configurations*, June 2007.

37. Office of Management and Budget Memorandum 08-22, *Guidance on the Federal Desktop Core Configuration (FDCC),* August 2008.

38. Office of Management and Budget Memorandum 08-23, *Securing the Federal Government's Domain Name System Infrastructure*, August 2008.

39. The White House, Office of the Press Secretary, *Designation and Sharing of Controlled Unclassified Information (CUI)*, May 2008.

40. The White House, Office of the Press Secretary, *Classified Information and Controlled Unclassified Information*, May 2009.

41. Office of Management and Budget Memorandum 11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors*, February 2011.

42. Office of Management and Budget Memorandum, *Requirements for Accepting Externally-Issued Identity Credentials*, October 2011.

43. Office of Management and Budget Memorandum 11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, September 2011.

STANDARDS

1. International Organization for Standardization/International Electrotechnical Commission 27001:2005, *Security techniques -- Information security management systems -- Requirements*.

2. International Organization for Standardization/International Electrotechnical Commission 15408-1:2009, *Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model*.

3. International Organization for Standardization/International Electrotechnical Commission 15408-2:2008, *Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements*.

4. International Organization for Standardization/International Electrotechnical Commission 15408-3:2008, *Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements*.

5. National Institute of Standards and Technology Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*, May 2001. National Institute of Standards and Technology Federal Information Processing Standards Publication 140-3 (Draft), *Security Requirements for Cryptographic Modules*, December 2009.

6. National Institute of Standards and Technology Federal Information Processing Standards Publication 180-4, *Secure Hash Standard (SHS)*, March 2012.

7. National Institute of Standards and Technology Federal Information Processing Standards Publication 186-3, *Digital Signature Standard (DSS)*, June 2009.

8. National Institute of Standards and Technology Federal Information Processing Standards Publication 188, *Standard Security Label for Information Transfer*, September 1994.

9. National Institute of Standards and Technology Federal Information Processing Standards Publication 190, *Guideline for the Use of Advanced Authentication Technology Alternatives*, September 1994.

10. National Institute of Standards and Technology Federal Information Processing Standards Publication 197, *Advanced Encryption Standard (AES)*, November 2001.

11. National Institute of Standards and Technology Federal Information Processing Standards Publication 198-1, *The Keyed-Hash Message Authentication Code (HMAC)*, July 2008.

12. National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

13. National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

14. National Institute of Standards and Technology Federal Information Processing Standards Publication 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, March 2006.

GUIDELINES AND INTERAGENCY REPORTS

1. National Institute of Standards and Technology Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.

2. National Institute of Standards and Technology Special Publication 800-13, *Telecommunications Security Guidelines for Telecommunications Management Network*, October 1995.

3. National Institute of Standards and Technology Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996.

4. National Institute of Standards and Technology Special Publication 800-15, *Minimum Interoperability Specification for PKI Components (MISPC),* Version 1, January 1998.

5. National Institute of Standards and Technology Special Publication 800-16, *Information Security Training Requirements: A Role- and Performance-Based Model*, April 1998.

6. National Institute of Standards and Technology Special Publication 800-17, *Modes of Operation Validation System (MOVS): Requirements and Procedures*, February 1998.

7. National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems,* February 2006.

8. National Institute of Standards and Technology Special Publication 800-19, *Mobile Agent Security*, October 1999.

9. National Institute of Standards and Technology Special Publication 800-20, *Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS)*: *Requirements and Procedures*, October 1999.

10. National Institute of Standards and Technology Special Publication 800-21-1, *Second Edition, Guideline for Implementing Cryptography in the Federal Government*, December 2005.

11. National Institute of Standards and Technology Special Publication 800-22, Revision 1a, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, April 2010.

12. National Institute of Standards and Technology Special Publication 800-23, *Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, August 2000.

13. National Institute of Standards and Technology Special Publication 800-24, *PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does,* August 2000.

14. National Institute of Standards and Technology Special Publication 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication,* October 2000.

15. National Institute of Standards and Technology Special Publication 800-27, Revision A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security),* June 2004.

16. National Institute of Standards and Technology Special Publication 800-28, Version 2, *Guidelines on Active Content and Mobile Code,* March 2008.

17. National Institute of Standards and Technology Special Publication 800-29, *A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2*, June 2001.

18. National Institute of Standards and Technology Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments,* September 2012.

19. National Institute of Standards and Technology Special Publication 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure,* February 2001.

20. National Institute of Standards and Technology Special Publication 800-33, *Underlying Technical Models for Information Technology Security*, December 2001.

21. National Institute of Standards and Technology Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, May 2010.

22. National Institute of Standards and Technology Special Publication 800-35, *Guide to Information Technology Security Services*, October 2003.

23. National Institute of Standards and Technology Special Publication 800-36, *Guide to Selecting Information Security Products*, October 2003.

24. National Institute of Standards and Technology Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010.

25. National Institute of Standards and Technology Special Publication 800-38A—Addendum, *Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode*, October 2010.

26. National Institute of Standards and Technology Special Publication 800-38B, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, May 2005.

27. National Institute of Standards and Technology Special Publication 800-38C, *Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality*, May 2004.

28. National Institute of Standards and Technology Special Publication 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*, November 2007.

29. National Institute of Standards and Technology Special Publication 800-38E, *Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices*, January 2010.

30. National Institute of Standards and Technology Special Publication 800-38F, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*, December 2012.

31. National Institute of Standards and Technology Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011.

32. National Institute of Standards and Technology Special Publication 800-40, Version 2, *Creating a Patch and Vulnerability Management Program*, November 2005.

33. National Institute of Standards and Technology Special Publication 800-41, Revision 1, *Guidelines on Firewalls and Firewall Policy*, September 2009.

34. National Institute of Standards and Technology Special Publication 800-43, *Systems Administration Guidance for Windows 2000 Professional System*, November 2002.

35. National Institute of Standards and Technology Special Publication 800-44, Version 2, *Guidelines on Securing Public Web Servers*, September 2007.

36. National Institute of Standards and Technology Special Publication 800-45, Version 2, *Guidelines on Electronic Mail Security*, February 2007.

37. National Institute of Standards and Technology Special Publication 800-46, Revision 1, *Guide to Enterprise Telework and Remote Access Security*, June 2009.

38. National Institute of Standards and Technology Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002.

39. National Institute of Standards and Technology Special Publication 800-48, Revision 1, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*, July 2008.

40. National Institute of Standards and Technology Special Publication 800-49, *Federal S/MIME V3 Client Profile*, November 2002.

41. National Institute of Standards and Technology Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003.

42. National Institute of Standards and Technology Special Publication 800-51, Revision 1, *Guide to Using Vulnerability Naming Schemes*, February 2011.

43. National Institute of Standards and Technology Special Publication 800-52, Revision 1 (Draft), *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*, September 2013.

44. National Institute of Standards and Technology Special Publication 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*, June 2010.

45. National Institute of Standards and Technology Special Publication 800-54, *Border Gateway Protocol Security*, July 2007.

46. National Institute of Standards and Technology Special Publication 800-55, Revision 1, *Performance Measurement Guide for Information Security*, July 2008.

47. National Institute of Standards and Technology Special Publication 800-56A (Revised), *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, March 2007.

48. National Institute of Standards and Technology Special Publication 800-57 Revision 3, *Recommendation for Key Management*, July 2012.

49. National Institute of Standards and Technology Special Publication 800-58, *Security Considerations for Voice Over IP Systems*, January 2005.

50. National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.

51. National Institute of Standards and Technology Special Publication 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008.

52. National Institute of Standards and Technology Special Publication 800-61, Revision 2, *Computer Security Incident Handling Guide*, August 2012.

53. National Institute of Standards and Technology Special Publication 800-63-1, *Electronic Authentication Guideline*, December 2011.

54. National Institute of Standards and Technology Special Publication 800-64, Revision 2, *Security Considerations in the System Development Life Cycle*, October 2008.

55. National Institute of Standards and Technology Special Publication 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*, January 2005.

56. National Institute of Standards and Technology Special Publication 800-66, Revision 1, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, October 2008.

57. National Institute of Standards and Technology Special Publication 800-67, Revision 1, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, January 2012.

58. National Institute of Standards and Technology Special Publication 800-68, Revision 1, *Guide to Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*, October 2008.

59. National Institute of Standards and Technology Special Publication 800-69, *Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist*, September 2006.

60. National Institute of Standards and Technology Special Publication 800-70, Revision 2, *National Checklist Program for IT Products--Guidelines for Checklist Users and Developers*, February 2011.

61. National Institute of Standards and Technology Special Publication 800-72, *Guidelines on PDA Forensics*, November 2004.

62. National Institute of Standards and Technology Special Publication 800-73-3, *Interfaces for Personal Identity Verification*, February 2010.

63. National Institute of Standards and Technology Special Publication 800-76-1, *Biometric Data Specification for Personal Identity Verification*, January 2007.

64. National Institute of Standards and Technology Special Publication 800-77, *Guide to IPsec VPNs*, December 2005.

65. National Institute of Standards and Technology Special Publication 800-78-3, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification (PIV)*, December 2010.

66. National Institute of Standards and Technology Special Publication 800-79-1, *Guidelines for the Accreditation of Personal Identity Verification Card Issuers*, June 2008.

67. National Institute of Standards and Technology Special Publication 800-81, *Secure Domain Name System (DNS) Deployment Guide*, Revision 1, April 2010.

68. National Institute of Standards and Technology Special Publication 800-82, Revision 1, *Guide to Industrial Control Systems (ICS) Security*, April 2013.

69. National Institute of Standards and Technology Special Publication 800-83, *Guide to Malware Incident Prevention and Handling*, November 2005.

70. National Institute of Standards and Technology Special Publication 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006.

71. National Institute of Standards and Technology Special Publication 800-85A-2, *PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-3 Compliance)*, July 2010.

72. National Institute of Standards and Technology Special Publication 800-85B-1, (Draft) *PIV Data Model Test Guidelines*, September 2009.

73. National Institute of Standards and Technology Special Publication 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, August 2006.

74. National Institute of Standards and Technology Special Publication 800-87, Revision 1, *Codes for the Identification of Federal and Federally-Assisted Organizations*, April 2008.

75. National Institute of Standards and Technology Special Publication 800-88, *Guidelines for Media Sanitization*, September 2006.

76. National Institute of Standards and Technology Special Publication 800-89, *Recommendation for Obtaining Assurances for Digital Signature Applications*, November 2006.

77. National Institute of Standards and Technology Special Publication 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, January 2012.

78. National Institute of Standards and Technology Special Publication 800-92, *Guide to Computer Security Log Management*, September 2006.

79. National Institute of Standards and Technology Special Publication 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, February 2007.

80. National Institute of Standards and Technology Special Publication 800-95, *Guide to Secure Web Services*, August 2007.

81. National Institute of Standards and Technology Special Publication 800-96, *PIV Card / Reader Interoperability Guidelines*, September 2006.

82. National Institute of Standards and Technology Special Publication 800-97, *Establishing Robust Security Networks: A Guide to IEEE 802.11i*, February 2007.

83. National Institute of Standards and Technology Special Publication 800-98, *Guidelines for Securing Radio Frequency Identification (RFID) Systems*, April 2007.

84. National Institute of Standards and Technology Special Publication 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.

85. National Institute of Standards and Technology Special Publication 800-101, *Guidelines on Cell Phone Forensics*, May 2007.

86. National Institute of Standards and Technology Special Publication 800-103 (Draft), *An Ontology of Identity Credentials, Part I: Background and Formulation*, October 2006.

87. National Institute of Standards and Technology Special Publication 800-104, *A Scheme for PIV Visual Card Topography*, June 2007.

88. National Institute of Standards and Technology Special Publication 800-106, *Randomized Hashing Digital Signatures*, February 2009.

89. National Institute of Standards and Technology Special Publication 800-107, *Recommendation for Applications Using Approved Hash Algorithms*, August 2012.

90. National Institute of Standards and Technology Special Publication 800-108, *Recommendation for Key Derivation Using Pseudorandom Functions*, October 2009.

91. National Institute of Standards and Technology Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*, November 2007.

92. National Institute of Standards and Technology Special Publication 800-113, *Guide to SSL VPNs*, July 2008.

93. National Institute of Standards and Technology Special Publication 800-114, *User's Guide to Securing External Devices for Telework and Remote Access*, November 2007.

94. National Institute of Standards and Technology Special Publication 800-115, *Technical Guide to Information Security Testing and Assessment*, September 2008.

95. National Institute of Standards and Technology Special Publication 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*, November 2008.

96. National Institute of Standards and Technology Special Publication 800-117, Version 1.0, *Guide to Adopting and Using the Security Content Automation Protocol (SCAP)*, July 2010.

97. National Institute of Standards and Technology Special Publication 800-118 (Draft), *Guide to Enterprise Password Management*, April 2009.

98. National Institute of Standards and Technology Special Publication 800-121, Revision 1, *Guide to Bluetooth Security*, June 2012.

99. National Institute of Standards and Technology Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010.

100. National Institute of Standards and Technology Special Publication 800-123, *Guide to General Server Security*, July 2008.

101. National Institute of Standards and Technology Special Publication 800-124, *Guidelines on Cell Phone and PDA Security*, October 2008.

102. National Institute of Standards and Technology Special Publication 800-125, *Guide to Security for Full Virtualization Technologies*, January 2011.

103. National Institute of Standards and Technology Special Publication 800-126, Revision 2, *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2*, September 2011.

104. National Institute of Standards and Technology Special Publication 800-127, *Guide to Securing WiMAX Wireless Communications*, September 2010.

105. National Institute of Standards and Technology Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, August 2011.

106. National Institute of Standards and Technology Special Publication 800-133, *Recommendation for Cryptographic Key Generation*, December 2012.

107. National Institute of Standards and Technology Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, September 2011.

108. National Institute of Standards and Technology Special Publication 800-142, *Practical Combinatorial Testing*, October 2010.

109. National Institute of Standards and Technology Special Publication 800-144, *Guidelines for Security and Privacy in Public Cloud Computing*, December 2011.

110. National Institute of Standards and Technology Special Publication 800-145, *The NIST Definition of Cloud Computing*, September 2011.

111. National Institute of Standards and Technology Special Publication 800-146, *Cloud Computing Synopsis and Recommendations*, May 2012.

112. National Institute of Standards and Technology Special Publication 800-147, *Basic Input/Output System (BIOS) Protection Guidelines*, April 2011.

113. National Institute of Standards and Technology Special Publication 800-153, *Guidelines for Securing Wireless Local Area Networks (WLANs)*, September 2011.

114. National Institute of Standards and Technology Interagency Report 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems*, October 2012.

APPENDIX B

GLOSSARY

COMMON TERMS AND DEFINITIONS

Appendix B provides definitions for security terminology used within Special Publication 800-53. Unless specifically defined in this glossary, all terms used in this publication are consistent with the definitions contained in CNSS Instruction 4009, *National Information Assurance Glossary*.

Adequate Security [OMB Circular A-130, Appendix III, Adapted]	Security commensurate with the risk resulting from the loss, misuse, or unauthorized access to or modification of information.
Advanced Persistent Threat	An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.
Agency	See *Executive Agency*.
All Source Intelligence [Department of Defense, Joint Publication 1-02]	Intelligence products and/or organizations and activities that incorporate all sources of information, most frequently including human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open source data in the production of finished intelligence.
Assessment	See *Security Control Assessment*.
Assessor	See *Security Control Assessor*.
Assurance [CNSSI 4009]	Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy.
Assurance Case [Software Engineering Institute, Carnegie Mellon University]	A structured set of arguments and a body of evidence showing that an information system satisfies specific claims with respect to a given quality attribute.
Audit Log [CNSSI 4009]	A chronological record of information system activities, including records of system accesses and operations performed in a given period.
Audit Record	An individual entry in an audit log related to an audited event.

Audit Reduction Tools [CNSSI 4009]	Preprocessors designed to reduce the volume of audit records to facilitate manual review. Before a security review, these tools can remove many audit records known to have little security significance. These tools generally remove records generated by specified classes of events, such as records generated by nightly backups.
Audit Trail [CNSSI 4009]	A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security-relevant transaction from inception to final result.
Authentication [FIPS 200]	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authenticator	The means used to confirm the identity of a user, processor, or device (e.g., user password or token).
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See *Authentication*.
Authorization (to operate)	The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.
Authorization Boundary	All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.
Authorize Processing	See *Authorization*.
Authorizing Official	A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
Availability [44 U.S.C., Sec. 3542]	Ensuring timely and reliable access to and use of information.
Baseline Configuration	A documented set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.

Blacklisting	The process used to identify: (i) software programs that are not authorized to execute on an information system; or (ii) prohibited Universal Resource Locators (URL)/websites.
Boundary Protection	Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., gateways, routers, firewalls, guards, encrypted tunnels).
Boundary Protection Device	A device with appropriate mechanisms that: (i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or (ii) provides information system boundary protection.
Central Management	The organization-wide management and implementation of selected security controls and related processes. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed security controls and processes.
Chief Information Officer [PL 104-106, Sec. 5125(b)]	Agency official responsible for: (i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; (ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and (iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency. Note: Organizations subordinate to federal agencies may use the term *Chief Information Officer* to denote individuals filling positions with similar security responsibilities to agency-level Chief Information Officers.
Chief Information Security Officer	See *Senior Agency Information Security Officer*.
Chief Privacy Officer	See *Senior Agency Official for Privacy*.
Classified Information	Information that has been determined: (i) pursuant to Executive Order 12958 as amended by Executive Order 13526, or any predecessor Order, to be classified national security information; or (ii) pursuant to the Atomic Energy Act of 1954, as amended, to be Restricted Data (RD).

Commodity Service	An information system service (e.g., telecommunications service) provided by a commercial service provider typically to a large and diverse set of consumers. The organization acquiring and/or receiving the commodity service possesses limited visibility into the management structure and operations of the provider, and while the organization may be able to negotiate service-level agreements, the organization is typically not in a position to require that the provider implement specific security controls.
Common Carrier	In a telecommunications context, a telecommunications company that holds itself out to the public for hire to provide communications transmission services. Note: In the United States, such companies are usually subject to regulation by federal and state regulatory commissions.
Common Control [NIST SP 800-37; CNSSI 4009]	A security control that is inheritable by one or more organizational information systems. See *Security Control Inheritance*.
Common Control Provider [NIST SP 800-37]	An organizational official responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inheritable by information systems).
Common Criteria [CNSSI 4009]	Governing document that provides a comprehensive, rigorous method for specifying security function and assurance requirements for products and systems.
Common Secure Configuration	A recognized standardized and established benchmark that stipulates specific secure configuration settings for a given information technology platform.
Compensating Security Controls [CNSSI 4009, Adapted]	The security controls employed in lieu of the recommended controls in the security control baselines described in NIST Special Publication 800-53 and CNSS Instruction 1253 that provide equivalent or comparable protection for an information system or organization.
Computer Matching Agreement	An agreement entered into by an organization in connection with a computer matching program to which the organization is a party, as required by the Computer Matching and Privacy Protection Act of 1988. With certain exceptions, a computer matching program is any computerized comparison of two or more automated systems of records or a system of records with nonfederal records for the purpose of establishing or verifying the eligibility of, or continuing compliance with, statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to cash or in-kind assistance or payments under federal benefit programs or computerized comparisons of two or more automated federal personnel or payroll systems of records or a system of federal personnel or payroll records with non-federal records.

Confidentiality [44 U.S.C., Sec. 3542]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Configuration Control [CNSSI 4009]	Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.
Configuration Item	An aggregation of information system components that is designated for configuration management and treated as a single entity in the configuration management process.
Configuration Management	A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.
Configuration Settings	The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and/or functionality of the information system.
Controlled Area	Any area or space for which an organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.
Controlled Interface [CNSSI 4009]	A boundary with a set of mechanisms that enforces the security policies and controls the flow of information between interconnected information systems.
Controlled Unclassified Information [E.O. 13556]	A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the federal government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.
Countermeasures [CNSSI 4009]	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.
Covert Channel Analysis [CNSSI 4009]	Determination of the extent to which the security policy model and subsequent lower-level program descriptions may allow unauthorized access to information.
Covert Storage Channel [CNSSI 4009]	Covert channel involving the direct or indirect writing to a storage location by one process and the direct or indirect reading of the storage location by another process. Covert storage channels typically involve a finite resource (e.g., sectors on a disk) that is shared by two subjects at different security levels.

Covert Timing Channel [CNSSI 4009]	Covert channel in which one process signals information to another process by modulating its own use of system resources (e.g., central processing unit time) in such a way that this manipulation affects the real response time observed by the second process.
Cross Domain Solution [CNSSI 4009]	A form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains.
Cyber Attack [CNSSI 4009]	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.
Cyber Security [CNSSI 4009]	The ability to protect or defend the use of cyberspace from cyber attacks.
Cyberspace [CNSSI 4009]	A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.
Data Mining/Harvesting	An analytical process that attempts to find correlations or patterns in large data sets for the purpose of data or knowledge discovery.
Defense-in-Breadth [CNSSI 4009]	A planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or subcomponent life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement).
Defense-in-Depth	Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.
Developer	A general term that includes: (i) developers or manufacturers of information systems, system components, or information system services; (ii) systems integrators; (iii) vendors; (iv) and product resellers. Development of systems, components, or services can occur internally within organizations (i.e., in-house development) or through external entities.
Digital Media	A form of electronic media where data are stored in digital (as opposed to analog) form.

Discretionary Access Control	An access control policy that is enforced over all subjects and objects in an information system where the policy specifies that a subject that has been granted access to information can do one or more of the following: (i) pass the information to other subjects or objects; (ii) grant its privileges to other subjects; (iii) change security attributes on subjects, objects, information systems, or system components; (iv) choose the security attributes to be associated with newly-created or revised objects; or (v) change the rules governing access control. Mandatory access controls restrict this capability.
[CNSSI 4009]	A means of restricting access to objects (e.g., files, data entities) based on the identity and need-to-know of subjects (e.g., users, processes) and/or groups to which the object belongs. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control).
Domain [CNSSI 4009]	An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. See *Security Domain*.
Enterprise [CNSSI 4009]	An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management. See *Organization*.
Enterprise Architecture [44 U.S.C. Sec. 3601]	A strategic information asset base, which defines the mission; the information necessary to perform the mission; the technologies necessary to perform the mission; and the transitional processes for implementing new technologies in response to changing mission needs; and includes a baseline architecture; a target architecture; and a sequencing plan.
Environment of Operation [NIST SP 800-37]	The physical surroundings in which an information system processes, stores, and transmits information.
Event [CNSSI 4009, Adapted]	Any observable occurrence in an information system.
Executive Agency [41 U.S.C., Sec. 403]	An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.
Exfiltration	The unauthorized transfer of information from an information system.

External Information System (or Component)	An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.
External Information System Service	An information system service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.
External Information System Service Provider	A provider of external information system services to an organization through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges.
External Network	A network not controlled by the organization.
Failover	The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination of the previously active system.
Fair Information Practice Principles	Principles that are widely accepted in the United States and internationally as a general framework for privacy and that are reflected in various federal and international laws and policies. In a number of organizations, the principles serve as the basis for analyzing privacy risks and determining appropriate mitigation strategies.
Federal Agency	See *Executive Agency*.
Federal Enterprise Architecture [FEA Program Management Office]	A business-based framework for governmentwide improvement developed by the Office of Management and Budget that is intended to facilitate efforts to transform the federal government to one that is citizen-centered, results-oriented, and market-based.
Federal Information System [40 U.S.C., Sec. 11331]	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
FIPS-Validated Cryptography	A cryptographic module validated by the Cryptographic Module Validation Program (CMVP) to meet requirements specified in FIPS Publication 140-2 (as amended). As a prerequisite to CMVP validation, the cryptographic module is required to employ a cryptographic algorithm implementation that has successfully passed validation testing by the Cryptographic Algorithm Validation Program (CAVP). See *NSA-Approved Cryptography*.

Firmware [CNSSI 4009]	Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs.
Guard (System) [CNSSI 4009, Adapted]	A mechanism limiting the exchange of information between information systems or subsystems.
Hardware [CNSSI 4009]	The physical components of an information system. See *Software* and *Firmware*.
High-Impact System [FIPS 200]	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS Publication 199 potential impact value of high.
Hybrid Security Control [CNSSI 4009]	A security control that is implemented in an information system in part as a common control and in part as a system-specific control. See *Common Control* and *System-Specific Security Control*.
Impact	The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or an information system.
Impact Value	The assessed potential impact resulting from a compromise of the confidentiality, integrity, or availability of information expressed as a value of low, moderate or high.
Incident [FIPS 200]	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Industrial Control System	An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCSs) and smaller control systems using programmable logic controllers to control localized processes.
Information [CNSSI 4009]	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.
[FIPS 199]	An instance of an information type.
Information Leakage	The intentional or unintentional release of information to an untrusted environment.
Information Owner [CNSSI 4009]	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

Information Resources [44 U.S.C., Sec. 3502]	Information and related resources, such as personnel, equipment, funds, and information technology.
Information Security [44 U.S.C., Sec. 3542]	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Security Architecture	An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's security processes, information security systems, personnel and organizational subunits, showing their alignment with the enterprise's mission and strategic plans.
Information Security Policy [CNSSI 4009]	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
Information Security Program Plan	Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements.
Information Security Risk	The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.
Information Steward [CNSSI 4009]	An agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information System [44 U.S.C., Sec. 3502]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.
Information System Boundary	See *Authorization Boundary*.
Information System Component [NIST SP 800-128, Adapted]	A discrete, identifiable information technology asset (e.g., hardware, software, firmware) that represents a building block of an information system. Information system components include commercial information technology products.
Information System Owner (or Program Manager)	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

Information System Resilience	The ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs.
Information System Security Officer [CNSSI 4009]	Individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program.
Information System Service	A capability provided by an information system that facilitates information processing, storage, or transmission.
Information System-Related Security Risks	Risks that arise through the loss of confidentiality, integrity, or availability of information or information systems and that considers impacts to the organization (including assets, mission, functions, image, or reputation), individuals, other organizations, and the Nation. See *Risk*.
Information Technology [40 U.S.C., Sec. 1401]	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term *information technology* includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Information Technology Product	See *Information System Component*.
Information Type [FIPS 199]	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor-sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.
Insider [Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs]	Any person with authorized access to any U.S. Government resource, to include personnel, facilities, information, equipment, networks, or systems.

Insider Threat [Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs]	The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.
[CNSSI 4009]	An entity with authorized access (i.e., within the security domain) that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service.
Insider Threat Program [Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs]	A coordinated group of capabilities under centralized management that is organized to detect and prevent the unauthorized disclosure of sensitive information. At a minimum, for departments and agencies that handle classified information, an insider threat program shall consist of capabilities that provide access to information; centralized information integration, analysis, and response; employee insider threat awareness training; and the monitoring of user activity on government computers. For department and agencies that do not handle classified information, these can be employed effectively for safeguarding information that is unclassified but sensitive.
Integrity [44 U.S.C., Sec. 3542]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Internal Network	A network where: (i) the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or (ii) cryptographic encapsulation or similar security technology implemented between organization-controlled endpoints, provides the same effect (at least with regard to confidentiality and integrity). An internal network is typically organization-owned, yet may be organization-controlled while not being organization-owned.
Label	See *Security Label*.
Line of Business	The following OMB-defined process areas common to virtually all federal agencies: Case Management, Financial Management, Grants Management, Human Resources Management, Federal Health Architecture, Information Systems Security, Budget Formulation and Execution, Geospatial, and IT Infrastructure.
Local Access	Access to an organizational information system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.

Logical Access Control System [FICAM Roadmap and Implementation Guidance]	An automated system that controls an individual's ability to access one or more computer system resources such as a workstation, network, application, or database. A logical access control system requires validation of an individual's identity through some mechanism such as a PIN, card, biometric, or other token. It has the capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization.
Low-Impact System [FIPS 200]	An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS Publication 199 potential impact value of low.
Malicious Code	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
Malware	See *Malicious Code*.
Managed Interface	An interface within an information system that provides boundary protection capability using automated mechanisms or devices.
Mandatory Access Control	An access control policy that is uniformly enforced across all subjects and objects within the boundary of an information system. A subject that has been granted access to information is constrained from doing any of the following: (i) passing the information to unauthorized subjects or objects; (ii) granting its privileges to other subjects; (iii) changing one or more security attributes on subjects, objects, the information system, or system components; (iv) choosing the security attributes to be associated with newly-created or modified objects; or (v) changing the rules governing access control. Organization-defined subjects may explicitly be granted organization-defined privileges (i.e., they are trusted subjects) such that they are not limited by some or all of the above constraints.
[CNSSI 4009]	A means of restricting access to objects based on the sensitivity (as represented by a security label) of the information contained in the objects and the formal authorization (i.e., clearance, formal access approvals, and need-to-know) of subjects to access information of such sensitivity. Mandatory Access Control is a type of nondiscretionary access control.
Marking	See *Security Marking*.
Media [FIPS 200]	Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

Metadata	Information describing the characteristics of data including, for example, structural metadata describing data structures (e.g., data format, syntax, and semantics) and descriptive metadata describing data contents (e.g., information security labels).
Mobile Code	Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.
Mobile Code Technologies	Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, VBScript).
Mobile Device	A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers.
Moderate-Impact System [FIPS 200]	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS Publication 199 potential impact value of moderate and no security objective is assigned a FIPS Publication 199 potential impact value of high.
Multifactor Authentication	Authentication using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). See *Authenticator*.
Multilevel Security [CNSSI 4009]	Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization.
Multiple Security Levels [CNSSI 4009]	Capability of an information system that is trusted to contain, and maintain separation between, resources (particularly stored data) of different security domains.
National Security Emergency Preparedness Telecommunications Services [47 C.F.R., Part 64, App A]	Telecommunications services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the national security or emergency preparedness posture of the United States.

National Security System [44 U.S.C., Sec. 3542]	Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—(i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
Network [CNSSI 4009]	Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
Network Access	Access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).
Nondiscretionary Access Control	See *Mandatory Access Control*.
Nonlocal Maintenance	Maintenance activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network.
Non-Organizational User	A user who is not an organizational user (including public users).
Non-repudiation	Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.
NSA-Approved Cryptography	Cryptography that consists of: (i) an approved algorithm; (ii) an implementation that has been approved for the protection of classified information and/or controlled unclassified information in a particular environment; and (iii) a supporting key management infrastructure.
Object	Passive information system-related entity (e.g., devices, files, records, tables, processes, programs, domains) containing or receiving information. Access to an object (by a subject) implies access to the information it contains. See *Subject*.

Operations Security [CNSSI 4009]	Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.
Organization [FIPS 200, Adapted]	An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements).
Organizational User	An organizational employee or an individual the organization deems to have equivalent status of an employee including, for example, contractor, guest researcher, individual detailed from another organization. Policy and procedures for granting equivalent status of employees to individuals may include need-to-know, relationship to the organization, and citizenship.
Overlay	A specification of security controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems.
Penetration Testing	A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.
Personally Identifiable Information [OMB Memorandum 07-16]	Information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.).
Physical Access Control System [FICAM Roadmap and Implementation Guidance]	An automated system that manages the passage of people or assets through an opening(s) in a secure perimeter(s) based on a set of authorization rules.
Plan of Action and Milestones [OMB Memorandum 02-01]	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Portable Storage Device	An information system component that can be inserted into and removed from an information system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain non-volatile memory).

Potential Impact [FIPS 199]	The loss of confidentiality, integrity, or availability could be expected to have: (i) a *limited* adverse effect (FIPS Publication 199 low); (ii) a *serious* adverse effect (FIPS Publication 199 moderate); or (iii) a *severe* or *catastrophic* adverse effect (FIPS Publication 199 high) on organizational operations, organizational assets, or individuals.
Privacy Act Statement	A disclosure statement required by Section (e)(3) of the Privacy Act of 1974, as amended, to appear on documents used by organizations to collect personally identifiable information from individuals to be maintained in a Privacy Act System of Records (SORN).
Privacy Impact Assessment [OMB Memorandum 03-22]	An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
Privileged Account	An information system account with authorizations of a privileged user.
Privileged Command	A human-initiated command executed on an information system involving the control, monitoring, or administration of the system including security functions and associated security-relevant information.
Privileged User [CNSSI 4009]	A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
Protective Distribution System	Wire line or fiber optic system that includes adequate safeguards and/or countermeasures (e.g., acoustic, electric, electromagnetic, and physical) to permit its use for the transmission of unencrypted information.
Provenance	The records describing the possession of, and changes to, components, component processes, information, systems, organization, and organizational processes. Provenance enables all changes to the baselines of components, component processes, information, systems, organizations, and organizational processes, to be reported to specific actors, functions, locales, or activities.
Public Key Infrastructure [CNSSI 4009]	The framework and services that provide for the generation, production, distribution, control, accounting, and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates.

Purge	Rendering sanitized data unrecoverable by laboratory attack methods.
Reciprocity [CNSSI 4009]	Mutual agreement among participating organizations to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information.
Records	The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).
Red Team Exercise	An exercise, reflecting real-world conditions, that is conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization.
Reference Monitor	A set of design requirements on a reference validation mechanism which as key component of an operating system, enforces an access control policy over all subjects and objects. A reference validation mechanism must be: (i) always invoked (i.e., complete mediation); (ii) tamperproof; and (iii) small enough to be subject to analysis and tests, the completeness of which can be assured (i.e., verifiable).
Remote Access	Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).
Remote Maintenance	Maintenance activities conducted by individuals communicating through an external network (e.g., the Internet).
Resilience	See *Information System Resilience*.
Restricted Data [Atomic Energy Act of 1954]	All data concerning (i) design, manufacture, or utilization of atomic weapons; (ii) the production of special nuclear material; or (iii) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to Section 142 [of the Atomic Energy Act of 1954].

Risk [FIPS 200, Adapted]	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.
Risk Executive (Function) [CNSSI 4009]	An individual or group within an organization that helps to ensure that: (i) security risk-related considerations for individual information systems, to include the authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and (ii) managing risk from individual information systems is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success.
Risk Management [CNSSI 4009, adapted]	The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.
Risk Mitigation [CNSSI 4009]	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.
Risk Monitoring	Maintaining ongoing awareness of an organization's risk environment, risk management program, and associated activities to support risk decisions.
Risk Response	Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.

Role-Based Access Control	Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.
Safeguards [CNSSI 4009]	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.
Sanitization	Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means. Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs.
Scoping Considerations	A part of tailoring guidance providing organizations with specific considerations on the applicability and implementation of security controls in the security control baseline. Areas of consideration include policy/regulatory, technology, physical infrastructure, system component allocation, operational/environmental, public access, scalability, common control, and security objective.
Security [CNSSI 4009]	A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.
Security Assessment	See *Security Control Assessment*.
Security Assessment Plan	The objectives for the security control assessment and a detailed roadmap of how to conduct such an assessment.
Security Assurance	See *Assurance*.
Security Attribute	An abstraction representing the basic properties or characteristics of an entity with respect to safeguarding information; typically associated with internal data structures (e.g., records, buffers, files) within the information system and used to enable the implementation of access control and flow control policies, reflect special dissemination, handling or distribution instructions, or support other aspects of the information security policy.

Security Authorization	See *Authorization.*
Security Authorization Boundary	See *Authorization Boundary*.
Security Capability	A combination of mutually-reinforcing security controls (i.e., safeguards and countermeasures) implemented by technical means (i.e., functionality in hardware, software, and firmware), physical means (i.e., physical devices and protective measures), and procedural means (i.e., procedures performed by individuals).
Security Categorization	The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS Publication 199 for other than national security systems. See *Security Category*.
Security Category [FIPS 199, Adapted; CNSSI 4009]	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the Nation.
Security Control [FIPS 199, Adapted]	A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.
Security Control Assessment [CNSSI 4009, Adapted]	The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.
Security Control Assessor	The individual, group, or organization responsible for conducting a security control assessment.
Security Control Baseline [FIPS 200, Adapted]	The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system that provides a starting point for the tailoring process.
Security Control Enhancement	Augmentation of a security control to: (i) build in additional, but related, functionality to the control; (ii) increase the strength of the control; or (iii) add assurance to the control.
Security Control Inheritance [CNSSI 4009]	A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See *Common Control*.
Security Control Overlay	See *Overlay.*

Security Domain [CNSSI 4009]	A domain that implements a security policy and is administered by a single authority.
Security Functionality	The security-related features, functions, mechanisms, services, procedures, and architectures implemented within organizational information systems or the environments in which those systems operate.
Security Functions	The hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based.
Security Impact Analysis [CNSSI 4009]	The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.
Security Incident	See *Incident*.
Security Kernel [CNSSI 4009]	Hardware, firmware, and software elements of a trusted computing base implementing the reference monitor concept. Security kernel must mediate all accesses, be protected from modification, and be verifiable as correct.
Security Label	The means used to associate a set of security attributes with a specific information object as part of the data structure for that object.
Security Marking	The means used to associate a set of security attributes with objects in a human-readable form, to enable organizational process-based enforcement of information security policies.
Security Objective [FIPS 199]	Confidentiality, integrity, or availability.
Security Plan	Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. See *System Security Plan* or *Information Security Program Plan*.
Security Policy [CNSSI 4009]	A set of criteria for the provision of security services.
Security Policy Filter	A hardware and/or software component that performs one or more of the following functions: (i) content verification to ensure the data type of the submitted content; (ii) content inspection, analyzing the submitted content to verify it complies with a defined policy (e.g., allowed vs. disallowed file constructs and content portions); (iii) malicious content checker that evaluates the content for malicious code; (iv) suspicious activity checker that evaluates or executes the content in a safe manner, such as in a sandbox/detonation chamber and monitors for suspicious activity; or (v) content sanitization, cleansing, and transformation, which modifies the submitted content to comply with a defined policy.

Security Requirement [FIPS 200, Adapted]	A requirement levied on an information system or an organization that is derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, and/or mission/business needs to ensure the confidentiality, integrity, and availability of information that is being processed, stored, or transmitted. Note: Security requirements can be used in a variety of contexts from high-level policy-related activities to low-level implementation-related activities in system development and engineering disciplines.
Security Service [CNSSI 4009]	A capability that supports one, or more, of the security requirements (Confidentiality, Integrity, Availability). Examples of security services are key management, access control, and authentication.
Security-Relevant Information	Any information within the information system that can potentially impact the operation of security functions or the provision of security services in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data.
Senior Agency Information Security Officer [44 U.S.C., Sec. 3544]	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers. Note: Organizations subordinate to federal agencies may use the term *Senior Information Security Officer* or *Chief Information Security Officer* to denote individuals filling positions with similar responsibilities to Senior Agency Information Security Officers.
Senior Agency Official for Privacy	The senior organizational official with overall organization-wide responsibility for information privacy issues.
Senior Information Security Officer	See *Senior Agency Information Security Officer*.
Sensitive Information [CNSSI 4009, Adapted]	Information where the loss, misuse, or unauthorized access or modification could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act); that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
Sensitive Compartmented Information [CNSSI 4009]	Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of National Intelligence.
Service-Oriented Architecture	A set of principles and methodologies for designing and developing software in the form of interoperable services. These services are well-defined business functions that are built as software components (i.e., discrete pieces of code and/or data structures) that can be reused for different purposes.

Software [CNSSI 4009]	Computer programs and associated data that may be dynamically written or modified during execution.
Spam	The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.
Special Access Program [CNSSI 4009]	A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.
Spyware	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.
Subject	Generally an individual, process, or device causing information to flow among objects or change to the system state. See *Object*.
Subsystem	A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions.
Supplemental Guidance	Statements used to provide additional explanatory information for security controls or security control enhancements.
Supplementation	The process of adding security controls or control enhancements to a security control baseline as part of the tailoring process (during security control selection) in order to adequately meet the organization's risk management needs.
Supply Chain [ISO 28001, Adapted]	Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.
Supply Chain Element	An information technology product or product component that contains programmable logic and that is critically important to the functioning of an information system.
System	See *Information System*.
System of Records Notice	An official public notice of an organization's system(s) of records, as required by the Privacy Act of 1974, that identifies: (i) the purpose for the system of records; (ii) the individuals covered by information in the system of records; (iii) the categories of records maintained about individuals; and (iv) the ways in which the information is shared.
System Security Plan [NIST SP 800-18]	Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

System-Specific Security Control	A security control for an information system that has not been designated as a common security control or the portion of a hybrid control that is to be implemented within an information system.
Tailored Security Control Baseline	A set of security controls resulting from the application of tailoring guidance to a security control baseline. See *Tailoring*.
Tailoring	The process by which security control baselines are modified by: (i) identifying and designating common controls; (ii) applying scoping considerations on the applicability and implementation of baseline controls; (iii) selecting compensating security controls; (iv) assigning specific values to organization-defined security control parameters; (v) supplementing baselines with additional security controls or control enhancements; and (vi) providing additional specification information for control implementation.
Threat [CNSSI 4009, Adapted]	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Threat Assessment [CNSSI 4009]	Formal description and evaluation of threat to an information system.
Threat Source [FIPS 200]	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent.
Trusted Path	A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can only be activated by the user or the security functions of the information system and cannot be imitated by untrusted software.
Trustworthiness [CNSSI 4009]	The attribute of a person or enterprise that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities.
Trustworthiness (Information System)	The degree to which an information system (including the information technology components that are used to build the system) can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system across the full range of threats. A trustworthy information system is a system that is believed to be capable of operating within defined levels of risk despite the environmental disruptions, human errors, structural failures, and purposeful attacks that are expected to occur in its environment of operation.

User [CNSSI 4009, adapted]	Individual, or (system) process acting on behalf of an individual, authorized to access an information system. See *Organizational User* and *Non-Organizational User*.
Virtual Private Network [CNSSI 4009]	Protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line.
Vulnerability [CNSSI 4009]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Vulnerability Analysis	See *Vulnerability Assessment*.
Vulnerability Assessment [CNSSI 4009]	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.
Whitelisting	The process used to identify: (i) software programs that are authorized to execute on an information system; or (ii) authorized Universal Resource Locators (URL)/websites.

APPENDIX C

ACRONYMS

COMMON ABBREVIATIONS

APT	Advanced Persistent Threat
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CAVP	Cryptographic Algorithm Validation Program
CMVP	Cryptographic Module Validation Program
CNSS	Committee on National Security Systems
CPO	Chief Privacy Officer
CUI	Controlled Unclassified Information
DCS	Distributed Control System
DNS	Domain Name System
DoD	Department of Defense
FAR	Federal Acquisition Regulation
FEA	Federal Enterprise Architecture
FICAM	Federal Identity, Credential, and Access Management
FIPP	Fair Information Practice Principles
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
HSPD	Homeland Security Presidential Directive
ICS	Industrial Control System
IEEE	Institute of Electrical and Electronics Engineers
IPsec	Internet Protocol Security
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ITL	Information Technology Laboratory
LACS	Logical Access Control System
LSI	Large-Scale Integration
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency or Internal Report
NSA	National Security Agency

NSTISSI	National Security Telecommunications and Information System Security Instruction
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OPSEC	Operations Security
PBX	Private Branch Exchange
PACS	Physical Access Control System
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RBAC	Role-Based Access Control
RD	Restricted Data
RMF	Risk Management Framework
SAISO	Senior Agency Information Security Officer
SAMI	Sources And Methods Information
SAOP	Senior Agency Official for Privacy
SAP	Special Access Program
SC	Security Category
SCADA	Supervisory Control and Data Acquisition
SCI	Sensitive Compartmented Information
SOA	Service-Oriented Architecture
SORN	System of Records Notice
SP	Special Publication
TCP/IP	Transmission Control Protocol/Internet Protocol
USB	Universal Serial Bus
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

APPENDIX D

SECURITY CONTROL BASELINES – SUMMARY

LOW-IMPACT, MODERATE-IMPACT, AND HIGH-IMPACT INFORMATION SYSTEMS

This appendix contains the security control baselines that represent the *starting point* in determining the security controls for low-impact, moderate-impact, and high-impact information systems.[90] The three security control baselines are hierarchical in nature with regard to the security controls employed in those baselines.[91] If a security control is selected for one of the baselines, the family identifier and control number are listed in the appropriate column. If a security control is not used in a particular baseline, the entry is marked *not selected*. Security control enhancements, when used to supplement security controls, are indicated by the number of the enhancement. For example, an IR-2 (1) in the high baseline entry for the IR-2 security control indicates that the second control from the Incident Response family has been selected along with control enhancement (1). Some security controls and enhancements in the security control catalog are not used in any of the baselines in this appendix but are available for use by organizations if needed. This situation occurs, for example, when the results of a risk assessment indicate the need for additional security controls or control enhancements in order to adequately mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.

Organizations can use the recommended *priority code* designation associated with each security control in the baselines to assist in making sequencing decisions for control implementation (i.e., a Priority Code 1 [P1] control has a higher priority for implementation than a Priority Code 2 [P2] control; a Priority Code 2 [P2] control has a higher priority for implementation than a Priority Code 3 [P3] control, and a Priority Code 0 [P0] indicates the security control is not selected in any baseline). This recommended sequencing prioritization helps ensure that security controls upon which other controls depend are implemented first, thus enabling organizations to deploy controls in a more structured and timely manner in accordance with available resources. The implementation of security controls by sequence priority code does not imply any defined level of risk mitigation until *all* controls in the security plan have been implemented. The priority codes are used only for implementation sequencing, not for making security control selection decisions. Table D-1 summarizes sequence priority codes for the baseline security controls in Table D-2.

TABLE D-1: SECURITY CONTROL PRIORITIZATION CODES

Priority Code	Sequencing	Action
Priority Code 1 (P1)	FIRST	Implement P1 security controls first.
Priority Code 2 (P2)	NEXT	Implement P2 security controls after implementation of P1 controls.
Priority Code 3 (P3)	LAST	Implement P3 security controls after implementation of P1 and P2 controls.
Unspecified Priority Code (P0)	NONE	Security control not selected in any baseline.

[90] A complete description of all security controls is provided in Appendices F and G. In addition, separate documents for individual security control baselines (listed as Annexes 1, 2, and 3) are available at http://csrc.nist.gov/publications. An online version of the catalog of security controls is also available at http://web.nvd.nist.gov/view/800-53/home.

[91] The hierarchical nature applies to the security requirements of each control (i.e., the base control plus all of its enhancements) at the low-impact, moderate-impact, and high-impact level in that the control requirements at a particular impact level (e.g., CP-4 *Contingency Plan Testing*—Moderate: CP-4 (1)) meets a stronger set of security requirements for that control than the next lower impact level of the same control (e.g., CP-4 *Contingency Plan Testing*—Low: CP-4).

Table D-2 provides a summary of the security controls and control enhancements from Appendix F that have been allocated to the initial security control baselines (i.e., low, moderate, and high). The sequence priority codes for security control implementation and those security controls that have been withdrawn from Appendix F are also indicated in Table D-2. In addition to Table D-2, the sequence priority codes and security control baselines are annotated in a priority and baseline allocation summary section below each security control in Appendix F.

TABLE D-2: SECURITY CONTROL BASELINES[92]

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Access Control					
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	Unsuccessful Logon Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P3	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11 (1)	AC-11 (1)
AC-12	Session Termination	P2	Not Selected	AC-12	AC-12
AC-13	**Withdrawn**	---	---	---	---
AC-14	Permitted Actions without Identification or Authentication	P3	AC-14	AC-14	AC-14
AC-15	**Withdrawn**	---	---	---	---
AC-16	Security Attributes	P0	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	P1	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	Wireless Access	P1	AC-18	AC-18 (1)	AC-18 (1) (4) (5)
AC-19	Access Control for Mobile Devices	P1	AC-19	AC-19 (5)	AC-19 (5)
AC-20	Use of External Information Systems	P1	AC-20	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	Information Sharing	P2	Not Selected	AC-21	AC-21
AC-22	Publicly Accessible Content	P3	AC-22	AC-22	AC-22
AC-23	Data Mining Protection	P0	Not Selected	Not Selected	Not Selected
AC-24	Access Control Decisions	P0	Not Selected	Not Selected	Not Selected
AC-25	Reference Monitor	P0	Not Selected	Not Selected	Not Selected

[92] The security control baselines in Table D-2 are the initial baselines selected by organizations prior to conducting the tailoring activities described in Section 3.2. The control baselines and priority codes are only applicable to non-national security systems. Security control baselines for national security systems are included in CNSS Instruction 1253.

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Awareness and Training					
AT-1	Security Awareness and Training Policy and Procedures	P1	AT-1	AT-1	AT-1
AT-2	Security Awareness Training	P1	AT-2	AT-2 (2)	AT-2 (2)
AT-3	Role-Based Security Training	P1	AT-3	AT-3	AT-3
AT-4	Security Training Records	P3	AT-4	AT-4	AT-4
AT-5	**Withdrawn**	---	---	---	---
Audit and Accountability					
AU-1	Audit and Accountability Policy and Procedures	P1	AU-1	AU-1	AU-1
AU-2	Audit Events	P1	AU-2	AU-2 (3)	AU-2 (3)
AU-3	Content of Audit Records	P1	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	P1	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	P1	AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Review, Analysis, and Reporting	P1	AU-6	AU-6 (1) (3)	AU-6 (1) (3) (5) (6)
AU-7	Audit Reduction and Report Generation	P2	Not Selected	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	P1	AU-8	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	P1	AU-9	AU-9 (4)	AU-9 (2) (3) (4)
AU-10	Non-repudiation	P2	Not Selected	Not Selected	AU-10
AU-11	Audit Record Retention	P3	AU-11	AU-11	AU-11
AU-12	Audit Generation	P1	AU-12	AU-12	AU-12 (1) (3)
AU-13	Monitoring for Information Disclosure	P0	Not Selected	Not Selected	Not Selected
AU-14	Session Audit	P0	Not Selected	Not Selected	Not Selected
AU-15	Alternate Audit Capability	P0	Not Selected	Not Selected	Not Selected
AU-16	Cross-Organizational Auditing	P0	Not Selected	Not Selected	Not Selected
Security Assessment and Authorization					
CA-1	Security Assessment and Authorization Policies and Procedures	P1	CA-1	CA-1	CA-1
CA-2	Security Assessments	P2	CA-2	CA-2 (1)	CA-2 (1) (2)
CA-3	System Interconnections	P1	CA-3	CA-3 (5)	CA-3 (5)
CA-4	**Withdrawn**	---	---	---	---
CA-5	Plan of Action and Milestones	P3	CA-5	CA-5	CA-5
CA-6	Security Authorization	P2	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	P2	CA-7	CA-7 (1)	CA-7 (1)
CA-8	Penetration Testing	P2	Not Selected	Not Selected	CA-8
CA-9	Internal System Connections	P2	CA-9	CA-9	CA-9
Configuration Management					
CM-1	Configuration Management Policy and Procedures	P1	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	P1	CM-2	CM-2 (1) (3) (7)	CM-2 (1) (2) (3) (7)
CM-3	Configuration Change Control	P1	Not Selected	CM-3 (2)	CM-3 (1) (2)
CM-4	Security Impact Analysis	P2	CM-4	CM-4	CM-4 (1)
CM-5	Access Restrictions for Change	P1	Not Selected	CM-5	CM-5 (1) (2) (3)

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
CM-6	Configuration Settings	P1	CM-6	CM-6	CM-6 (1) (2)
CM-7	Least Functionality	P1	CM-7	CM-7 (1) (2) (4)	CM-7 (1) (2) (5)
CM-8	Information System Component Inventory	P1	CM-8	CM-8 (1) (3) (5)	CM-8 (1) (2) (3) (4) (5)
CM-9	Configuration Management Plan	P1	Not Selected	CM-9	CM-9
CM-10	Software Usage Restrictions	P2	CM-10	CM-10	CM-10
CM-11	User-Installed Software	P1	CM-11	CM-11	CM-11
Contingency Planning					
CP-1	Contingency Planning Policy and Procedures	P1	CP-1	CP-1	CP-1
CP-2	Contingency Plan	P1	CP-2	CP-2 (1) (3) (8)	CP-2 (1) (2) (3) (4) (5) (8)
CP-3	Contingency Training	P2	CP-3	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing	P2	CP-4	CP-4 (1)	CP-4 (1) (2)
CP-5	**Withdrawn**	---	---	---	---
CP-6	Alternate Storage Site	P1	Not Selected	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Site	P1	Not Selected	CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)
CP-8	Telecommunications Services	P1	Not Selected	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	Information System Backup	P1	CP-9	CP-9 (1)	CP-9 (1) (2) (3) (5)
CP-10	Information System Recovery and Reconstitution	P1	CP-10	CP-10 (2)	CP-10 (2) (4)
CP-11	Alternate Communications Protocols	P0	Not Selected	Not Selected	Not Selected
CP-12	Safe Mode	P0	Not Selected	Not Selected	Not Selected
CP-13	Alternative Security Mechanisms	P0	Not Selected	Not Selected	Not Selected
Identification and Authentication					
IA-1	Identification and Authentication Policy and Procedures	P1	IA-1	IA-1	IA-1
IA-2	Identification and Authentication (Organizational Users)	P1	IA-2 (1) (12)	IA-2 (1) (2) (3) (8) (11) (12)	IA-2 (1) (2) (3) (4) (8) (9) (11) (12)
IA-3	Device Identification and Authentication	P1	Not Selected	IA-3	IA-3
IA-4	Identifier Management	P1	IA-4	IA-4	IA-4
IA-5	Authenticator Management	P1	IA-5 (1) (11)	IA-5 (1) (2) (3) (11)	IA-5 (1) (2) (3) (11)
IA-6	Authenticator Feedback	P2	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	P1	IA-7	IA-7	IA-7
IA-8	Identification and Authentication (Non-Organizational Users)	P1	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)
IA-9	Service Identification and Authentication	P0	Not Selected	Not Selected	Not Selected
IA-10	Adaptive Identification and Authentication	P0	Not Selected	Not Selected	Not Selected
IA-11	Re-authentication	P0	Not Selected	Not Selected	Not Selected
Incident Response					
IR-1	Incident Response Policy and Procedures	P1	IR-1	IR-1	IR-1
IR-2	Incident Response Training	P2	IR-2	IR-2	IR-2 (1) (2)

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
IR-3	Incident Response Testing	P2	Not Selected	IR-3 (2)	IR-3 (2)
IR-4	Incident Handling	P1	IR-4	IR-4 (1)	IR-4 (1) (4)
IR-5	Incident Monitoring	P1	IR-5	IR-5	IR-5 (1)
IR-6	Incident Reporting	P1	IR-6	IR-6 (1)	IR-6 (1)
IR-7	Incident Response Assistance	P2	IR-7	IR-7 (1)	IR-7 (1)
IR-8	Incident Response Plan	P1	IR-8	IR-8	IR-8
IR-9	Information Spillage Response	P0	Not Selected	Not Selected	Not Selected
IR-10	Integrated Information Security Analysis Team	P0	Not Selected	Not Selected	Not Selected
Maintenance					
MA-1	System Maintenance Policy and Procedures	P1	MA-1	MA-1	MA-1
MA-2	Controlled Maintenance	P2	MA-2	MA-2	MA-2 (2)
MA-3	Maintenance Tools	P3	Not Selected	MA-3 (1) (2)	MA-3 (1) (2) (3)
MA-4	Nonlocal Maintenance	P2	MA-4	MA-4 (2)	MA-4 (2) (3)
MA-5	Maintenance Personnel	P2	MA-5	MA-5	MA-5 (1)
MA-6	Timely Maintenance	P2	Not Selected	MA-6	MA-6
Media Protection					
MP-1	Media Protection Policy and Procedures	P1	MP-1	MP-1	MP-1
MP-2	Media Access	P1	MP-2	MP-2	MP-2
MP-3	Media Marking	P2	Not Selected	MP-3	MP-3
MP-4	Media Storage	P1	Not Selected	MP-4	MP-4
MP-5	Media Transport	P1	Not Selected	MP-5 (4)	MP-5 (4)
MP-6	Media Sanitization	P1	MP-6	MP-6	MP-6 (1) (2) (3)
MP-7	Media Use	P1	MP-7	MP-7 (1)	MP-7 (1)
MP-8	Media Downgrading	P0	Not Selected	Not Selected	Not Selected
Physical and Environmental Protection					
PE-1	Physical and Environmental Protection Policy and Procedures	P1	PE-1	PE-1	PE-1
PE-2	Physical Access Authorizations	P1	PE-2	PE-2	PE-2
PE-3	Physical Access Control	P1	PE-3	PE-3	PE-3 (1)
PE-4	Access Control for Transmission Medium	P1	Not Selected	PE-4	PE-4
PE-5	Access Control for Output Devices	P2	Not Selected	PE-5	PE-5
PE-6	Monitoring Physical Access	P1	PE-6	PE-6 (1)	PE-6 (1) (4)
PE-7	**Withdrawn**	---	---	---	---
PE-8	Visitor Access Records	P3	PE-8	PE-8	PE-8 (1)
PE-9	Power Equipment and Cabling	P1	Not Selected	PE-9	PE-9
PE-10	Emergency Shutoff	P1	Not Selected	PE-10	PE-10
PE-11	Emergency Power	P1	Not Selected	PE-11	PE-11 (1)
PE-12	Emergency Lighting	P1	PE-12	PE-12	PE-12
PE-13	Fire Protection	P1	PE-13	PE-13 (3)	PE-13 (1) (2) (3)
PE-14	Temperature and Humidity Controls	P1	PE-14	PE-14	PE-14
PE-15	Water Damage Protection	P1	PE-15	PE-15	PE-15 (1)
PE-16	Delivery and Removal	P2	PE-16	PE-16	PE-16

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
PE-17	Alternate Work Site	P2	Not Selected	PE-17	PE-17
PE-18	Location of Information System Components	P3	Not Selected	Not Selected	PE-18
PE-19	Information Leakage	P0	Not Selected	Not Selected	Not Selected
PE-20	Asset Monitoring and Tracking	P0	Not Selected	Not Selected	Not Selected
Planning					
PL-1	Security Planning Policy and Procedures	P1	PL-1	PL-1	PL-1
PL-2	System Security Plan	P1	PL-2	PL-2 (3)	PL-2 (3)
PL-3	**Withdrawn**	---	---	---	---
PL-4	Rules of Behavior	P2	PL-4	PL-4 (1)	PL-4 (1)
PL-5	**Withdrawn**	---	---	---	---
PL-6	**Withdrawn**	---	---	---	---
PL-7	Security Concept of Operations	P0	Not Selected	Not Selected	Not Selected
PL-8	Information Security Architecture	P1	Not Selected	PL-8	PL-8
PL-9	Central Management	P0	Not Selected	Not Selected	Not Selected
Personnel Security					
PS-1	Personnel Security Policy and Procedures	P1	PS-1	PS-1	PS-1
PS-2	Position Risk Designation	P1	PS-2	PS-2	PS-2
PS-3	Personnel Screening	P1	PS-3	PS-3	PS-3
PS-4	Personnel Termination	P1	PS-4	PS-4	PS-4 (2)
PS-5	Personnel Transfer	P2	PS-5	PS-5	PS-5
PS-6	Access Agreements	P3	PS-6	PS-6	PS-6
PS-7	Third-Party Personnel Security	P1	PS-7	PS-7	PS-7
PS-8	Personnel Sanctions	P3	PS-8	PS-8	PS-8
Risk Assessment					
RA-1	Risk Assessment Policy and Procedures	P1	RA-1	RA-1	RA-1
RA-2	Security Categorization	P1	RA-2	RA-2	RA-2
RA-3	Risk Assessment	P1	RA-3	RA-3	RA-3
RA-4	**Withdrawn**	---	---	---	---
RA-5	Vulnerability Scanning	P1	RA-5	RA-5 (1) (2) (5)	RA-5 (1) (2) (4) (5)
RA-6	Technical Surveillance Countermeasures Survey	P0	Not Selected	Not Selected	Not Selected
System and Services Acquisition					
SA-1	System and Services Acquisition Policy and Procedures	P1	SA-1	SA-1	SA-1
SA-2	Allocation of Resources	P1	SA-2	SA-2	SA-2
SA-3	System Development Life Cycle	P1	SA-3	SA-3	SA-3
SA-4	Acquisition Process	P1	SA-4 (10)	SA-4 (1) (2) (9) (10)	SA-4 (1) (2) (9) (10)
SA-5	Information System Documentation	P2	SA-5	SA-5	SA-5
SA-6	**Withdrawn**	---	---	---	---
SA-7	**Withdrawn**	---	---	---	---
SA-8	Security Engineering Principles	P1	Not Selected	SA-8	SA-8
SA-9	External Information System Services	P1	SA-9	SA-9 (2)	SA-9 (2)

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
SA-10	Developer Configuration Management	P1	Not Selected	SA-10	SA-10
SA-11	Developer Security Testing and Evaluation	P1	Not Selected	SA-11	SA-11
SA-12	Supply Chain Protection	P1	Not Selected	Not Selected	SA-12
SA-13	Trustworthiness	P0	Not Selected	Not Selected	Not Selected
SA-14	Criticality Analysis	P0	Not Selected	Not Selected	Not Selected
SA-15	Development Process, Standards, and Tools	P2	Not Selected	Not Selected	SA-15
SA-16	Developer-Provided Training	P2	Not Selected	Not Selected	SA-16
SA-17	Developer Security Architecture and Design	P1	Not Selected	Not Selected	SA-17
SA-18	Tamper Resistance and Detection	P0	Not Selected	Not Selected	Not Selected
SA-19	Component Authenticity	P0	Not Selected	Not Selected	Not Selected
SA-20	Customized Development of Critical Components	P0	Not Selected	Not Selected	Not Selected
SA-21	Developer Screening	P0	Not Selected	Not Selected	Not Selected
SA-22	Unsupported System Components	P0	Not Selected	Not Selected	Not Selected
System and Communications Protection					
SC-1	System and Communications Protection Policy and Procedures	P1	SC-1	SC-1	SC-1
SC-2	Application Partitioning	P1	Not Selected	SC-2	SC-2
SC-3	Security Function Isolation	P1	Not Selected	Not Selected	SC-3
SC-4	Information in Shared Resources	P1	Not Selected	SC-4	SC-4
SC-5	Denial of Service Protection	P1	SC-5	SC-5	SC-5
SC-6	Resource Availability	P0	Not Selected	Not Selected	Not Selected
SC-7	Boundary Protection	P1	SC-7	SC-7 (3) (4) (5) (7)	SC-7 (3) (4) (5) (7) (8) (18) (21)
SC-8	Transmission Confidentiality and Integrity	P1	Not Selected	SC-8 (1)	SC-8 (1)
SC-9	**Withdrawn**	---	---	---	---
SC-10	Network Disconnect	P2	Not Selected	SC-10	SC-10
SC-11	Trusted Path	P0	Not Selected	Not Selected	Not Selected
SC-12	Cryptographic Key Establishment and Management	P1	SC-12	SC-12	SC-12 (1)
SC-13	Cryptographic Protection	P1	SC-13	SC-13	SC-13
SC-14	**Withdrawn**	---	---	---	---
SC-15	Collaborative Computing Devices	P1	SC-15	SC-15	SC-15
SC-16	Transmission of Security Attributes	P0	Not Selected	Not Selected	Not Selected
SC-17	Public Key Infrastructure Certificates	P1	Not Selected	SC-17	SC-17
SC-18	Mobile Code	P2	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	P1	Not Selected	SC-19	SC-19
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	P1	SC-20	SC-20	SC-20
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	P1	SC-21	SC-21	SC-21
SC-22	Architecture and Provisioning for Name/Address Resolution Service	P1	SC-22	SC-22	SC-22
SC-23	Session Authenticity	P1	Not Selected	SC-23	SC-23
SC-24	Fail in Known State	P1	Not Selected	Not Selected	SC-24

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
SC-25	Thin Nodes	P0	Not Selected	Not Selected	Not Selected
SC-26	Honeypots	P0	Not Selected	Not Selected	Not Selected
SC-27	Platform-Independent Applications	P0	Not Selected	Not Selected	Not Selected
SC-28	Protection of Information at Rest	P1	Not Selected	SC-28	SC-28
SC-29	Heterogeneity	P0	Not Selected	Not Selected	Not Selected
SC-30	Concealment and Misdirection	P0	Not Selected	Not Selected	Not Selected
SC-31	Covert Channel Analysis	P0	Not Selected	Not Selected	Not Selected
SC-32	Information System Partitioning	P0	Not Selected	Not Selected	Not Selected
SC-33	**Withdrawn**	---	---	---	---
SC-34	Non-Modifiable Executable Programs	P0	Not Selected	Not Selected	Not Selected
SC-35	Honeyclients	P0	Not Selected	Not Selected	Not Selected
SC-36	Distributed Processing and Storage	P0	Not Selected	Not Selected	Not Selected
SC-37	Out-of-Band Channels	P0	Not Selected	Not Selected	Not Selected
SC-38	Operations Security	P0	Not Selected	Not Selected	Not Selected
SC-39	Process Isolation	P1	SC-39	SC-39	SC-39
SC-40	Wireless Link Protection	P0	Not Selected	Not Selected	Not Selected
SC-41	Port and I/O Device Access	P0	Not Selected	Not Selected	Not Selected
SC-42	Sensor Capability and Data	P0	Not Selected	Not Selected	Not Selected
SC-43	Usage Restrictions	P0	Not Selected	Not Selected	Not Selected
SC-44	Detonation Chambers	P0	Not Selected	Not Selected	Not Selected
System and Information Integrity					
SI-1	System and Information Integrity Policy and Procedures	P1	SI-1	SI-1	SI-1
SI-2	Flaw Remediation	P1	SI-2	SI-2 (2)	SI-2 (1) (2)
SI-3	Malicious Code Protection	P1	SI-3	SI-3 (1) (2)	SI-3 (1) (2)
SI-4	Information System Monitoring	P1	SI-4	SI-4 (2) (4) (5)	SI-4 (2) (4) (5)
SI-5	Security Alerts, Advisories, and Directives	P1	SI-5	SI-5	SI-5 (1)
SI-6	Security Function Verification	P1	Not Selected	Not Selected	SI-6
SI-7	Software, Firmware, and Information Integrity	P1	Not Selected	SI-7 (1) (7)	SI-7 (1) (2) (5) (7) (14)
SI-8	Spam Protection	P2	Not Selected	SI-8 (1) (2)	SI-8 (1) (2)
SI-9	**Withdrawn**	---	---	---	---
SI-10	Information Input Validation	P1	Not Selected	SI-10	SI-10
SI-11	Error Handling	P2	Not Selected	SI-11	SI-11
SI-12	Information Handling and Retention	P2	SI-12	SI-12	SI-12
SI-13	Predictable Failure Prevention	P0	Not Selected	Not Selected	Not Selected
SI-14	Non-Persistence	P0	Not Selected	Not Selected	Not Selected
SI-15	Information Output Filtering	P0	Not Selected	Not Selected	Not Selected
SI-16	Memory Protection	P1	Not Selected	SI-16	SI-16
SI-17	Fail-Safe Procedures	P0	Not Selected	Not Selected	Not Selected

Tables D-3 through D-19 provide a more detailed summary of the security controls and control enhancements in Appendix F. Each table focuses on a different security control family. Whereas Table D-2 includes only those security controls and control enhancements allocated to the three security control baselines, Tables D-3 through D-19 include all controls and enhancements for the respective security control families. The tables include the following information: (i) the security controls and control enhancements that have been selected for the security control baselines as indicated by an "x" in the column for the selected baseline;[93] (ii) the security controls and control enhancements that have not been selected for any security control baseline (i.e., the controls and control enhancements available for selection to achieve greater protection) as indicated by blank cells in the baseline columns; (iii) the security controls and control enhancements that have been withdrawn from Appendix F as indicated by an "x" in the respective withdrawn column; and (iv) the security controls and control enhancements that have assurance-related characteristics or properties (i.e., assurance-related controls) as indicated by an "x" in the respective assurance column. Assurance-related controls are discussed in greater detail in Appendix E to include the allocation of such controls to security control baselines (see Tables E-1 through E-3).

[93] The security control baselines in Tables D-3 through D-19 are only applicable to non-national security systems. Security control baselines for national security systems are included in CNSS Instruction 1253.

TABLE D-3: SUMMARY — ACCESS CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AC-1	**Access Control Policy and Procedures**		x	x	x	x
AC-2	**Account Management**			x	x	x
AC-2 (1)	*ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT*				x	x
AC-2 (2)	*ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS*				x	x
AC-2 (3)	*ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS*				x	x
AC-2 (4)	*ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS*				x	x
AC-2 (5)	*ACCOUNT MANAGEMENT | INACTIVITY LOGOUT*					x
AC-2 (6)	*ACCOUNT MANAGEMENT | DYNAMIC PRIVILEGE MANAGEMENT*					
AC-2 (7)	*ACCOUNT MANAGEMENT | ROLE-BASED SCHEMES*					
AC-2 (8)	*ACCOUNT MANAGEMENT | DYNAMIC ACCOUNT CREATION*					
AC-2 (9)	*ACCOUNT MANAGEMENT | RESTRICTIONS ON USE OF SHARED GROUPS / ACCOUNTS*					
AC-2 (10)	*ACCOUNT MANAGEMENT | SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION*					
AC-2 (11)	*ACCOUNT MANAGEMENT | USAGE CONDITIONS*					x
AC-2 (12)	*ACCOUNT MANAGEMENT | ACCOUNT MONITORING / ATYPICAL USAGE*					x
AC-2 (13)	*ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS*					x
AC-3	**Access Enforcement**			x	x	x
AC-3 (1)	*ACCESS ENFORCEMENT | RESTRICTED ACCESS TO PRIVILEGED FUNCTIONS*	x	Incorporated into AC-6.			
AC-3 (2)	*ACCESS ENFORCEMENT | DUAL AUTHORIZATION*					
AC-3 (3)	*ACCESS ENFORCEMENT | MANDATORY ACCESS CONTROL*					
AC-3 (4)	*ACCESS ENFORCEMENT | DISCRETIONARY ACCESS CONTROL*					
AC-3 (5)	*ACCESS ENFORCEMENT | SECURITY-RELEVANT INFORMATION*					
AC-3 (6)	*ACCESS ENFORCEMENT | PROTECTION OF USER AND SYSTEM INFORMATION*	x	Incorporated into MP-4 and SC-28.			
AC-3 (7)	*ACCESS ENFORCEMENT | ROLE-BASED ACCESS CONTROL*					
AC-3 (8)	*ACCESS ENFORCEMENT | REVOCATION OF ACCESS AUTHORIZATIONS*					
AC-3 (9)	*ACCESS ENFORCEMENT | CONTROLLED RELEASE*					
AC-3 (10)	*ACCESS ENFORCEMENT | AUDITED OVERRIDE OF ACCESS CONTROL MECHANISMS*					
AC-4	**Information Flow Enforcement**				x	x
AC-4 (1)	*INFORMATION FLOW ENFORCEMENT | OBJECT SECURITY ATTRIBUTES*					
AC-4 (2)	*INFORMATION FLOW ENFORCEMENT | PROCESSING DOMAINS*					
AC-4 (3)	*INFORMATION FLOW ENFORCEMENT | DYNAMIC INFORMATION FLOW CONTROL*					
AC-4 (4)	*INFORMATION FLOW ENFORCEMENT | CONTENT CHECK ENCRYPTED INFORMATION*					
AC-4 (5)	*INFORMATION FLOW ENFORCEMENT | EMBEDDED DATA TYPES*					
AC-4 (6)	*INFORMATION FLOW ENFORCEMENT | METADATA*					
AC-4 (7)	*INFORMATION FLOW ENFORCEMENT | ONE-WAY FLOW MECHANISMS*					
AC-4 (8)	*INFORMATION FLOW ENFORCEMENT | SECURITY POLICY FILTERS*					
AC-4 (9)	*INFORMATION FLOW ENFORCEMENT | HUMAN REVIEWS*					
AC-4 (10)	*INFORMATION FLOW ENFORCEMENT | ENABLE / DISABLE SECURITY POLICY FILTERS*					

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AC-4 (11)	*INFORMATION FLOW ENFORCEMENT | CONFIGURATION OF SECURITY POLICY FILTERS*					
AC-4 (12)	*INFORMATION FLOW ENFORCEMENT | DATA TYPE IDENTIFIERS*					
AC-4 (13)	*INFORMATION FLOW ENFORCEMENT | DECOMPOSITION INTO POLICY-RELEVANT SUBCOMPONENTS*					
AC-4 (14)	*INFORMATION FLOW ENFORCEMENT | SECURITY POLICY FILTER CONSTRAINTS*					
AC-4 (15)	*INFORMATION FLOW ENFORCEMENT | DETECTION OF UNSANCTIONED INFORMATION*					
AC-4 (16)	*INFORMATION FLOW ENFORCEMENT | INFORMATION TRANSFERS ON INTERCONNECTED SYSTEMS*	x	Incorporated into AC-4.			
AC-4 (17)	*INFORMATION FLOW ENFORCEMENT | DOMAIN AUTHENTICATION*					
AC-4 (18)	*INFORMATION FLOW ENFORCEMENT | SECURITY ATTRIBUTE BINDING*					
AC-4 (19)	*INFORMATION FLOW ENFORCEMENT | VALIDATION OF METADATA*					
AC-4 (20)	*INFORMATION FLOW ENFORCEMENT | APPROVED SOLUTIONS*					
AC-4 (21)	*INFORMATION FLOW ENFORCEMENT | PHYSICAL / LOGICAL SEPARATION OF INFORMATION FLOWS*					
AC-4 (22)	*INFORMATION FLOW ENFORCEMENT | ACCESS ONLY*					
AC-5	**Separation of Duties**				x	x
AC-6	**Least Privilege**				x	x
AC-6 (1)	*LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS*				x	x
AC-6 (2)	*LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS*				x	x
AC-6 (3)	*LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS*					x
AC-6 (4)	*LEAST PRIVILEGE | SEPARATE PROCESSING DOMAINS*					
AC-6 (5)	*LEAST PRIVILEGE | PRIVILEGED ACCOUNTS*				x	x
AC-6 (6)	*LEAST PRIVILEGE | PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS*					
AC-6 (7)	*LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES*					
AC-6 (8)	*LEAST PRIVILEGE | PRIVILEGE LEVELS FOR CODE EXECUTION*					
AC-6 (9)	*LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS*				x	x
AC-6 (10)	*LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS*				x	x
AC-7	**Unsuccessful Logon Attempts**			x	x	x
AC-7 (1)	*UNSUCCESSFUL LOGON ATTEMPTS | AUTOMATIC ACCOUNT LOCK*	x	Incorporated into AC-7.			
AC-7 (2)	*UNSUCCESSFUL LOGON ATTEMPTS | PURGE / WIPE MOBILE DEVICE*					
AC-8	**System Use Notification**			x	x	x
AC-9	**Previous Logon (Access) Notification**					
AC-9 (1)	*PREVIOUS LOGON NOTIFICATION | UNSUCCESSFUL LOGONS*					
AC-9 (2)	*PREVIOUS LOGON NOTIFICATION | SUCCESSFUL / UNSUCCESSFUL LOGONS*					
AC-9 (3)	*PREVIOUS LOGON NOTIFICATION | NOTIFICATION OF ACCOUNT CHANGES*					
AC-9 (4)	*PREVIOUS LOGON NOTIFICATION | ADDITIONAL LOGON INFORMATION*					
AC-10	**Concurrent Session Control**					x
AC-11	**Session Lock**				x	x
AC-11 (1)	*SESSION LOCK | PATTERN-HIDING DISPLAYS*				x	x
AC-12	**Session Termination**				x	x

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AC-12 (1)	*SESSION TERMINATION | USER-INITIATED LOGOUTS / MESSAGE DISPLAYS*					
AC-13	**Supervision and Review — Access Control**	X	Incorporated into AC-2 and AU-6.			
AC-14	**Permitted Actions without Identification or Authentication**			X	X	X
AC-14 (1)	*PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION | NECESSARY USES*	X	Incorporated into AC-14.			
AC-15	**Automated Marking**	X	Incorporated into MP-3.			
AC-16	**Security Attributes**					
AC-16 (1)	*SECURITY ATTRIBUTES | DYNAMIC ATTRIBUTE ASSOCIATION*					
AC-16 (2)	*SECURITY ATTRIBUTES | ATTRIBUTE VALUE CHANGES BY AUTHORIZED INDIVIDUALS*					
AC-16 (3)	*SECURITY ATTRIBUTES | MAINTENANCE OF ATTRIBUTE ASSOCIATIONS BY INFORMATION SYSTEM*					
AC-16 (4)	*SECURITY ATTRIBUTES | ASSOCIATION OF ATTRIBUTES BY AUTHORIZED INDIVIDUALS*					
AC-16 (5)	*SECURITY ATTRIBUTES | ATTRIBUTE DISPLAYS FOR OUTPUT DEVICES*					
AC-16 (6)	*SECURITY ATTRIBUTES | MAINTENANCE OF ATTRIBUTE ASSOCIATION BY ORGANIZATION*					
AC-16 (7)	*SECURITY ATTRIBUTES | CONSISTENT ATTRIBUTE INTERPRETATION*					
AC-16 (8)	*SECURITY ATTRIBUTES | ASSOCIATION TECHNIQUES / TECHNOLOGIES*					
AC-16 (9)	*SECURITY ATTRIBUTES | ATTRIBUTE REASSIGNMENT*					
AC-16 (10)	*SECURITY ATTRIBUTES | ATTRIBUTE CONFIGURATION BY AUTHORIZED INDIVIDUALS*					
AC-17	**Remote Access**			X	X	X
AC-17 (1)	*REMOTE ACCESS | AUTOMATED MONITORING / CONTROL*				X	X
AC-17 (2)	*REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION*				X	X
AC-17 (3)	*REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS*				X	X
AC-17 (4)	*REMOTE ACCESS | PRIVILEGED COMMANDS / ACCESS*				X	X
AC-17 (5)	*REMOTE ACCESS | MONITORING FOR UNAUTHORIZED CONNECTIONS*	X	Incorporated into SI-4.			
AC-17 (6)	*REMOTE ACCESS | PROTECTION OF INFORMATION*					
AC-17 (7)	*REMOTE ACCESS | ADDITIONAL PROTECTION FOR SECURITY FUNCTION ACCESS*	X	Incorporated into AC-3 (10).			
AC-17 (8)	*REMOTE ACCESS | DISABLE NONSECURE NETWORK PROTOCOLS*	X	Incorporated into CM-7.			
AC-17 (9)	*REMOTE ACCESS | DISCONNECT / DISABLE ACCESS*					
AC-18	**Wireless Access**			X	X	X
AC-18 (1)	*WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION*				X	X
AC-18 (2)	*WIRELESS ACCESS | MONITORING UNAUTHORIZED CONNECTIONS*	X	Incorporated into SI-4.			
AC-18 (3)	*WIRELESS ACCESS | DISABLE WIRELESS NETWORKING*					
AC-18 (4)	*WIRELESS ACCESS | RESTRICT CONFIGURATIONS BY USERS*					X
AC-18 (5)	*WIRELESS ACCESS | ANTENNAS / TRANSMISSION POWER LEVELS*					X
AC-19	**Access Control for Mobile Devices**			X	X	X
AC-19 (1)	*ACCESS CONTROL FOR MOBILE DEVICES | USE OF WRITABLE / PORTABLE STORAGE DEVICES*	X	Incorporated into MP-7.			
AC-19 (2)	*ACCESS CONTROL FOR MOBILE DEVICES | USE OF PERSONALLY OWNED PORTABLE STORAGE DEVICES*	X	Incorporated into MP-7.			
AC-19 (3)	*ACCESS CONTROL FOR MOBILE DEVICES | USE OF PORTABLE STORAGE DEVICES WITH NO IDENTIFIABLE OWNER*	X	Incorporated into MP-7.			

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AC-19 (4)	*ACCESS CONTROL FOR MOBILE DEVICES | RESTRICTIONS FOR CLASSIFIED INFORMATION*					
AC-19 (5)	*ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE / CONTAINER-BASED ENCRYPTION*				X	X
AC-20	**Use of External Information Systems**			X	X	X
AC-20 (1)	*USE OF EXTERNAL INFORMATION SYSTEMS | LIMITS ON AUTHORIZED USE*				X	X
AC-20 (2)	*USE OF EXTERNAL INFORMATION SYSTEMS | PORTABLE STORAGE DEVICES*				X	X
AC-20 (3)	*USE OF EXTERNAL INFORMATION SYSTEMS | NON-ORGANIZATIONALLY OWNED SYSTEMS / COMPONENTS / DEVICES*					
AC-20 (4)	*USE OF EXTERNAL INFORMATION SYSTEMS | NETWORK ACCESSIBLE STORAGE DEVICES*					
AC-21	**Information Sharing**				X	X
AC-21 (1)	*INFORMATION SHARING | AUTOMATED DECISION SUPPORT*					
AC-21 (2)	*INFORMATION SHARING | INFORMATION SEARCH AND RETRIEVAL*					
AC-22	**Publicly Accessible Content**			X	X	X
AC-23	**Data Mining Protection**					
AC-24	**Access Control Decisions**					
AC-24 (1)	*ACCESS CONTROL DECISIONS | TRANSMIT ACCESS AUTHORIZATION INFORMATION*					
AC-24 (2)	*ACCESS CONTROL DECISIONS | NO USER OR PROCESS IDENTITY*					
AC-25	**Reference Monitor**		X			

TABLE D-4: SUMMARY — AWARENESS AND TRAINING CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AT-1	**Security Awareness and Training Policy and Procedures**		x	x	x	x
AT-2	**Security Awareness Training**		x	x	x	x
AT-2 (1)	*SECURITY AWARENESS | PRACTICAL EXERCISES*		x			
AT-2 (2)	*SECURITY AWARENESS | INSIDER THREAT*		x		x	x
AT-3	**Role-Based Security Training**		x	x	x	x
AT-3 (1)	*SECURITY TRAINING | ENVIRONMENTAL CONTROLS*		x			
AT-3 (2)	*SECURITY TRAINING | PHYSICAL SECURITY CONTROLS*		x			
AT-3 (3)	*SECURITY TRAINING | PRACTICAL EXERCISES*		x			
AT-3 (4)	*SECURITY TRAINING | SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR*		x			
AT-4	**Security Training Records**		x	x	x	x
AT-5	**Contacts with Security Groups and Associations**	x	Incorporated into PM-15.			

TABLE D-5: SUMMARY — AUDIT AND ACCOUNTABILITY CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AU-1	**Audit and Accountability Policy and Procedures**		x	x	x	x
AU-2	**Audit Events**			x	x	x
AU-2 (1)	*AUDIT EVENTS | COMPILATION OF AUDIT RECORDS FROM MULTIPLE SOURCES*	x	Incorporated into AU-12.			
AU-2 (2)	*AUDIT EVENTS | SELECTION OF AUDIT EVENTS BY COMPONENT*	x	Incorporated into AU-12.			
AU-2 (3)	*AUDIT EVENTS | REVIEWS AND UPDATES*				x	x
AU-2 (4)	*AUDIT EVENTS | PRIVILEGED FUNCTIONS*	x	Incorporated into AC-6 (9).			
AU-3	**Content of Audit Records**			x	x	x
AU-3 (1)	*CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION*				x	x
AU-3 (2)	*CONTENT OF AUDIT RECORDS | CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT*					x
AU-4	**Audit Storage Capacity**			x	x	x
AU-4 (1)	*AUDIT STORAGE CAPACITY | TRANSFER TO ALTERNATE STORAGE*					
AU-5	**Response to Audit Processing Failures**			x	x	x
AU-5 (1)	*RESPONSE TO AUDIT PROCESSING FAILURES | AUDIT STORAGE CAPACITY*					x
AU-5 (2)	*RESPONSE TO AUDIT PROCESSING FAILURES | REAL-TIME ALERTS*					x
AU-5 (3)	*RESPONSE TO AUDIT PROCESSING FAILURES | CONFIGURABLE TRAFFIC VOLUME THRESHOLDS*					
AU-5 (4)	*RESPONSE TO AUDIT PROCESSING FAILURES | SHUTDOWN ON FAILURE*					
AU-6	**Audit Review, Analysis, and Reporting**		x	x	x	x
AU-6 (1)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | PROCESS INTEGRATION*		x		x	x
AU-6 (2)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | AUTOMATED SECURITY ALERTS*	x	Incorporated into SI-4.			
AU-6 (3)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT REPOSITORIES*		x		x	x
AU-6 (4)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | CENTRAL REVIEW AND ANALYSIS*		x			
AU-6 (5)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | INTEGRATION / SCANNING AND MONITORING CAPABILITIES*		x			x
AU-6 (6)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH PHYSICAL MONITORING*		x			x
AU-6 (7)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | PERMITTED ACTIONS*		x			
AU-6 (8)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS*		x			
AU-6 (9)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH INFORMATION FROM NONTECHNICAL SOURCES*		x			
AU-6 (10)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | AUDIT LEVEL ADJUSTMENT*		x			
AU-7	**Audit Reduction and Report Generation**		x		x	x
AU-7 (1)	*AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING*		x		x	x
AU-7 (2)	*AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC SORT AND SEARCH*					
AU-8	**Time Stamps**			x	x	x
AU-8 (1)	*TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE*				x	x
AU-8 (2)	*TIME STAMPS | SECONDARY AUTHORITATIVE TIME SOURCE*					

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AU-9	**Protection of Audit Information**			x	x	x
AU-9 (1)	*PROTECTION OF AUDIT INFORMATION | HARDWARE WRITE-ONCE* MEDIA					
AU-9 (2)	*PROTECTION OF AUDIT INFORMATION | AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS*					x
AU-9 (3)	*PROTECTION OF AUDIT INFORMATION | CRYPTOGRAPHIC PROTECTION*					x
AU-9 (4)	*PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS*				x	x
AU-9 (5)	*PROTECTION OF AUDIT INFORMATION | DUAL AUTHORIZATION*					
AU-9 (6)	*PROTECTION OF AUDIT INFORMATION | READ-ONLY ACCESS*					
AU-10	**Non-repudiation**		x			x
AU-10 (1)	*NON-REPUDIATION | ASSOCIATION OF IDENTITIES*		x			
AU-10 (2)	*NON-REPUDIATION | VALIDATE BINDING OF INFORMATION PRODUCER IDENTITY*		x			
AU-10 (3)	*NON-REPUDIATION | CHAIN OF CUSTODY*		x			
AU-10 (4)	*NON-REPUDIATION | VALIDATE BINDING OF INFORMATION REVIEWER IDENTITY*		x			
AU-10 (5)	*NON-REPUDIATION | DIGITAL SIGNATURES*	x	Incorporated into SI-7.			
AU-11	**Audit Record Retention**			x	x	x
AU-11 (1)	*AUDIT RECORD RETENTION | LONG-TERM RETRIEVAL CAPABILITY*		x			
AU-12	**Audit Generation**			x	x	x
AU-12 (1)	*AUDIT GENERATION | SYSTEM-WIDE / TIME-CORRELATED AUDIT TRAIL*					x
AU-12 (2)	*AUDIT GENERATION | STANDARDIZED FORMATS*					
AU-12 (3)	*AUDIT GENERATION | CHANGES BY AUTHORIZED INDIVIDUALS*					x
AU-13	**Monitoring for Information Disclosure**		x			
AU-13 (1)	*MONITORING FOR INFORMATION DISCLOSURE | USE OF AUTOMATED TOOLS*		x			
AU-13 (2)	*MONITORING FOR INFORMATION DISCLOSURE | REVIEW OF MONITORED SITES*		x			
AU-14	**Session Audit**		x			
AU-14 (1)	*SESSION AUDIT | SYSTEM START-UP*		x			
AU-14 (2)	*SESSION AUDIT | CAPTURE/RECORD AND LOG CONTENT*		x			
AU-14 (3)	*SESSION AUDIT | REMOTE VIEWING / LISTENING*		x			
AU-15	**Alternate Audit Capability**					
AU-16	**Cross-Organizational Auditing**					
AU-16 (1)	*CROSS-ORGANIZATIONAL AUDITING | IDENTITY PRESERVATION*					
AU-16 (2)	*CROSS-ORGANIZATIONAL AUDITING | SHARING OF AUDIT INFORMATION*					

TABLE D-6: SUMMARY — SECURITY ASSESSMENT AND AUTHORIZATION CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CA-1	**Security Assessment and Authorization Policies and Procedures**		x	x	x	x
CA-2	**Security Assessments**		x	x	x	x
CA-2 (1)	*SECURITY ASSESSMENTS | INDEPENDENT ASSESSORS*		x		x	x
CA-2 (2)	*SECURITY ASSESSMENTS | SPECIALIZED ASSESSMENTS*		x			x
CA-2 (3)	*SECURITY ASSESSMENTS | EXTERNAL ORGANIZATIONS*		x			
CA-3	**System Interconnections**		x	x	x	x
CA-3 (1)	*SYSTEM INTERCONNECTIONS | UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS*					
CA-3 (2)	*SYSTEM INTERCONNECTIONS | CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS*					
CA-3 (3)	*SYSTEM INTERCONNECTIONS | UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS*					
CA-3 (4)	*SYSTEM INTERCONNECTIONS | CONNECTIONS TO PUBLIC NETWORKS*					
CA-3 (5)	*SYSTEM INTERCONNECTIONS | RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS*				x	x
CA-4	**Security Certification**	x	Incorporated into CA-2.			
CA-5	**Plan of Action and Milestones**		x	x	x	x
CA-5 (1)	*PLAN OF ACTION AND MILESTONES | AUTOMATION SUPPORT FOR ACCURACY / CURRENCY*		x			
CA-6	**Security Authorization**		x	x	x	x
CA-7	**Continuous Monitoring**		x	x	x	x
CA-7 (1)	*CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT*		x		x	x
CA-7 (2)	*CONTINUOUS MONITORING | TYPES OF ASSESSMENTS*	x	Incorporated into CA-2.			
CA-7 (3)	*CONTINUOUS MONITORING | TREND ANALYSES*		x			
CA-8	**Penetration Testing**		x			x
CA-8 (1)	*PENETRATION TESTING | INDEPENDENT PENETRATION AGENT OR TEAM*		x			
CA-8 (2)	*PENETRATION TESTING | RED TEAM EXERCISES*		x			
CA-9	**Internal System Connections**		x	x	x	x
CA-9 (1)	*INTERNAL SYSTEM CONNECTIONS | SECURITY COMPLIANCE CHECKS*		x			

TABLE D-7: SUMMARY — CONFIGURATION MANAGEMENT CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CM-1	**Configuration Management Policy and Procedures**		x	x	x	x
CM-2	**Baseline Configuration**		x	x	x	x
CM-2 (1)	*BASELINE CONFIGURATION | REVIEWS AND UPDATES*		x		x	x
CM-2 (2)	*BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY / CURRENCY*		x			x
CM-2 (3)	*BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS*		x		x	x
CM-2 (4)	*BASELINE CONFIGURATION | UNAUTHORIZED SOFTWARE*	x	Incorporated into CM-7.			
CM-2 (5)	*BASELINE CONFIGURATION | AUTHORIZED SOFTWARE*	x	Incorporated into CM-7.			
CM-2 (6)	*BASELINE CONFIGURATION | DEVELOPMENT AND TEST ENVIRONMENTS*		x			
CM-2 (7)	*BASELINE CONFIGURATION | CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS*		x		x	x
CM-3	**Configuration Change Control**		x		x	x
CM-3 (1)	*CONFIGURATION CHANGE CONTROL | AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES*		x			x
CM-3 (2)	*CONFIGURATION CHANGE CONTROL | TEST / VALIDATE / DOCUMENT CHANGES*		x		x	x
CM-3 (3)	*CONFIGURATION CHANGE CONTROL | AUTOMATED CHANGE IMPLEMENTATION*					
CM-3 (4)	*CONFIGURATION CHANGE CONTROL | SECURITY REPRESENTATIVE*					
CM-3 (5)	*CONFIGURATION CHANGE CONTROL | AUTOMATED SECURITY RESPONSE*					
CM-3 (6)	*CONFIGURATION CHANGE CONTROL | CRYPTOGRAPHY MANAGEMENT*					
CM-4	**Security Impact Analysis**		x	x	x	x
CM-4 (1)	*SECURITY IMPACT ANALYSIS | SEPARATE TEST ENVIRONMENTS*		x			x
CM-4 (2)	*SECURITY IMPACT ANALYSIS | VERIFICATION OF SECURITY FUNCTIONS*		x			
CM-5	**Access Restrictions for Change**				x	x
CM-5 (1)	*ACCESS RESTRICTIONS FOR CHANGE | AUTOMATED ACCESS ENFORCEMENT / AUDITING*					x
CM-5 (2)	*ACCESS RESTRICTIONS FOR CHANGE | REVIEW SYSTEM CHANGES*					x
CM-5 (3)	*ACCESS RESTRICTIONS FOR CHANGE | SIGNED COMPONENTS*					x
CM-5 (4)	*ACCESS RESTRICTIONS FOR CHANGE | DUAL AUTHORIZATION*					
CM-5 (5)	*ACCESS RESTRICTIONS FOR CHANGE | LIMIT PRODUCTION / OPERATIONAL PRIVILEGES*					
CM-5 (6)	*ACCESS RESTRICTIONS FOR CHANGE | LIMIT LIBRARY PRIVILEGES*					
CM-5 (7)	*ACCESS RESTRICTIONS FOR CHANGE | AUTOMATIC IMPLEMENTATION OF SECURITY SAFEGUARDS*	x	Incorporated into SI-7.			
CM-6	**Configuration Settings**			x	x	x
CM-6 (1)	*CONFIGURATION SETTINGS | AUTOMATED CENTRAL MANAGEMENT / APPLICATION / VERIFICATION*					x
CM-6 (2)	*CONFIGURATION SETTINGS | RESPOND TO UNAUTHORIZED CHANGES*					x
CM-6 (3)	*CONFIGURATION SETTINGS | UNAUTHORIZED CHANGE DETECTION*	x	Incorporated into SI-7.			
CM-6 (4)	*CONFIGURATION SETTINGS | CONFORMANCE DEMONSTRATION*	x	Incorporated into CM-4.			
CM-7	**Least Functionality**			x	x	x
CM-7 (1)	*LEAST FUNCTIONALITY | PERIODIC REVIEW*				x	x
CM-7 (2)	*LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION*				x	x

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CM-7 (3)	*LEAST FUNCTIONALITY | REGISTRATION COMPLIANCE*					
CM-7 (4)	*LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE / BLACKLISTING*				X	
CM-7 (5)	*LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE / WHITELISTING*					X
CM-8	**Information System Component Inventory**		X	X	X	X
CM-8 (1)	*INFORMATION SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATIONS / REMOVALS*		X		X	X
CM-8 (2)	*INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE*		X			X
CM-8 (3)	*INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION*		X		X	X
CM-8 (4)	*INFORMATION SYSTEM COMPONENT INVENTORY | ACCOUNTABILITY INFORMATION*		X			X
CM-8 (5)	*INFORMATION SYSTEM COMPONENT INVENTORY | NO DUPLICATE ACCOUNTING OF COMPONENTS*		X		X	X
CM-8 (6)	*INFORMATION SYSTEM COMPONENT INVENTORY | ASSESSED CONFIGURATIONS / APPROVED DEVIATIONS*		X			
CM-8 (7)	*INFORMATION SYSTEM COMPONENT INVENTORY | CENTRALIZED REPOSITORY*		X			
CM-8 (8)	*INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED LOCATION TRACKING*		X			
CM-8 (9)	*INFORMATION SYSTEM COMPONENT INVENTORY | ASSIGNMENT OF COMPONENTS TO SYSTEMS*		X			
CM-9	**Configuration Management Plan**				X	X
CM-9 (1)	*CONFIGURATION MANAGEMENT PLAN | ASSIGNMENT OF RESPONSIBILITY*					
CM-10	**Software Usage Restrictions**			X	X	X
CM-10 (1)	*SOFTWARE USAGE RESTRICTIONS | OPEN SOURCE SOFTWARE*					
CM-11	**User-Installed Software**			X	X	X
CM-11 (1)	*USER-INSTALLED SOFTWARE | ALERTS FOR UNAUTHORIZED INSTALLATIONS*					
CM-11 (2)	*USER-INSTALLED SOFTWARE | PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS*					

TABLE D-8: SUMMARY — CONTINGENCY PLANNING CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CP-1	**Contingency Planning Policy and Procedures**		x	x	x	x
CP-2	**Contingency Plan**			x	x	x
CP-2 (1)	*CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS*				x	x
CP-2 (2)	*CONTINGENCY PLAN | CAPACITY PLANNING*					x
CP-2 (3)	*CONTINGENCY PLAN | RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*				x	x
CP-2 (4)	*CONTINGENCY PLAN | RESUME ALL MISSIONS / BUSINESS FUNCTIONS*					x
CP-2 (5)	*CONTINGENCY PLAN | CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*					x
CP-2 (6)	*CONTINGENCY PLAN | ALTERNATE PROCESSING / STORAGE SITE*					
CP-2 (7)	*CONTINGENCY PLAN | COORDINATE WITH EXTERNAL SERVICE PROVIDERS*					
CP-2 (8)	*CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS*				x	x
CP-3	**Contingency Training**		x	x	x	x
CP-3 (1)	*CONTINGENCY TRAINING | SIMULATED EVENTS*		x			x
CP-3 (2)	*CONTINGENCY TRAINING | AUTOMATED TRAINING ENVIRONMENTS*		x			
CP-4	**Contingency Plan Testing**		x	x	x	x
CP-4 (1)	*CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS*		x		x	x
CP-4 (2)	*CONTINGENCY PLAN TESTING | ALTERNATE PROCESSING SITE*		x			x
CP-4 (3)	*CONTINGENCY PLAN TESTING | AUTOMATED TESTING*		x			
CP-4 (4)	*CONTINGENCY PLAN TESTING | FULL RECOVERY / RECONSTITUTION*		x			
CP-5	**Contingency Plan Update**	x	Incorporated into CP-2.			
CP-6	**Alternate Storage Site**				x	x
CP-6 (1)	*ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE*				x	x
CP-6 (2)	*ALTERNATE STORAGE SITE | RECOVERY TIME / POINT OBJECTIVES*					x
CP-6 (3)	*ALTERNATE STORAGE SITE | ACCESSIBILITY*				x	x
CP-7	**Alternate Processing Site**				x	x
CP-7 (1)	*ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE*				x	x
CP-7 (2)	*ALTERNATE PROCESSING SITE | ACCESSIBILITY*				x	x
CP-7 (3)	*ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE*				x	x
CP-7 (4)	*ALTERNATE PROCESSING SITE | PREPARATION FOR USE*					x
CP-7 (5)	*ALTERNATE PROCESSING SITE | EQUIVALENT INFORMATION SECURITY SAFEGUARDS*	x	Incorporated into CP-7.			
CP-7 (6)	*ALTERNATE PROCESSING SITE | INABILITY TO RETURN TO PRIMARY SITE*					
CP-8	**Telecommunications Services**				x	x
CP-8 (1)	*TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS*				x	x
CP-8 (2)	*TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE*				x	x
CP-8 (3)	*TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY / ALTERNATE PROVIDERS*					x
CP-8 (4)	*TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN*					x
CP-8 (5)	*TELECOMMUNICATIONS SERVICES | ALTERNATE TELECOMMUNICATION SERVICE TESTING*					
CP-9	**Information System Backup**			x	x	x
CP-9 (1)	*INFORMATION SYSTEM BACKUP | TESTING FOR RELIABILITY / INTEGRITY*				x	x

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CP-9 (2)	*INFORMATION SYSTEM BACKUP | TEST RESTORATION USING SAMPLING*					x
CP-9 (3)	*INFORMATION SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION*					x
CP-9 (4)	*INFORMATION SYSTEM BACKUP | PROTECTION FROM UNAUTHORIZED MODIFICATION*	x	Incorporated into CP-9.			
CP-9 (5)	*INFORMATION SYSTEM BACKUP | TRANSFER TO ALTERNATE STORAGE SITE*					x
CP-9 (6)	*INFORMATION SYSTEM BACKUP | REDUNDANT SECONDARY SYSTEM*					
CP-9 (7)	*INFORMATION SYSTEM BACKUP | DUAL AUTHORIZATION*					
CP-10	**Information System Recovery and Reconstitution**			x	x	x
CP-10 (1)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | CONTINGENCY PLAN TESTING*	x	Incorporated into CP-4.			
CP-10 (2)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY*				x	x
CP-10 (3)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | COMPENSATING SECURITY CONTROLS*	x	Addressed by tailoring procedures.			
CP-10 (4)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME PERIOD*					x
CP-10 (5)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | FAILOVER CAPABILITY*	x	Incorporated into SI-13.			
CP-10 (6)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | COMPONENT PROTECTION*					
CP-11	**Alternate Communications Protocols**					
CP-12	**Safe Mode**		x			
CP-13	**Alternative Security Mechanisms**					

TABLE D-9: SUMMARY — IDENTIFICATION AND AUTHENTICATION CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
IA-1	**Identification and Authentication Policy and Procedures**		x	x	x	x
IA-2	**Identification and Authentication (Organizational Users)**			x	x	x
IA-2 (1)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO PRIVILEGED ACCOUNTS*			x	x	x
IA-2 (2)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS*				x	x
IA-2 (3)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | LOCAL ACCESS TO PRIVILEGED ACCOUNTS*				x	x
IA-2 (4)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS*					x
IA-2 (5)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | GROUP AUTHENTICATION*					
IA-2 (6)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - SEPARATE DEVICE*					
IA-2 (7)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - SEPARATE DEVICE*					
IA-2 (8)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT*				x	x
IA-2 (9)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - REPLAY RESISTANT*					x
IA-2 (10)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | SINGLE SIGN-ON*					
IA-2 (11)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | REMOTE ACCESS - SEPARATE DEVICE*				x	x
IA-2 (12)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS*			x	x	x
IA-2 (13)	*IDENTIFICATION AND AUTHENTICATION | OUT-OF-BAND AUTHENTICATION*					
IA-3	**Device Identification and Authentication**				x	x
IA-3 (1)	*DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION*					
IA-3 (2)	*DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL NETWORK AUTHENTICATION*	x	Incorporated into IA-3 (1).			
IA-3 (3)	*DEVICE IDENTIFICATION AND AUTHENTICATION | DYNAMIC ADDRESS ALLOCATION*					
IA-3 (4)	*DEVICE IDENTIFICATION AND AUTHENTICATION | DEVICE ATTESTATION*					
IA-4	**Identifier Management**			x	x	x
IA-4 (1)	*IDENTIFIER MANAGEMENT | PROHIBIT ACCOUNT IDENTIFIERS AS PUBLIC IDENTIFIERS*					
IA-4 (2)	*IDENTIFIER MANAGEMENT | SUPERVISOR AUTHORIZATION*					
IA-4 (3)	*IDENTIFIER MANAGEMENT | MULTIPLE FORMS OF CERTIFICATION*					
IA-4 (4)	*IDENTIFIER MANAGEMENT | IDENTIFY USER STATUS*					
IA-4 (5)	*IDENTIFIER MANAGEMENT | DYNAMIC MANAGEMENT*					
IA-4 (6)	*IDENTIFIER MANAGEMENT | CROSS-ORGANIZATION MANAGEMENT*					
IA-4 (7)	*IDENTIFIER MANAGEMENT | IN-PERSON REGISTRATION*					
IA-5	**Authenticator Management**			x	x	x

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
IA-5 (1)	*AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION*			X	X	X
IA-5 (2)	*AUTHENTICATOR MANAGEMENT | PKI-BASED AUTHENTICATION*				X	X
IA-5 (3)	*AUTHENTICATOR MANAGEMENT | IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION*				X	X
IA-5 (4)	*AUTHENTICATOR MANAGEMENT | AUTOMATED SUPPORT FOR PASSWORD STRENGTH DETERMINATION*					
IA-5 (5)	*AUTHENTICATOR MANAGEMENT | CHANGE AUTHENTICATORS PRIOR TO DELIVERY*					
IA-5 (6)	*AUTHENTICATOR MANAGEMENT | PROTECTION OF AUTHENTICATORS*					
IA-5 (7)	*AUTHENTICATOR MANAGEMENT | NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS*					
IA-5 (8)	*AUTHENTICATOR MANAGEMENT | MULTIPLE INFORMATION SYSTEM ACCOUNTS*					
IA-5 (9)	*AUTHENTICATOR MANAGEMENT | CROSS-ORGANIZATION CREDENTIAL MANAGEMENT*					
IA-5 (10)	*AUTHENTICATOR MANAGEMENT | DYNAMIC CREDENTIAL ASSOCIATION*					
IA-5 (11)	*AUTHENTICATOR MANAGEMENT | HARDWARE TOKEN-BASED AUTHENTICATION*			X	X	X
IA-5 (12)	*AUTHENTICATOR MANAGEMENT | BIOMETRIC AUTHENTICATION*					
IA-5 (13)	*AUTHENTICATOR MANAGEMENT | EXPIRATION OF CACHED AUTHENTICATORS*					
IA-5 (14)	*AUTHENTICATOR MANAGEMENT | MANAGING CONTENT OF PKI TRUST STORES*					
IA-5 (15)	*AUTHENTICATOR MANAGEMENT | FICAM-APPROVED PRODUCTS AND SERVICES*					
IA-6	**Authenticator Feedback**			X	X	X
IA-7	**Cryptographic Module Authentication**			X	X	X
IA-8	**Identification and Authentication (Non-Organizational Users)**			X	X	X
IA-8 (1)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES*			X	X	X
IA-8 (2)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF THIRD-PARTY CREDENTIALS*			X	X	X
IA-8 (3)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF FICAM-APPROVED PRODUCTS*			X	X	X
IA-8 (4)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF FICAM-ISSUED PROFILES*			X	X	X
IA-8 (5)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV-I CREDENTIALS*					
IA-9	**Service Identification and Authentication**					
IA-9 (1)	*SERVICE IDENTIFICATION AND AUTHENTICATION | INFORMATION EXCHANGE*					
IA-9 (2)	*SERVICE IDENTIFICATION AND AUTHENTICATION | TRANSMISSION OF DECISIONS*					
IA-10	**Adaptive Identification and Authentication**					
IA-11	**Re-authentication**					

TABLE D-10: SUMMARY — INCIDENT RESPONSE CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
IR-1	**Incident Response Policy and Procedures**		X	X	X	X
IR-2	**Incident Response Training**		X	X	X	X
IR-2 (1)	*INCIDENT RESPONSE TRAINING | SIMULATED EVENTS*		X			X
IR-2 (2)	*INCIDENT RESPONSE TRAINING | AUTOMATED TRAINING ENVIRONMENTS*		X			X
IR-3	**Incident Response Testing**		X		X	X
IR-3 (1)	*INCIDENT RESPONSE TESTING | AUTOMATED TESTING*		X			
IR-3 (2)	*INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS*		X		X	X
IR-4	**Incident Handling**			X	X	X
IR-4 (1)	*INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES*				X	X
IR-4 (2)	*INCIDENT HANDLING | DYNAMIC RECONFIGURATION*					
IR-4 (3)	*INCIDENT HANDLING | CONTINUITY OF OPERATIONS*					
IR-4 (4)	*INCIDENT HANDLING | INFORMATION CORRELATION*					X
IR-4 (5)	*INCIDENT HANDLING | AUTOMATIC DISABLING OF INFORMATION SYSTEM*					
IR-4 (6)	*INCIDENT HANDLING | INSIDER THREATS - SPECIFIC CAPABILITIES*					
IR-4 (7)	*INCIDENT HANDLING | INSIDER THREATS - INTRA-ORGANIZATION COORDINATION*					
IR-4 (8)	*INCIDENT HANDLING | CORRELATION WITH EXTERNAL ORGANIZATIONS*					
IR-4 (9)	*INCIDENT HANDLING | DYNAMIC RESPONSE CAPABILITY*					
IR-4 (10)	*INCIDENT HANDLING | SUPPLY CHAIN COORDINATION*					
IR-5	**Incident Monitoring**		X	X	X	X
IR-5 (1)	*INCIDENT MONITORING | AUTOMATED TRACKING / DATA COLLECTION / ANALYSIS*		X			X
IR-6	**Incident Reporting**			X	X	X
IR-6 (1)	*INCIDENT REPORTING | AUTOMATED REPORTING*				X	X
IR-6 (2)	*INCIDENT REPORTING | VULNERABILITIES RELATED TO INCIDENTS*					
IR-6 (3)	*INCIDENT REPORTING | COORDINATION WITH SUPPLY CHAIN*					
IR-7	**Incident Response Assistance**			X	X	X
IR-7 (1)	*INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT*				X	X
IR-7 (2)	*INCIDENT RESPONSE ASSISTANCE | COORDINATION WITH EXTERNAL PROVIDERS*					
IR-8	**Incident Response Plan**			X	X	X
IR-9	**Information Spillage Response**					
IR-9 (1)	*INFORMATION SPILLAGE RESPONSE | RESPONSIBLE PERSONNEL*					
IR-9 (2)	*INFORMATION SPILLAGE RESPONSE | TRAINING*					
IR-9 (3)	*INFORMATION SPILLAGE RESPONSE | POST-SPILL OPERATIONS*					
IR-9 (4)	*INFORMATION SPILLAGE RESPONSE | EXPOSURE TO UNAUTHORIZED PERSONNEL*					
IR-10	**Integrated Information Security Analysis Team**					

TABLE D-11: SUMMARY — MAINTENANCE CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
MA-1	**System Maintenance Policy and Procedures**		x	x	x	x
MA-2	**Controlled Maintenance**			x	x	x
MA-2 (1)	*CONTROLLED MAINTENANCE | RECORD CONTENT*	x	Incorporated into MA-2.			
MA-2 (2)	*CONTROLLED MAINTENANCE | AUTOMATED MAINTENANCE ACTIVITIES*					x
MA-3	**Maintenance Tools**				x	x
MA-3 (1)	*MAINTENANCE TOOLS | INSPECT TOOLS*				x	x
MA-3 (2)	*MAINTENANCE TOOLS | INSPECT MEDIA*				x	x
MA-3 (3)	*MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL*					x
MA-3 (4)	*MAINTENANCE TOOLS | RESTRICTED TOOL USE*					
MA-4	**Nonlocal Maintenance**			x	x	x
MA-4 (1)	*NONLOCAL MAINTENANCE | AUDITING AND REVIEW*					
MA-4 (2)	*NONLOCAL MAINTENANCE | DOCUMENT NONLOCAL MAINTENANCE*				x	x
MA-4 (3)	*NONLOCAL MAINTENANCE | COMPARABLE SECURITY / SANITIZATION*					x
MA-4 (4)	*NONLOCAL MAINTENANCE | AUTHENTICATION / SEPARATION OF MAINTENANCE SESSIONS*					
MA-4 (5)	*NONLOCAL MAINTENANCE | APPROVALS AND NOTIFICATIONS*					
MA-4 (6)	*NONLOCAL MAINTENANCE | CRYPTOGRAPHIC PROTECTION*					
MA-4 (7)	*NONLOCAL MAINTENANCE | REMOTE DISCONNECT VERIFICATION*					
MA-5	**Maintenance Personnel**			x	x	x
MA-5 (1)	*MAINTENANCE PERSONNEL | INDIVIDUALS WITHOUT APPROPRIATE ACCESS*					x
MA-5 (2)	*MAINTENANCE PERSONNEL | SECURITY CLEARANCES FOR CLASSIFIED SYSTEMS*					
MA-5 (3)	*MAINTENANCE PERSONNEL | CITIZENSHIP REQUIREMENTS FOR CLASSIFIED SYSTEMS*					
MA-5 (4)	*MAINTENANCE PERSONNEL | FOREIGN NATIONALS*					
MA-5 (5)	*MAINTENANCE PERSONNEL | NON-SYSTEM-RELATED MAINTENANCE*					
MA-6	**Timely Maintenance**				x	x
MA-6 (1)	*TIMELY MAINTENANCE | PREVENTIVE MAINTENANCE*					
MA-6 (2)	*TIMELY MAINTENANCE | PREDICTIVE MAINTENANCE*					
MA-6 (3)	*TIMELY MAINTENANCE | AUTOMATED SUPPORT FOR PREDICTIVE MAINTENANCE*					

TABLE D-12: SUMMARY — MEDIA PROTECTION CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
MP-1	**Media Protection Policy and Procedures**		x	x	x	x
MP-2	**Media Access**			x	x	x
MP-2 (1)	*MEDIA ACCESS | AUTOMATED RESTRICTED ACCESS*	x	Incorporated into MP-4 (2).			
MP-2 (2)	*MEDIA ACCESS | CRYPTOGRAPHIC PROTECTION*	x	Incorporated into SC-28 (1).			
MP-3	**Media Marking**				x	x
MP-4	**Media Storage**				x	x
MP-4 (1)	*MEDIA STORAGE | CRYPTOGRAPHIC PROTECTION*	x	Incorporated into SC-28 (1).			
MP-4 (2)	*MEDIA STORAGE | AUTOMATED RESTRICTED ACCESS*					
MP-5	**Media Transport**				x	x
MP-5 (1)	*MEDIA TRANSPORT | PROTECTION OUTSIDE OF CONTROLLED AREAS*	x	Incorporated into MP-5.			
MP-5 (2)	*MEDIA TRANSPORT | DOCUMENTATION OF ACTIVITIES*	x	Incorporated into MP-5.			
MP-5 (3)	*MEDIA TRANSPORT | CUSTODIANS*					
MP-5 (4)	*MEDIA TRANSPORT | CRYPTOGRAPHIC PROTECTION*				x	x
MP-6	**Media Sanitization**			x	x	x
MP-6 (1)	*MEDIA SANITIZATION | REVIEW / APPROVE / TRACK / DOCUMENT / VERIFY*					x
MP-6 (2)	*MEDIA SANITIZATION | EQUIPMENT TESTING*					x
MP-6 (3)	*MEDIA SANITIZATION | NONDESTRUCTIVE TECHNIQUES*					x
MP-6 (4)	*MEDIA SANITIZATION | CONTROLLED UNCLASSIFIED INFORMATION*	x	Incorporated into MP-6.			
MP-6 (5)	*MEDIA SANITIZATION | CLASSIFIED INFORMATION*	x	Incorporated into MP-6.			
MP-6 (6)	*MEDIA SANITIZATION | MEDIA DESTRUCTION*	x	Incorporated into MP-6.			
MP-6 (7)	*MEDIA SANITIZATION | DUAL AUTHORIZATION*					
MP-6 (8)	*MEDIA SANITIZATION | REMOTE PURGING / WIPING OF INFORMATION*					
MP-7	**Media Use**			x	x	x
MP-7 (1)	*MEDIA USE | PROHIBIT USE WITHOUT OWNER*				x	x
MP-7 (2)	*MEDIA USE | PROHIBIT USE OF SANITIZATION-RESISTANT MEDIA*					
MP-8	**Media Downgrading**					
MP-8 (1)	*MEDIA DOWNGRADING | DOCUMENTATION OF PROCESS*					
MP-8 (2)	*MEDIA DOWNGRADING | EQUIPMENT TESTING*					
MP-8 (3)	*MEDIA DOWNGRADING | CONTROLLED UNCLASSIFIED INFORMATION*					
MP-8 (4)	*MEDIA DOWNGRADING | CLASSIFIED INFORMATION*					

TABLE D-13: SUMMARY — PHYSICAL AND ENVIRONMENTAL PROTECTION CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
PE-1	**Physical and Environmental Protection Policy and Procedures**		x	x	x	x
PE-2	**Physical Access Authorizations**			x	x	x
PE-2 (1)	*PHYSICAL ACCESS AUTHORIZATIONS | ACCESS BY POSITION / ROLE*					
PE-2 (2)	*PHYSICAL ACCESS AUTHORIZATIONS | TWO FORMS OF IDENTIFICATION*					
PE-2 (3)	*PHYSICAL ACCESS AUTHORIZATIONS | RESTRICT UNESCORTED ACCESS*					
PE-3	**Physical Access Control**			x	x	x
PE-3 (1)	*PHYSICAL ACCESS CONTROL | INFORMATION SYSTEM ACCESS*					x
PE-3 (2)	*PHYSICAL ACCESS CONTROL | FACILITY / INFORMATION SYSTEM BOUNDARIES*					
PE-3 (3)	*PHYSICAL ACCESS CONTROL | CONTINUOUS GUARDS / ALARMS / MONITORING*					
PE-3 (4)	*PHYSICAL ACCESS CONTROL | LOCKABLE CASINGS*					
PE-3 (5)	*PHYSICAL ACCESS CONTROL | TAMPER PROTECTION*					
PE-3 (6)	*PHYSICAL ACCESS CONTROL | FACILITY PENETRATION TESTING*					
PE-4	**Access Control for Transmission Medium**				x	x
PE-5	**Access Control for Output Devices**				x	x
PE-5 (1)	*ACCESS CONTROL FOR OUTPUT DEVICES | ACCESS TO OUTPUT BY AUTHORIZED INDIVIDUALS*					
PE-5 (2)	*ACCESS CONTROL FOR OUTPUT DEVICES | ACCESS TO OUTPUT BY INDIVIDUAL IDENTITY*					
PE-5 (3)	*ACCESS CONTROL FOR OUTPUT DEVICES | MARKING OUTPUT DEVICES*					
PE-6	**Monitoring Physical Access**		x	x	x	x
PE-6 (1)	*MONITORING PHYSICAL ACCESS | INTRUSION ALARMS / SURVEILLANCE EQUIPMENT*		x		x	x
PE-6 (2)	*MONITORING PHYSICAL ACCESS | AUTOMATED INTRUSION RECOGNITION / RESPONSES*		x			
PE-6 (3)	*MONITORING PHYSICAL ACCESS | VIDEO SURVEILLANCE*		x			
PE-6 (4)	*MONITORING PHYSICAL ACCESS | MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS*		x			x
PE-7	**Visitor Control**	x	Incorporated into PE-2 and PE-3.			
PE-8	**Visitor Access Records**		x	x	x	x
PE-8 (1)	*VISITOR ACCESS RECORDS | AUTOMATED RECORDS MAINTENANCE / REVIEW*					x
PE-8 (2)	*VISITOR ACCESS RECORDS | PHYSICAL ACCESS RECORDS*	x	Incorporated into PE-2.			
PE-9	**Power Equipment and Cabling**				x	x
PE-9 (1)	*POWER EQUIPMENT AND CABLING | REDUNDANT CABLING*					
PE-9 (2)	*POWER EQUIPMENT AND CABLING | AUTOMATIC VOLTAGE CONTROLS*					
PE-10	**Emergency Shutoff**				x	x
PE-10 (1)	*EMERGENCY SHUTOFF | ACCIDENTAL / UNAUTHORIZED ACTIVATION*	x	Incorporated into PE-10.			
PE-11	**Emergency Power**				x	x
PE-11 (1)	*EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY - MINIMAL OPERATIONAL CAPABILITY*					x
PE-11 (2)	*EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY - SELF-CONTAINED*					

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
PE-12	**Emergency Lighting**			x	x	x
PE-12 (1)	*EMERGENCY LIGHTING | ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*					
PE-13	**Fire Protection**			x	x	x
PE-13 (1)	*FIRE PROTECTION | DETECTION DEVICES / SYSTEMS*					x
PE-13 (2)	*FIRE PROTECTION | SUPPRESSION DEVICES / SYSTEMS*					x
PE-13 (3)	*FIRE PROTECTION | AUTOMATIC FIRE SUPPRESSION*				x	x
PE-13 (4)	*FIRE PROTECTION | INSPECTIONS*					
PE-14	**Temperature and Humidity Controls**			x	x	x
PE-14 (1)	*TEMPERATURE AND HUMIDITY CONTROLS | AUTOMATIC CONTROLS*					
PE-14 (2)	*TEMPERATURE AND HUMIDITY CONTROLS | MONITORING WITH ALARMS / NOTIFICATIONS*					
PE-15	**Water Damage Protection**			x	x	x
PE-15 (1)	*WATER DAMAGE PROTECTION | AUTOMATION SUPPORT*					x
PE-16	**Delivery and Removal**			x	x	x
PE-17	**Alternate Work Site**				x	x
PE-18	**Location of Information System Components**					x
PE-18 (1)	*LOCATION OF INFORMATION SYSTEM COMPONENTS | FACILITY SITE*					
PE-19	**Information Leakage**					
PE-19 (1)	*INFORMATION LEAKAGE | NATIONAL EMISSIONS / TEMPEST POLICIES AND PROCEDURES*					
PE-20	**Asset Monitoring and Tracking**					

TABLE D-14: SUMMARY — PLANNING CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
PL-1	**Security Planning Policy and Procedures**		x	x	x	x
PL-2	**System Security Plan**		x	x	x	x
PL-2 (1)	*SYSTEM SECURITY PLAN | CONCEPT OF OPERATIONS*	x	Incorporated into PL-7.			
PL-2 (2)	*SYSTEM SECURITY PLAN | FUNCTIONAL ARCHITECTURE*	x	Incorporated into PL-8.			
PL-2 (3)	*SYSTEM SECURITY PLAN | PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES*		x		x	x
PL-3	**System Security Plan Update**	x	Incorporated into PL-2.			
PL-4	**Rules of Behavior**		x	x	x	x
PL-4 (1)	*RULES OF BEHAVIOR | SOCIAL MEDIA AND NETWORKING RESTRICTIONS*		x		x	x
PL-5	**Privacy Impact Assessment**	x	Incorporated into Appendix J, AR-2.			
PL-6	**Security-Related Activity Planning**	x	Incorporated into PL-2.			
PL-7	**Security Concept of Operations**					
PL-8	**Information Security Architecture**		x		x	x
PL-8 (1)	*INFORMATION SECURITY ARCHITECTURE | DEFENSE-IN-DEPTH*		x			
PL-8 (2)	*INFORMATION SECURITY ARCHITECTURE | SUPPLIER DIVERSITY*		x			
PL-9	**Central Management**		x			

TABLE D-15: SUMMARY — PERSONNEL SECURITY CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
PS-1	**Personnel Security Policy and Procedures**		x	x	x	x
PS-2	**Position Risk Designation**			x	x	x
PS-3	**Personnel Screening**			x	x	x
PS-3 (1)	*PERSONNEL SCREENING | CLASSIFIED INFORMATION*					
PS-3 (2)	*PERSONNEL SCREENING | FORMAL INDOCTRINATION*					
PS-3 (3)	*PERSONNEL SCREENING | INFORMATION WITH SPECIAL PROTECTION MEASURES*					
PS-4	**Personnel Termination**			x	x	x
PS-4 (1)	*PERSONNEL TERMINATION | POST-EMPLOYMENT REQUIREMENTS*					
PS-4 (2)	*PERSONNEL TERMINATION | AUTOMATED NOTIFICATION*					x
PS-5	**Personnel Transfer**			x	x	x
PS-6	**Access Agreements**		x	x	x	x
PS-6 (1)	*ACCESS AGREEMENTS | INFORMATION REQUIRING SPECIAL PROTECTION*	x	Incorporated into PS-3.			
PS-6 (2)	*ACCESS AGREEMENTS | CLASSIFIED INFORMATION REQUIRING SPECIAL PROTECTION*		x			
PS-6 (3)	*ACCESS AGREEMENTS | POST-EMPLOYMENT REQUIREMENTS*		x			
PS-7	**Third-Party Personnel Security**		x	x	x	x
PS-8	**Personnel Sanctions**			x	x	x

TABLE D-16: SUMMARY — RISK ASSESSMENT CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
RA-1	**Risk Assessment Policy and Procedures**		x	x	x	x
RA-2	**Security Categorization**			x	x	x
RA-3	**Risk Assessment**		x	x	x	x
RA-4	**Risk Assessment Update**	x	Incorporated into RA-3.			
RA-5	**Vulnerability Scanning**		x	x	x	x
RA-5 (1)	*VULNERABILITY SCANNING | UPDATE TOOL CAPABILITY*		x		x	x
RA-5 (2)	*VULNERABILITY SCANNING | UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED*		x		x	x
RA-5 (3)	*VULNERABILITY SCANNING | BREADTH / DEPTH OF COVERAGE*		x			
RA-5 (4)	*VULNERABILITY SCANNING | DISCOVERABLE INFORMATION*		x			x
RA-5 (5)	*VULNERABILITY SCANNING | PRIVILEGED ACCESS*		x		x	x
RA-5 (6)	*VULNERABILITY SCANNING | AUTOMATED TREND ANALYSES*		x			
RA-5 (7)	*VULNERABILITY SCANNING | AUTOMATED DETECTION AND NOTIFICATION OF UNAUTHORIZED COMPONENTS*	x	Incorporated into CM-8.			
RA-5 (8)	*VULNERABILITY SCANNING | REVIEW HISTORIC AUDIT LOGS*		x			
RA-5 (9)	*VULNERABILITY SCANNING | PENETRATION TESTING AND ANALYSES*	x	Incorporated into CA-8.			
RA-5 (10)	*VULNERABILITY SCANNING | CORRELATE SCANNING INFORMATION*		x			
RA-6	**Technical Surveillance Countermeasures Survey**		x			

TABLE D-17: SUMMARY — SYSTEM AND SERVICES ACQUISITION CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SA-1	**System and Services Acquisition Policy and Procedures**		x	x	x	x
SA-2	**Allocation of Resources**		x	x	x	x
SA-3	**System Development Life Cycle**		x	x	x	x
SA-4	**Acquisition Process**		x	x	x	x
SA-4 (1)	*ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS*		x		x	x
SA-4 (2)	*ACQUISITION PROCESS | DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS*		x		x	x
SA-4 (3)	*ACQUISITION PROCESS | DEVELOPMENT METHODS / TECHNIQUES / PRACTICES*		x			
SA-4 (4)	*ACQUISITION PROCESS | ASSIGNMENT OF COMPONENTS TO SYSTEMS*	x	Incorporated into CM-8 (9).			
SA-4 (5)	*ACQUISITION PROCESS | SYSTEM / COMPONENT / SERVICE CONFIGURATIONS*		x			
SA-4 (6)	*ACQUISITION PROCESS | USE OF INFORMATION ASSURANCE PRODUCTS*		x			
SA-4 (7)	*ACQUISITION PROCESS | NIAP-APPROVED PROTECTION PROFILES*		x			
SA-4 (8)	*ACQUISITION PROCESS | CONTINUOUS MONITORING PLAN*		x			
SA-4 (9)	*ACQUISITION PROCESS | FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE*		x		x	x
SA-4 (10)	*ACQUISITION PROCESS | USE OF APPROVED PIV PRODUCTS*		x	x	x	x
SA-5	**Information System Documentation**		x	x	x	x
SA-5 (1)	*INFORMATION SYSTEM DOCUMENTATION | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS*	x	Incorporated into SA-4 (1).			
SA-5 (2)	*INFORMATION SYSTEM DOCUMENTATION | SECURITY-RELEVANT EXTERNAL SYSTEM INTERFACES*	x	Incorporated into SA-4 (2).			
SA-5 (3)	*INFORMATION SYSTEM DOCUMENTATION | HIGH-LEVEL DESIGN*	x	Incorporated into SA-4 (2).			
SA-5 (4)	*INFORMATION SYSTEM DOCUMENTATION | LOW-LEVEL DESIGN*	x	Incorporated into SA-4 (2).			
SA-5 (5)	*INFORMATION SYSTEM DOCUMENTATION | SOURCE CODE*	x	Incorporated into SA-4 (2).			
SA-6	**Software Usage Restrictions**	x	Incorporated into CM-10 and SI-7.			
SA-7	**User-Installed Software**	x	Incorporated into CM-11 and SI-7.			
SA-8	**Security Engineering Principles**		x		x	x
SA-9	**External Information System Services**		x	x	x	x
SA-9 (1)	*EXTERNAL INFORMATION SYSTEMS | RISK ASSESSMENTS / ORGANIZATIONAL APPROVALS*		x			
SA-9 (2)	*EXTERNAL INFORMATION SYSTEMS | IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES*		x		x	x
SA-9 (3)	*EXTERNAL INFORMATION SYSTEMS | ESTABLISH / MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS*		x			
SA-9 (4)	*EXTERNAL INFORMATION SYSTEMS | CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS*		x			
SA-9 (5)	*EXTERNAL INFORMATION SYSTEMS | PROCESSING, STORAGE, AND SERVICE LOCATION*		x			
SA-10	**Developer Configuration Management**		x		x	x
SA-10 (1)	*DEVELOPER CONFIGURATION MANAGEMENT | SOFTWARE / FIRMWARE INTEGRITY VERIFICATION*		x			
SA-10 (2)	*DEVELOPER CONFIGURATION MANAGEMENT | ALTERNATIVE CONFIGURATION MANAGEMENT PROCESSES*		x			

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SA-10 (3)	*DEVELOPER CONFIGURATION MANAGEMENT | HARDWARE INTEGRITY VERIFICATION*		X			
SA-10 (4)	*DEVELOPER CONFIGURATION MANAGEMENT | TRUSTED GENERATION*		X			
SA-10 (5)	*DEVELOPER CONFIGURATION MANAGEMENT | MAPPING INTEGRITY FOR VERSION CONTROL*		X			
SA-10 (6)	*DEVELOPER CONFIGURATION MANAGEMENT | TRUSTED DISTRIBUTION*		X			
SA-11	**Developer Security Testing and Evaluation**		X		X	X
SA-11 (1)	*DEVELOPER SECURITY TESTING AND EVALUATION | STATIC CODE ANALYSIS*		X			
SA-11 (2)	*DEVELOPER SECURITY TESTING AND EVALUATION | THREAT AND VULNERABILITY ANALYSES*		X			
SA-11 (3)	*DEVELOPER SECURITY TESTING AND EVALUATION | INDEPENDENT VERIFICATION OF ASSESSMENT PLANS / EVIDENCE*		X			
SA-11 (4)	*DEVELOPER SECURITY TESTING AND EVALUATION | MANUAL CODE REVIEWS*		X			
SA-11 (5)	*DEVELOPER SECURITY TESTING AND EVALUATION | PENETRATION TESTING / ANALYSIS*		X			
SA-11 (6)	*DEVELOPER SECURITY TESTING AND EVALUATION | ATTACK SURFACE REVIEWS*		X			
SA-11 (7)	*DEVELOPER SECURITY TESTING AND EVALUATION | VERIFY SCOPE OF TESTING / EVALUATION*		X			
SA-11 (8)	*DEVELOPER SECURITY TESTING AND EVALUATION | DYNAMIC CODE ANALYSIS*		X			
SA-12	**Supply Chain Protection**		X			X
SA-12 (1)	*SUPPLY CHAIN PROTECTION | ACQUISITION STRATEGIES / TOOLS / METHODS*		X			
SA-12 (2)	*SUPPLY CHAIN PROTECTION | SUPPLIER REVIEWS*		X			
SA-12 (3)	*SUPPLY CHAIN PROTECTION | TRUSTED SHIPPING AND WAREHOUSING*	X	Incorporated into SA-12 (1).			
SA-12 (4)	*SUPPLY CHAIN PROTECTION | DIVERSITY OF SUPPLIERS*	X	Incorporated into SA-12 (13).			
SA-12 (5)	*SUPPLY CHAIN PROTECTION | LIMITATION OF HARM*		X			
SA-12 (6)	*SUPPLY CHAIN PROTECTION | MINIMIZING PROCUREMENT TIME*	X	Incorporated into SA-12 (1).			
SA-12 (7)	*SUPPLY CHAIN PROTECTION | ASSESSMENTS PRIOR TO SELECTION / ACCEPTANCE / UPDATE*		X			
SA-12 (8)	*SUPPLY CHAIN PROTECTION | USE OF ALL-SOURCE INTELLIGENCE*		X			
SA-12 (9)	*SUPPLY CHAIN PROTECTION | OPERATIONS SECURITY*		X			
SA-12 (10)	*SUPPLY CHAIN PROTECTION | VALIDATE AS GENUINE AND NOT ALTERED*		X			
SA-12 (11)	*SUPPLY CHAIN PROTECTION | PENETRATION TESTING / ANALYSIS OF ELEMENTS, PROCESSES, AND ACTORS*		X			
SA-12 (12)	*SUPPLY CHAIN PROTECTION | INTER-ORGANIZATIONAL AGREEMENTS*		X			
SA-12 (13)	*SUPPLY CHAIN PROTECTION | CRITICAL INFORMATION SYSTEM COMPONENTS*		X			
SA-12 (14)	*SUPPLY CHAIN PROTECTION | IDENTITY AND TRACEABILITY*		X			
SA-12 (15)	*SUPPLY CHAIN PROTECTION | PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES*		X			
SA-13	**Trustworthiness**		X			
SA-14	**Criticality Analysis**		X			
SA-14 (1)	*CRITICALITY ANALYSIS | CRITICAL COMPONENTS WITH NO VIABLE ALTERNATIVE SOURCING*	X	Incorporated into SA-20.			

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SA-15	**Development Process, Standards, and Tools**		x			x
SA-15 (1)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | QUALITY METRICS*		x			
SA-15 (2)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | SECURITY TRACKING TOOLS*		x			
SA-15 (3)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CRITICALITY ANALYSIS*		x			
SA-15 (4)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | THREAT MODELING / VULNERABILITY ANALYSIS*		x			
SA-15 (5)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ATTACK SURFACE REDUCTION*		x			
SA-15 (6)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CONTINUOUS IMPROVEMENT*		x			
SA-15 (7)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | AUTOMATED VULNERABILITY ANALYSIS*		x			
SA-15 (8)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | REUSE OF THREAT / VULNERABILITY INFORMATION*		x			
SA-15 (9)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | USE OF LIVE DATA*		x			
SA-15 (10)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | INCIDENT RESPONSE PLAN*		x			
SA-15 (11)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ARCHIVE INFORMATION SYSTEM / COMPONENT*		x			
SA-16	**Developer-Provided Training**		x			x
SA-17	**Developer Security Architecture and Design**		x			x
SA-17 (1)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | FORMAL POLICY MODEL*		x			
SA-17 (2)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | SECURITY-RELEVANT COMPONENTS*		x			
SA-17 (3)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | FORMAL CORRESPONDENCE*		x			
SA-17 (4)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | INFORMAL CORRESPONDENCE*		x			
SA-17 (5)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | CONCEPTUALLY SIMPLE DESIGN*		x			
SA-17 (6)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | STRUCTURE FOR TESTING*		x			
SA-17 (7)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | STRUCTURE FOR LEAST PRIVILEGE*		x			
SA-18	**Tamper Resistance and Detection**		x			
SA-18 (1)	*TAMPER RESISTANCE AND DETECTION | MULTIPLE PHASES OF SDLC*		x			
SA-18 (2)	*TAMPER RESISTANCE AND DETECTION | INSPECTION OF INFORMATION SYSTEMS, COMPONENTS, OR DEVICES*		x			
SA-19	**Component Authenticity**		x			
SA-19 (1)	*COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT TRAINING*		x			
SA-19 (2)	*COMPONENT AUTHENTICITY | CONFIGURATION CONTROL FOR COMPONENT SERVICE / REPAIR*		x			
SA-19 (3)	*COMPONENT AUTHENTICITY | COMPONENT DISPOSAL*		x			
SA-19 (4)	*COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT SCANNING*		x			
SA-20	**Customized Development of Critical Components**		x			
SA-21	**Developer Screening**		x			

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SA-21 (1)	*DEVELOPER SCREENING | VALIDATION OF SCREENING*		x			
SA-22	**Unsupported System Components**		x			
SA-22 (1)	*UNSUPPORTED SYSTEM COMPONENTS | ALTERNATIVE SOURCES FOR CONTINUED SUPPORT*		x			

TABLE D-18: SUMMARY — SYSTEM AND COMMUNICATIONS PROTECTION CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SC-1	**System and Communications Protection Policy and Procedures**		x	x	x	x
SC-2	**Application Partitioning**		x		x	x
SC-2 (1)	*APPLICATION PARTITIONING | INTERFACES FOR NON-PRIVILEGED USERS*		x			
SC-3	**Security Function Isolation**		x			x
SC-3 (1)	*SECURITY FUNCTION ISOLATION | HARDWARE SEPARATION*		x			
SC-3 (2)	*SECURITY FUNCTION ISOLATION | ACCESS / FLOW CONTROL FUNCTIONS*		x			
SC-3 (3)	*SECURITY FUNCTION ISOLATION | MINIMIZE NONSECURITY FUNCTIONALITY*		x			
SC-3 (4)	*SECURITY FUNCTION ISOLATION | MODULE COUPLING AND COHESIVENESS*		x			
SC-3 (5)	*SECURITY FUNCTION ISOLATION | LAYERED STRUCTURES*		x			
SC-4	**Information in Shared Resources**				x	x
SC-4 (1)	*INFORMATION IN SHARED RESOURCES | SECURITY LEVELS*	x	Incorporated into SC-4.			
SC-4 (2)	*INFORMATION IN SHARED RESOURCES | PERIODS PROCESSING*					
SC-5	**Denial of Service Protection**			x	x	x
SC-5 (1)	*DENIAL OF SERVICE PROTECTION | RESTRICT INTERNAL USERS*					
SC-5 (2)	*DENIAL OF SERVICE PROTECTION | EXCESS CAPACITY / BANDWIDTH / REDUNDANCY*					
SC-5 (3)	*DENIAL OF SERVICE PROTECTION | DETECTION / MONITORING*					
SC-6	**Resource Availability**		x			
SC-7	**Boundary Protection**			x	x	x
SC-7 (1)	*BOUNDARY PROTECTION | PHYSICALLY SEPARATED SUBNETWORKS*	x	Incorporated into SC-7.			
SC-7 (2)	*BOUNDARY PROTECTION | PUBLIC ACCESS*	x	Incorporated into SC-7.			
SC-7 (3)	*BOUNDARY PROTECTION | ACCESS POINTS*				x	x
SC-7 (4)	*BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES*				x	x
SC-7 (5)	*BOUNDARY PROTECTION | DENY BY DEFAULT / ALLOW BY EXCEPTION*				x	x
SC-7 (6)	*BOUNDARY PROTECTION | RESPONSE TO RECOGNIZED FAILURES*	x	Incorporated into SC-7 (18).			
SC-7 (7)	*BOUNDARY PROTECTION | PREVENT SPLIT TUNNELING FOR REMOTE DEVICES*				x	x
SC-7 (8)	*BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS*					x
SC-7 (9)	*BOUNDARY PROTECTION | RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC*					
SC-7 (10)	*BOUNDARY PROTECTION | PREVENT UNAUTHORIZED EXFILTRATION*					
SC-7 (11)	*BOUNDARY PROTECTION | RESTRICT INCOMING COMMUNICATIONS TRAFFIC*					
SC-7 (12)	*BOUNDARY PROTECTION | HOST-BASED PROTECTION*					
SC-7 (13)	*BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS / MECHANISMS / SUPPORT COMPONENTS*					
SC-7 (14)	*BOUNDARY PROTECTION | PROTECTS AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS*					
SC-7 (15)	*BOUNDARY PROTECTION | ROUTE PRIVILEGED NETWORK ACCESSES*					
SC-7 (16)	*BOUNDARY PROTECTION | PREVENT DISCOVERY OF COMPONENTS / DEVICES*					

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SC-7 (17)	*BOUNDARY PROTECTION | AUTOMATED ENFORCEMENT OF PROTOCOL FORMATS*					
SC-7 (18)	*BOUNDARY PROTECTION | FAIL SECURE*		X			X
SC-7 (19)	*BOUNDARY PROTECTION | BLOCKS COMMUNICATION FROM NON-ORGANIZATIONALLY CONFIGURED HOSTS*					
SC-7 (20)	*BOUNDARY PROTECTION | DYNAMIC ISOLATION / SEGREGATION*					
SC-7 (21)	*BOUNDARY PROTECTION | ISOLATION OF INFORMATION SYSTEM COMPONENTS*		X			X
SC-7 (22)	*BOUNDARY PROTECTION | SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS*		X			
SC-7 (23)	*BOUNDARY PROTECTION | DISABLE SENDER FEEDBACK ON PROTOCOL VALIDATION FAILURE*					
SC-8	**Transmission Confidentiality and Integrity**				X	X
SC-8 (1)	*TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION*				X	X
SC-8 (2)	*TRANSMISSION CONFIDENTIALITY AND INTEGRITY | PRE / POST TRANSMISSION HANDLING*					
SC-8 (3)	*TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC PROTECTION FOR MESSAGE EXTERNALS*					
SC-8 (4)	*TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CONCEAL / RANDOMIZE COMMUNICATIONS*					
SC-9	**Transmission Confidentiality**	X	Incorporated into SC-8.			
SC-10	**Network Disconnect**				X	X
SC-11	**Trusted Path**		X			
SC-11 (1)	*TRUSTED PATH | LOGICAL ISOLATION*		X			
SC-12	**Cryptographic Key Establishment and Management**			X	X	X
SC-12 (1)	*CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY*					X
SC-12 (2)	*CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | SYMMETRIC KEYS*					
SC-12 (3)	*CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | ASYMMETRIC KEYS*					
SC-12 (4)	*CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES*	X	Incorporated into SC-12.			
SC-12 (5)	*CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES / HARDWARE TOKENS*	X	Incorporated into SC-12.			
SC-13	**Cryptographic Protection**			X	X	X
SC-13 (1)	*CRYPTOGRAPHIC PROTECTION | FIPS-VALIDATED CRYPTOGRAPHY*	X	Incorporated into SC-13.			
SC-13 (2)	*CRYPTOGRAPHIC PROTECTION | NSA-APPROVED CRYPTOGRAPHY*	X	Incorporated into SC-13.			
SC-13 (3)	*CRYPTOGRAPHIC PROTECTION | INDIVIDUALS WITHOUT FORMAL ACCESS APPROVALS*	X	Incorporated into SC-13.			
SC-13 (4)	*CRYPTOGRAPHIC PROTECTION | DIGITAL SIGNATURES*	**X**	Incorporated into SC-13.			
SC-14	**Public Access Protections**	**X**	Capability provided by AC-2, AC-3, AC-5, SI-3, SI-4, SI-5, SI-7, SI-10.			
SC-15	**Collaborative Computing Devices**			X	X	X
SC-15 (1)	*COLLABORATIVE COMPUTING DEVICES | PHYSICAL DISCONNECT*					
SC-15 (2)	*COLLABORATIVE COMPUTING DEVICES | BLOCKING INBOUND / OUTBOUND COMMUNICATIONS TRAFFIC*	X	Incorporated into SC-7.			
SC-15 (3)	*COLLABORATIVE COMPUTING DEVICES | DISABLING / REMOVAL IN SECURE WORK AREAS*					

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SC-15 (4)	*COLLABORATIVE COMPUTING DEVICES | EXPLICITLY INDICATE CURRENT PARTICIPANTS*					
SC-16	**Transmission of Security Attributes**					
SC-16 (1)	*TRANSMISSION OF SECURITY ATTRIBUTES | INTEGRITY VALIDATION*					
SC-17	**Public Key Infrastructure Certificates**				X	X
SC-18	**Mobile Code**				X	X
SC-18 (1)	*MOBILE CODE | IDENTIFY UNACCEPTABLE CODE / TAKE CORRECTIVE ACTIONS*					
SC-18 (2)	*MOBILE CODE | ACQUISITION / DEVELOPMENT / USE*					
SC-18 (3)	*MOBILE CODE | PREVENT DOWNLOADING / EXECUTION*					
SC-18 (4)	*MOBILE CODE | PREVENT AUTOMATIC EXECUTION*					
SC-18 (5)	*MOBILE CODE | ALLOW EXECUTION ONLY IN CONFINED ENVIRONMENTS*					
SC-19	**Voice Over Internet Protocol**				X	X
SC-20	**Secure Name /Address Resolution Service (Authoritative Source)**			X	X	X
SC-20 (1)	*SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) | CHILD SUBSPACES*	X	Incorporated into SC-20.			
SC-20 (2)	*SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) | DATA ORIGIN / INTEGRITY*					
SC-21	**Secure Name /Address Resolution Service (Recursive or Caching Resolver)**			X	X	X
SC-21 (1)	*SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER) | DATA ORIGIN / INTEGRITY*	X	Incorporated into SC-21.			
SC-22	**Architecture and Provisioning for Name/Address Resolution Service**			X	X	X
SC-23	**Session Authenticity**				X	X
SC-23 (1)	*SESSION AUTHENTICITY | INVALIDATE SESSION IDENTIFIERS AT LOGOUT*					
SC-23 (2)	*SESSION AUTHENTICITY | USER-INITIATED LOGOUTS / MESSAGE DISPLAYS*	X	Incorporated into AC-12 (1).			
SC-23 (3)	*SESSION AUTHENTICITY | UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION*					
SC-23 (4)	*SESSION AUTHENTICITY | UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION*	X	Incorporated into SC-23 (3).			
SC-23 (5)	*SESSION AUTHENTICITY | ALLOWED CERTIFICATE AUTHORITIES*					
SC-24	**Fail in Known State**		X			X
SC-25	**Thin Nodes**					
SC-26	**Honeypots**					
SC-26 (1)	*HONEYPOTS | DETECTION OF MALICIOUS CODE*	X	Incorporated into SC-35.			
SC-27	**Platform-Independent Applications**					
SC-28	**Protection of Information at Rest**				X	X
SC-28 (1)	*PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION*					
SC-28 (2)	*PROTECTION OF INFORMATION AT REST | OFF-LINE STORAGE*					
SC-29	**Heterogeneity**		X			
SC-29 (1)	*HETEROGENEITY | VIRTUALIZATION TECHNIQUES*		X			
SC-30	**Concealment and Misdirection**		X			
SC-30 (1)	*CONCEALMENT AND MISDIRECTION | VIRTUALIZATION TECHNIQUES*	X	Incorporated into SC-29 (1).			

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SC-30 (2)	*CONCEALMENT AND MISDIRECTION | RANDOMNESS*		x			
SC-30 (3)	*CONCEALMENT AND MISDIRECTION | CHANGE PROCESSING / STORAGE LOCATIONS*		x			
SC-30 (4)	*CONCEALMENT AND MISDIRECTION | MISLEADING INFORMATION*		x			
SC-30 (5)	*CONCEALMENT AND MISDIRECTION | CONCEALMENT OF SYSTEM COMPONENTS*		x			
SC-31	**Covert Channel Analysis**		x			
SC-31 (1)	*COVERT CHANNEL ANALYSIS | TEST COVERT CHANNELS FOR EXPLOITABILITY*		x			
SC-31 (2)	*COVERT CHANNEL ANALYSIS | MAXIMUM BANDWIDTH*		x			
SC-31 (3)	*COVERT CHANNEL ANALYSIS | MEASURE BANDWIDTH IN OPERATIONAL ENVIRONMENTS*		x			
SC-32	**Information System Partitioning**		x			
SC-33	**Transmission Preparation Integrity**	x	Incorporated into SC-8.			
SC-34	**Non-Modifiable Executable Programs**		x			
SC-34 (1)	*NON-MODIFIABLE EXECUTABLE PROGRAMS | NO WRITABLE STORAGE*		x			
SC-34 (2)	*NON-MODIFIABLE EXECUTABLE PROGRAMS | INTEGRITY PROTECTION / READ-ONLY MEDIA*		x			
SC-34 (3)	*NON-MODIFIABLE EXECUTABLE PROGRAMS | HARDWARE-BASED PROTECTION*		x			
SC-35	**Honeyclients**					
SC-36	**Distributed Processing and Storage**		x			
SC-36 (1)	*DISTRIBUTED PROCESSING AND STORAGE | POLLING TECHNIQUES*		x			
SC-37	**Out-of-Band Channels**		x			
SC-37 (1)	*OUT-OF-BAND CHANNELS | ENSURE DELIVERY / TRANSMISSION*		x			
SC-38	**Operations Security**		x			
SC-39	**Process Isolation**		x	x	x	x
SC-39 (1)	*PROCESS ISOLATION | HARDWARE SEPARATION*		x			
SC-39 (2)	*PROCESS ISOLATION | THREAD ISOLATION*		x			
SC-40	**Wireless Link Protection**					
SC-40 (1)	*WIRELESS LINK PROTECTION | ELECTROMAGNETIC INTERFERENCE*					
SC-40 (2)	*WIRELESS LINK PROTECTION | REDUCE DETECTION POTENTIAL*					
SC-40 (3)	*WIRELESS LINK PROTECTION | IMITATIVE OR MANIPULATIVE COMMUNICATIONS DECEPTION*					
SC-40 (4)	*WIRELESS LINK PROTECTION | SIGNAL PARAMETER IDENTIFICATION*					
SC-41	**Port and I/O Device Access**					
SC-42	**Sensor Capability and Data**					
SC-42 (1)	*SENSOR CAPABILITY AND DATA | REPORTING TO AUTHORIZED INDIVIDUALS OR ROLES*					
SC-42 (2)	*SENSOR CAPABILITY AND DATA | AUTHORIZED USE*					
SC-42 (3)	*SENSOR CAPABILITY AND DATA | PROHIBIT USE OF DEVICES*					
SC-43	**Usage Restrictions**					
SC-44	**Detonation Chambers**					

TABLE D-19: SUMMARY — SYSTEM AND INFORMATION INTEGRITY CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SI-1	**System and Information Integrity Policy and Procedures**		x	x	x	x
SI-2	**Flaw Remediation**			x	x	x
SI-2 (1)	*FLAW REMEDIATION | CENTRAL MANAGEMENT*					x
SI-2 (2)	*FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS*				x	x
SI-2 (3)	*FLAW REMEDIATION | TIME TO REMEDIATE FLAWS / BENCHMARKS FOR CORRECTIVE ACTIONS*					
SI-2 (4)	*FLAW REMEDIATION | AUTOMATED PATCH MANAGEMENT TOOLS*	x	Incorporated into SI-2.			
SI-2 (5)	*FLAW REMEDIATION | AUTOMATIC SOFTWARE / FIRMWARE UPDATES*					
SI-2 (6)	*FLAW REMEDIATION | REMOVAL OF PREVIOUS VERSIONS OF SOFTWARE / FIRMWARE*					
SI-3	**Malicious Code Protection**			x	x	x
SI-3 (1)	*MALICIOUS CODE PROTECTION | CENTRAL MANAGEMENT*				x	x
SI-3 (2)	*MALICIOUS CODE PROTECTION | AUTOMATIC UPDATES*				x	x
SI-3 (3)	*MALICIOUS CODE PROTECTION | NON-PRIVILEGED USERS*	x	Incorporated into AC-6 (10).			
SI-3 (4)	*MALICIOUS CODE PROTECTION | UPDATES ONLY BY PRIVILEGED USERS*					
SI-3 (5)	*MALICIOUS CODE PROTECTION | PORTABLE STORAGE DEVICES*	x	Incorporated into MP-7.			
SI-3 (6)	*MALICIOUS CODE PROTECTION | TESTING / VERIFICATION*					
SI-3 (7)	*MALICIOUS CODE PROTECTION | NONSIGNATURE-BASED DETECTION*					
SI-3 (8)	*MALICIOUS CODE PROTECTION | DETECT UNAUTHORIZED COMMANDS*					
SI-3 (9)	*MALICIOUS CODE PROTECTION | AUTHENTICATE REMOTE COMMANDS*					
SI-3 (10)	*MALICIOUS CODE PROTECTION | MALICIOUS CODE ANALYSIS*					
SI-4	**Information System Monitoring**		x	x	x	x
SI-4 (1)	*INFORMATION SYSTEM MONITORING | SYSTEM-WIDE INTRUSION DETECTION SYSTEM*		x			
SI-4 (2)	*INFORMATION SYSTEM MONITORING | AUTOMATED TOOLS FOR REAL-TIME ANALYSIS*		x		x	x
SI-4 (3)	*INFORMATION SYSTEM MONITORING | AUTOMATED TOOL INTEGRATION*		x			
SI-4 (4)	*INFORMATION SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC*		x		x	x
SI-4 (5)	*INFORMATION SYSTEM MONITORING | SYSTEM-GENERATED ALERTS*		x		x	x
SI-4 (6)	*INFORMATION SYSTEM MONITORING | RESTRICT NON-PRIVILEGED USERS*	x	Incorporated into AC-6 (10).			
SI-4 (7)	*INFORMATION SYSTEM MONITORING | AUTOMATED RESPONSE TO SUSPICIOUS EVENTS*		x			
SI-4 (8)	*INFORMATION SYSTEM MONITORING | PROTECTION OF MONITORING INFORMATION*	x	Incorporated into SI-4.			
SI-4 (9)	*INFORMATION SYSTEM MONITORING | TESTING OF MONITORING TOOLS*		x			
SI-4 (10)	*INFORMATION SYSTEM MONITORING | VISIBILITY OF ENCRYPTED COMMUNICATIONS*		x			
SI-4 (11)	*INFORMATION SYSTEM MONITORING | ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES*		x			
SI-4 (12)	*INFORMATION SYSTEM MONITORING | AUTOMATED ALERTS*		x			
SI-4 (13)	*INFORMATION SYSTEM MONITORING | ANALYZE TRAFFIC / EVENT PATTERNS*		x			
SI-4 (14)	*INFORMATION SYSTEM MONITORING | WIRELESS INTRUSION DETECTION*		x			

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SI-4 (15)	*INFORMATION SYSTEM MONITORING | WIRELESS TO WIRELINE COMMUNICATIONS*		X			
SI-4 (16)	*INFORMATION SYSTEM MONITORING | CORRELATE MONITORING INFORMATION*		X			
SI-4 (17)	*INFORMATION SYSTEM MONITORING | INTEGRATED SITUATIONAL AWARENESS*		X			
SI-4 (18)	*INFORMATION SYSTEM MONITORING | ANALYZE TRAFFIC / COVERT EXFILTRATION*		X			
SI-4 (19)	*INFORMATION SYSTEM MONITORING | INDIVIDUALS POSING GREATER RISK*		X			
SI-4 (20)	*INFORMATION SYSTEM MONITORING | PRIVILEGED USER*		X			
SI-4 (21)	*INFORMATION SYSTEM MONITORING | PROBATIONARY PERIODS*		X			
SI-4 (22)	*INFORMATION SYSTEM MONITORING | UNAUTHORIZED NETWORK SERVICES*		X			
SI-4 (23)	*INFORMATION SYSTEM MONITORING | HOST-BASED DEVICES*		X			
SI-4 (24)	*INFORMATION SYSTEM MONITORING | INDICATORS OF COMPROMISE*		X			
SI-5	**Security Alerts, Advisories, and Directives**		X	X	X	X
SI-5 (1)	*SECURITY ALERTS, ADVISORIES, AND DIRECTIVES | AUTOMATED ALERTS AND ADVISORIES*		X			X
SI-6	**Security Function Verification**		X			X
SI-6 (1)	*SECURITY FUNCTION VERIFICATION | NOTIFICATION OF FAILED SECURITY TESTS*	X	Incorporated into SI-6.			
SI-6 (2)	*SECURITY FUNCTION VERIFICATION | AUTOMATION SUPPORT FOR DISTRIBUTED TESTING*					
SI-6 (3)	*SECURITY FUNCTION VERIFICATION | REPORT VERIFICATION RESULTS*					
SI-7	**Software, Firmware, and Information Integrity**		X		X	X
SI-7 (1)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS*		X		X	X
SI-7 (2)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS*		X			X
SI-7 (3)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CENTRALLY MANAGED INTEGRITY TOOLS*		X			
SI-7 (4)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | TAMPER-EVIDENT PACKAGING*	X	Incorporated into SA-12.			
SI-7 (5)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS*		X			X
SI-7 (6)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CRYPTOGRAPHIC PROTECTION*		X			
SI-7 (7)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE*		X		X	X
SI-7 (8)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUDITING CAPABILITY FOR SIGNIFICANT EVENTS*		X			
SI-7 (9)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | VERIFY BOOT PROCESS*		X			
SI-7 (10)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | PROTECTION OF BOOT FIRMWARE*		X			
SI-7 (11)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES*		X			
SI-7 (12)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY VERIFICATION*		X			

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SI-7 (13)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE EXECUTION IN PROTECTED ENVIRONMENTS*		X			
SI-7 (14)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | BINARY OR MACHINE EXECUTABLE CODE*		X			X
SI-7 (15)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE AUTHENTICATION*		X			
SI-7 (16)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION*		X			
SI-8	**Spam Protection**				X	X
SI-8 (1)	*SPAM PROTECTION | CENTRAL MANAGEMENT*				X	X
SI-8 (2)	*SPAM PROTECTION | AUTOMATIC UPDATES*				X	X
SI-8 (3)	*SPAM PROTECTION | CONTINUOUS LEARNING CAPABILITY*					
SI-9	**Information Input Restrictions**	X	Incorporated into AC-2, AC-3, AC-5, AC-6.			
SI-10	**Information Input Validation**		X		X	X
SI-10 (1)	*INFORMATION INPUT VALIDATION | MANUAL OVERRIDE CAPABILITY*		X			
SI-10 (2)	*INFORMATION INPUT VALIDATION | REVIEW / RESOLUTION OF ERRORS*		X			
SI-10 (3)	*INFORMATION INPUT VALIDATION | PREDICTABLE BEHAVIOR*		X			
SI-10 (4)	*INFORMATION INPUT VALIDATION | REVIEW / TIMING INTERACTIONS*		X			
SI-10 (5)	*INFORMATION INPUT VALIDATION | REVIEW / RESTRICT INPUTS TO TRUSTED SOURCES AND APPROVED FORMATS*		X			
SI-11	**Error Handling**				X	X
SI-12	**Information Handling and Retention**			X	X	X
SI-13	**Predictable Failure Prevention**		X			
SI-13 (1)	*PREDICTABLE FAILURE PREVENTION | TRANSFERRING COMPONENT RESPONSIBILITIES*		X			
SI-13 (2)	*PREDICTABLE FAILURE PREVENTION | TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION*	X	Incorporated into SI-7 (16).			
SI-13 (3)	*PREDICTABLE FAILURE PREVENTION | MANUAL TRANSFER BETWEEN COMPONENTS*		X			
SI-13 (4)	*PREDICTABLE FAILURE PREVENTION | STANDBY COMPONENT INSTALLATION / NOTIFICATION*		X			
SI-13 (5)	*PREDICTABLE FAILURE PREVENTION | FAILOVER CAPABILITY*		X			
SI-14	**Non-Persistence**		X			
SI-14 (1)	*NON-PERSISTENCE | REFRESH FROM TRUSTED SOURCES*		X			
SI-15	**Information Output Filtering**		X			
SI-16	**Memory Protection**		X		X	X
SI-17	**Fail-Safe Procedures**		X			

ADJUSTMENTS TO SECURITY CONTROL BASELINES

ALLOCATION OF SECURITY CONTROLS AND ASSIGNMENT OF PRIORITY SEQUENCING CODES

With each revision to SP 800-53, minor adjustments may occur with the security control baselines including, for example, allocating additional controls and/or control enhancements, eliminating selected controls/enhancements, and changing sequencing priority codes (P-codes). These changes reflect: (i) the ongoing receipt and analysis of threat information; (ii) the periodic reexamination of the initial assumptions that generated the security control baselines; (iii) the desire for common security control baseline starting points for national security and non-national security systems to achieve community-wide convergence (relying subsequently on specific overlays to describe any adjustments from the common starting points); and (iv) the periodic reassessment of priority codes to appropriately balance the workload of security control implementation. Over time, as the security control catalog expands to address the continuing challenges from a dynamic and growing threat space that is increasingly sophisticated, organizations will come to rely to a much greater degree on overlays to provide the needed specialization for their security plans.

APPENDIX E

ASSURANCE AND TRUSTWORTHINESS

MEASURES OF CONFIDENCE FOR INFORMATION SYSTEMS

Security assurance is a critical aspect in determining the trustworthiness of information systems. Assurance is the measure of confidence that the security functions, features, practices, policies, procedures, mechanisms, and architecture of organizational information systems accurately mediate and enforce established security policies.[94] The objective of this appendix is:

- To encourage organizations to include assurance requirements in procurements of information systems, system components, and services;
- To encourage hardware, software, and firmware developers to employ development practices that result in more trustworthy information technology products and systems;
- To encourage organizations to identify, select, and use information technology products that have been built with appropriate levels of assurance and to employ sound systems and security engineering techniques and methods during the system development life cycle process;
- To reduce information security risk by deploying more trustworthy information technology products within critical information systems or system components; and
- To encourage developers and organizations to obtain on an ongoing basis, assurance evidence for maintaining trustworthiness of information systems.

Minimum security requirements for federal information and information systems are defined in FIPS Publication 200. These requirements can be satisfied by selecting, tailoring, implementing, and obtaining assurance evidence for the security controls in the low, moderate, or high baselines in Appendix D.[95] The baselines also include the assurance-related controls for the minimum assurance requirements that are generally applicable to federal information and information systems.[96] However, considering the current threat space and the increasing risk to organizational operations and assets, individuals, other organizations, and the Nation, posed by the advanced persistent threat (APT), organizations may choose to implement additional assurance-related controls from Appendix F. These additional controls can be selected based on the tailoring guidance provided in Section 3.2. Organizations can also consider developing high-assurance overlays for critical missions/business functions, specialized environments of operation, and/or information technologies (see Section 3.3 and Appendix I). When assurance-related controls cannot be satisfied, organizations can propose compensating controls (e.g., procedural/operational

[94] Section 2.6 provides an introduction to the concepts of assurance and trustworthiness and how the two concepts are related. A trustworthiness model is illustrated in Figure 3.

[95] CNSS Instruction 1253 provides security control baselines for national security systems. Therefore, the assurance-related controls in the baselines established for the national security community, if so designated, may differ from those controls designated in Tables E-1 through E-3.

[96] It is difficult to determine if a given security control baseline from Appendix D provides the assurance needed across all information technologies, users, platforms, and organizations. For example, while the use of formal methods might be appropriate in a cross-domain product, different assurance techniques might be appropriate for a complex air traffic control system or for a web server providing emergency preparedness information from the Department of Homeland Security. Still, the existing baselines do have assurance aspects that reflect the minimum assurance that is anticipated to be common across all technologies, users, platforms, and organizations.

solutions to compensate for insufficient technology-based solutions) or assume a greater degree of risk with regard to the actual security capability achieved.

The New Look for Assurance

While previous versions of Special Publication 800-53 addressed minimum assurance requirements, the focus was on higher-level, more abstract requirements applied to the low, moderate, and high baselines. This revision takes a fundamentally different approach to assurance by defining specific assurance-related security controls in Appendix F that can be implemented by organizations based on the security categorizations of their information systems—making the assurance requirements more *actionable* and providing opportunities for increasing the levels of assurance based on mission and business needs, current/projected threats, unique operating environments, or the use of new technologies. The identification of specific assurance-related controls in the low, moderate, and high baselines in easy-to read tables (Tables E-1, E-2, E-3) helps organizations to quickly define controls necessary to satisfy minimum assurance requirements. The optional assurance-related controls in Table E-4 provide organizations with specification language to use in acquisitions targeted at the developers of information systems, system components, and information system services. The controls address specific methodologies, techniques, design, and architectural considerations as well as sound system and security engineering principles to fundamentally improve the quality of hardware, software, and firmware components that will be integrated into organizational information systems or the critical infrastructure. The designation of assurance-related controls is not intended to imply a greater level of importance for such controls. Achieving adequate security for organizational information systems requires the correct combination of both functionality- and assurance-related security controls. Only by understanding the importance of the concept of assurance and recognizing which security controls are more assurance-oriented versus functionality-oriented can organizations select the most appropriate combination of controls to protect their organizational operations and assets, individuals, other organizations, and the Nation.

The following sections provide a description of the assurance-related controls that are included in each of the security control baselines in Appendix D. The criteria for whether a security control is assurance-related or functionality-related is based on the overall characteristics of the control. In general, assurance-related controls are controls that: (i) define processes, procedures, techniques, or methodologies for designing and developing information systems and system components (i.e., hardware, software, firmware); (ii) provide supporting operational processes including improving the quality of systems/components/processes; (iii) produce security evidence from developmental or operational activities; (iv) determine security control effectiveness or risk (e.g., audit, testing, evaluation, analysis, assessment, verification, validation, monitoring); or (v) improve personnel skills, expertise, and understanding (e.g., security awareness/training, incident response training, contingency training).

Security controls may be designated as assurance-related controls even when the controls exhibit some functional characteristics or properties (e.g., SI-4, Information System Monitoring). The distinction between functionality and assurance is less important when describing the assurance-related controls in the baselines—primarily because the security controls in the three baselines after the tailoring process is applied, become part of the security plans for information systems and for organizations.[97] However, the distinction becomes more important when organizations exercise the option of selecting additional security controls to increase the level of assurance (or the degree of confidence) in the security functionality and security capability.

[97] Organizations are cautioned to carefully examine the assurance-related controls in the baselines during the tailoring process, including the development of overlays, to help ensure that controls are not being inadvertently eliminated that provide the measures of confidence in the security functionality needed for mission/business protection.

Minimum Assurance Requirements – Low-Impact Systems

Assurance Requirement: The organization, based on its security requirements, security policies, and needed security capabilities, has an expectation of: (i) a **limited** strength of security functionality; and (ii) a **limited** degree of confidence supported by the depth and coverage of associated security evidence, that the security functionality is complete, consistent, and correct.

Supplemental Guidance: Security functionality and assurance for low-impact systems are achieved by the implementation of security controls from the tailored low baseline in Appendix D. Assurance requirements for low-impact systems (including the information technology components that are part of those systems), align with that which is readily achievable with unmodified, commercial off-the-shelf (COTS) products and services. Due to the limited strength of functionality expected for low-impact systems, the depth/coverage of security evidence[98] produced is minimal and is not expected to be more than what is routinely provided by COTS manufacturers, vendors, and resellers. The depth/coverage evidence is further supplemented by the results of security control assessments and the ongoing monitoring of organizational information systems and environments in which the systems operate. For other than technology-based functionality, the emphasis is on a limited degree of confidence in the completeness, correctness, and consistency of procedural and/or operational security functionality (e.g., policies, procedures, physical security, and personnel security). Assurance requirements specified in the form of developmental and operational assurance controls for low-impact systems are listed in Table E-1. Organizations, through the tailoring process (including an organizational assessment of risk), may choose to add other assurance-related controls and/or control enhancements to the set included in Table E-1.

TABLE E-1: ASSURANCE-RELATED CONTROLS FOR LOW-IMPACT SYSTEMS[99]

ID	CONTROLS	ID	CONTROLS
AC	AC-1	MP	MP-1
AT	AT-1, AT-2, AT-3, AT-4	PE	PE-1, PE-6, PE-8
AU	AU-1, AU-6	PL	PL-1, PL-2, PL-4
CA	CA-1, CA-2, CA-3, CA-5, CA-6, CA-7, CA-9	PS	PS-1, PS-6, PS-7
CM	CM-1, CM-2, CM-4, CM-8	RA	RA-1, RA-3, RA-5
CP	CP-1, CP-3, CP-4	SA	SA-1, SA-2, SA-3, SA-4, SA-4 (10), SA-5, SA-9
IA	IA-1	SC	SC-1, SC-39
IR	IR-1, IR-2, IR-5	SI	SI-1, SI-4, SI-5
MA	MA-1		

[98] NIST Special Publication 800-53A provides additional information on depth and coverage in security control assessments.

[99] The assurance-related controls in Table E-1 are a *subset* of the security controls contained in the security control baseline for low-impact systems in Appendix D. Implementing the assurance-related controls in Table E-1 (including depth/coverage security evidence from NIST Special Publication 800-53A) will satisfy the minimum assurance requirements for low-impact systems mandated by FIPS Publication 200.

Minimum Assurance Requirements – Moderate-Impact Systems

Assurance Requirement: The organization, based on its security requirements, security policies, and needed security capabilities, has an expectation of: (i) a **moderate** strength of security functionality; and (ii) a **moderate** degree of confidence supported by the depth and coverage of associated security evidence, that the security functionality is complete, consistent, and correct.

Supplemental Guidance: Security functionality and assurance for moderate-impact systems are achieved by the implementation of security controls from the tailored moderate baseline in Appendix D. Assurance requirements for moderate-impact systems (including the information technology components that are part of those systems) add to the expectations at the low-assurance level by: (i) incorporating COTS security functionality with greater strength of mechanism and capability than the strength of mechanism and capability achieved in low-impact systems; (ii) requiring perhaps, some special development; (iii) establishing more secure configuration settings; and (iv) requiring some additional assessment of the implemented capability. Due to the moderate strength of functionality expected for moderate-impact systems, the depth/coverage of security evidence[100] produced is more substantial than the minimal evidence produced for low-impact systems but still in the range of what can be provided by COTS manufacturers, vendors, and resellers. The depth/coverage evidence is further supplemented by the results of additional security control assessments and the ongoing monitoring of organizational information systems and environments of operation. For other than technology-based functionality, the emphasis is on a moderate degree of confidence in the completeness, correctness, and consistency of procedural and/or operational security functionality (e.g., policies, procedures, physical security, and personnel security). Assurance requirements in the form of developmental and operational assurance controls for moderate-impact systems are listed in Table E-2. Organizations, through the tailoring process (including an organizational assessment of risk), may choose to add other assurance-related controls and/or control enhancements to the set included in Table E-2.

TABLE E-2: ASSURANCE-RELATED CONTROLS FOR MODERATE-IMPACT SYSTEMS[101]

ID	CONTROLS	ID	CONTROLS
AC	AC-1	MP	MP-1
AT	AT-1, AT-2, **AT-2 (2)**, AT-3, AT-4	PE	PE-1, PE-6, **PE-6 (1)**, PE-8
AU	AU-1, AU-6, **AU-6 (1)**, **AU-6 (3)**, AU-7, **AU-7 (1)**	PL	PL-1, PL-2, **PL-2 (3)**, PL-4, **PL-4 (1)**, PL-8
CA	CA-1, CA-2, **CA-2 (1)**, CA-3, CA-5, CA-6, CA-7, **CA-7 (1)**, CA-9	PS	PS-1, PS-6, PS-7
CM	CM-1, CM-2, **CM-2 (1)**, **CM-2 (3)**, **CM-2 (7)**, CM-3, **CM-3 (2)**, CM-4, CM-8, **CM-8 (1)**, **CM-8 (3)**, **CM-8 (5)**	RA	RA-1, RA-3, RA-5, **RA-5 (1)**, **RA-5 (2)**, **RA-5 (5)**
CP	CP-1, CP-3, CP-4, **CP-4 (1)**	SA	SA-1, SA-2, SA-3, SA-4, **SA-4 (1)**, **SA-4 (2)**, **SA-4 (9)**, **SA-4 (10)**, SA-5, SA-8, SA-9, **SA-9 (2)**, SA-10, SA-11
IA	IA-1	SC	SC-1, SC-2, SC-39
IR	IR-1, IR-2, IR-3, **IR-3 (2)**, IR-5	SI	SI-1, SI-4, **SI-4 (2)**, **SI-4 (4)**, **SI-4 (5)**, SI-5, SI-7, **SI-7 (1)**, **SI-7 (7)**, SI-10, SI-16
MA	MA-1		

[100] NIST Special Publication 800-53A provides additional information on depth and coverage in security control assessments.

[101] The assurance-related controls in Table E-2 are a *subset* of the security controls contained in the security control baseline for moderate-impact systems in Appendix D. Implementing the assurance-related controls in Table E-2 (including depth/coverage security evidence from NIST Special Publication 800-53A) will satisfy the minimum assurance requirements for moderate-impact systems mandated by FIPS Publication 200. The **bold** text indicates the *delta* from the low baseline (i.e., the assurance-related controls added to the low baseline to produce the increased level of assurance in the moderate baseline).

Minimum Assurance Requirements – High-Impact Systems

Assurance Requirement: The organization, based on its security requirements, security policies, and needed security capabilities, has an expectation of: (i) a **high** strength of security functionality; and (ii) a **high** degree of confidence supported by the depth and coverage of associated security evidence, that the security functionality is complete, consistent, and correct.

Supplemental Guidance: Security functionality and assurance for high-impact systems are achieved by the implementation of security controls from the tailored high baseline in Appendix D. Assurance requirements for high-impact systems (including the information technology components that are part of those systems), add to the expectations at the moderate assurance level by: (i) incorporating higher-end COTS security capabilities that result from the application of commonly accepted best commercial development practices for reducing latent flaw rates, some special development, and additional assessment of the implemented capability. Due to the high strength of functionality expected for high-impact systems, the depth/coverage of security evidence[102] produced is more comprehensive than the evidence produced for moderate-impact systems. Although the evidence may still be in the range of what can be provided by COTS manufacturers, vendors, and resellers, greater assurance from independent assessment providers may be required. The depth/coverage evidence is supplemented by the results of additional security control assessments and the ongoing monitoring of organizational information systems/environments of operation. For other than technology-based functionality, there is a high degree of confidence in the completeness, correctness, and consistency of procedural and/or operational security functionality (e.g., policies, procedures, physical security, and personnel security). Assurance requirements in the form of developmental and operational assurance controls for high-impact information systems are listed in Table E-3. Organizations, through the tailoring process (including an organizational assessment of risk), may choose to add other assurance-related controls and/or control enhancements to the set included in Table E-3.

TABLE E-3: ASSURANCE-RELATED CONTROLS FOR HIGH-IMPACT SYSTEMS[103]

ID	CONTROLS	ID	CONTROLS
AC	AC-1	MP	MP-1
AT	AT-1, AT-2, AT-2 (2), AT-3, AT-4	PE	PE-1, PE-6, PE-6 (1), **PE-6 (4)**, PE-8
AU	AU-1, AU-6, AU-6 (1), AU-6 (3), **AU-6 (5)**, **AU-6 (6)**, AU-7, AU-7 (1), **AU-10**	PL	PL-1, PL-2, PL-2 (3), PL-4, PL-4 (1), PL-8
CA	CA-1, CA-2, CA-2 (1), **CA-2 (2)**, CA-3, CA-5, CA-6, CA-7, CA-7 (1), **CA-8**, CA-9	PS	PS-1, PS-6, PS-7
CM	CM-1, CM-2, CM-2 (1), **CM-2 (2)**, CM-2 (3), CM-2 (7), CM-3, **CM-3 (1)**, CM-3 (2), CM-4, **CM-4 (1)**, CM-8, CM-8 (1), **CM-8 (2)**, CM-8 (3), **CM-8 (4)**, CM-8 (5)	RA	RA-1, RA-3, RA-5, RA-5 (1), RA-5 (2), **RA-5 (4)**, RA-5 (5)
CP	CP-1, CP-3, **CP-3 (1)**, CP-4, CP-4 (1), **CP-4 (2)**	SA	SA-1, SA-2, SA-3, SA-4, SA-4 (1), SA-4 (2), SA-4 (9), SA-4 (10), SA-5, SA-8, SA-9, SA-9 (2), SA-10, SA-11, **SA-12**, **SA-15**, **SA-16**, **SA-17**
IA	IA-1	SC	SC-1, SC-2, **SC-3**, **SC-7 (18)**, **SC-7 (21)**, **SC-24**, SC-39
IR	IR-1, IR-2, IR-2 **(1)**, IR-2 **(2)**, IR-3, IR-3 (2), IR-5, IR-5 **(1)**	SI	SI-1, SI-4, SI-4 (2), SI-4 (4), SI-4 (5), SI-5, SI-5 **(1)**, SI-6, SI-7, SI-7 (1), SI-7 **(2)**, SI-7 **(5)**, SI-7 (7), SI-7 **(14)**, SI-10, SI-16
MA	MA-1		

[102] NIST Special Publication 800-53A provides additional information on depth and coverage in security control assessments.

[103] The assurance-related controls in Table E-3 are a *subset* of the security controls contained in the security control baseline for high-impact systems in Appendix D. Implementing the assurance-related controls in Table E-3 (including depth/coverage security evidence from NIST Special Publication 800-53A) will satisfy the minimum assurance requirements for high-impact systems mandated by FIPS Publication 200. The **bold** text indicates the *delta* from the moderate baseline (i.e., the assurance-related controls added to the moderate baseline to produce the increased level of assurance in the high baseline).

Security Controls to Achieve Enhanced Assurance

While the assurance-related controls allocated to the low, moderate, and high baselines in the previous sections, represent minimum assurance requirements, organizations can, over time, choose to raise the level of assurance in their information systems—increasing the level of trustworthiness accordingly. This is accomplished by adding assurance-related controls to the controls in the baselines to increase both the strength of security functionality and degree of confidence that the functionality is correct, complete, and consistent—making the functionality highly resistant to penetration, tamper, or bypass. Security functionality that is highly resistant to penetration, tamper, and bypass requires a significant work factor on the part of adversaries to compromise the confidentiality, integrity, or availability of the information system or system components where that functionality is employed.

Since high-assurance information technology products may be more costly and difficult to obtain, organizations may choose to partition their information systems into distinct subsystems to isolate the critical components and focus the high-assurance efforts on a more narrowly defined subset of information resources. Organizations that find it difficult to achieve high-assurance information technology solutions may have to rely to a greater extent on procedural or operational protections to ensure mission and business success. This includes, for example, reengineering critical mission and business processes to be less susceptible to high-end threats. Table E-4 provides additional developmental and operational activities (e.g., in the SA, SI, and CM security control families), that organizations can select to achieve an enhanced level of assurance (up to and including high assurance). The list of assurance-related controls is not intended to be exhaustive. Organizations, during the tailoring process, may choose to designate other security controls as assurance-related and add to the exemplar set in Table E-4.

TABLE E-4: SECURITY CONTROLS FOR ENHANCED ASSURANCE[104]

ID	CONTROLS	ID	CONTROLS
AC	AC-25	MP	No additional controls.
AT	AT-2 (1), AT-3 (all enhancements)	PE	PE-6 (2), PE-6 (3)
AU	AU-6 (4), AU-6 (7), AU-6 (8), AU-6 (9), AU-6 (10), AU-10 (all enhancements), AU-11 (1), AU-13 (plus enhancements), AU-14 (plus enhancements)	PL	PL-8 (all enhancements), PL-9
CA	CA-2 (3), CA-5 (1), CA-7 (3), CA-8 (all enhancements), CA-9 (1)	PS	PS-6 (2), PS-6 (3)
CM	CM-2 (6), CM-4 (2), CM-8 (6), CM-8 (7), CM-8 (8), CM-8 (9)	RA	RA-5 (3), RA-5 (6), RA-5 (8), RA-5 (10), RA-6
CP	CP-3 (2), CP-4 (3), CP-4 (4), CP-12	SA	SA-4 (3), SA-4 (5), SA-4 (6), SA-4 (7), SA-4 (8), SA-9 (1), SA-9 (3), SA-9 (4), SA-9 (5), SA-10 (all enhancements), SA-11 (all enhancements), SA-12 (all enhancements), SA-13, SA-14, SA-15 (all enhancements), SA-17 (all enhancements), SA-18 (plus enhancements), SA-19 (plus enhancements), SA-20, SA-21 (plus enhancement), SA-22 (plus enhancement)
IA	No additional controls.	SC	SC-2 (1), SC-3 (all enhancements), SC-6, SC-7 (22), SC-11 (plus enhancement), SC-29 (plus enhancement), SC-30 (plus enhancements), SC-31 (plus enhancements), SC-32, SC-34 (plus enhancements), SC-36 (plus enhancement), SC-37 (plus enhancement), SC-38, SC-39 (all enhancements)
IR	IR-3 (1)	SI	SI-4 (1), SI-4 (3), SI-4 (7), SI-4 (9), SI-4 (10), SI-4 (11), SI-4 (12), SI-4 (13), SI-4 (14), SI-4 (15), SI-4 (16), SI-4 (17), SI-4 (18), SI-4 (19), SI-4 (20), SI-4 (21), SI-4 (22), SI-4 (23), SI-4 (24), SI-7 (3), SI-7 (6), SI-7 (8), SI-7 (9), SI-7 (10), SI-7 (11), SI-7 (12), SI-7 (13), SI-7 (15), SI-7 (16), SI-10 (all enhancements), SI-13 (plus enhancements), SI-14 (plus enhancement), SI-15, SI-17
MA	No additional controls.		

[104] The assurance-related controls in Table E-4 represent the additional security controls needed to achieve enhanced levels of assurance (i.e., the controls needed to go beyond the minimum assurance levels that are represented by the assurance-related controls in Tables E-1, E-2, and E-3). When an assurance-related control is allocated to a baseline (i.e., listed in Tables E-1, E-2, or E-3), but all of its control enhancements are in Table E-4, it is designated in the table as **Control** (*all enhancements*). When an assurance-related control and all of its control enhancements are not allocated to baselines, it is designated in the table as **Control** (*plus enhancements*). When assurance-related control enhancements from a particular control are allocated to one of the baselines, the remaining unselected control enhancements are listed individually in Table E-4.

APPENDIX F

SECURITY CONTROL CATALOG

SECURITY CONTROLS, ENHANCEMENTS, AND SUPPLEMENTAL GUIDANCE

The catalog of security controls in this appendix provides a range of safeguards and countermeasures for organizations and information systems.[105] The security controls have been designed to facilitate compliance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.[106] The organization of the security control catalog, the structure of the security controls, and the concept of allocating security controls and control enhancements to the initial baselines in Appendix D are described in Chapter Two. The security controls in the catalog with few exceptions, have been designed to be policy- and technology-neutral. This means that security controls and control enhancements focus on the fundamental safeguards and countermeasures necessary to protect information during processing, while in storage, and during transmission. Therefore, it is beyond the scope of this publication to provide guidance on the application of security controls to specific technologies, communities of interest, environments of operation, or missions/business functions. These areas are addressed by the use of the tailoring process described in Chapter Three and the development of overlays described in Appendix I.

In the few cases where specific technologies are called out in security controls (e.g., mobile, PKI, wireless, VOIP), organizations are cautioned that the need to provide adequate security goes well beyond the requirements in a single control associated with a particular technology. Many of the needed safeguards/countermeasures are obtained from the other security controls in the catalog allocated to the initial control baselines as the starting point for the development of security plans and overlays using the tailoring process. In addition to the organization-driven development of specialized security plans and overlays, NIST Special Publications and Interagency Reports may provide guidance on recommended security controls for specific technologies and sector-specific applications (e.g., Smart Grid, healthcare, Industrial Control Systems, and mobile).

Employing a policy- and technology-neutral security control catalog has the following benefits:

- It encourages organizations to focus on the *security capabilities* required for mission/business success and the protection of information, irrespective of the information technologies that are employed in organizational information systems;
- It encourages organizations to analyze each security control for its applicability to specific technologies, environments of operation, missions/business functions, and communities of interest; and

[105] An online version of the catalog of security controls is also available at http://web.nvd.nist.gov/view/800-53/home.

[106] Compliance necessitates organizations executing *due diligence* with regard to information security and risk management. Information security due diligence includes using all appropriate information as part of an organization-wide risk management program to effectively use the tailoring guidance and inherent flexibility in NIST publications so that the selected security controls documented in organizational security plans meet the specific mission and business requirements of organizations. Using the risk management tools and techniques that are available to organizations is essential in developing, implementing, and maintaining the safeguards and countermeasures with the necessary and sufficient strength of mechanism to address the current threats to organizational operations and assets, individuals, other organizations, and the Nation. Employing effective risk-based processes, procedures, and technologies will help ensure that all federal information systems and organizations have the necessary resilience to support ongoing federal responsibilities, critical infrastructure applications, and continuity of government.

- It encourages organizations to specify security policies as part of the tailoring process for security controls that have variable parameters.

For example, organizations using smart phones, tablets, or other types of mobile devices would start the tailoring process by assuming that *all* security controls and control enhancements in the appropriate baseline (low, moderate, or high) are needed. The tailoring process may result in certain security controls being eliminated for a variety of reasons, including, for example, the inability of the technology to support the implementation of the control. However, the elimination of such controls without understanding the potential adverse impacts to organizational missions and business functions can significantly increase information security risk and should be carefully analyzed. This type of analysis is essential in order for organizations to make effective risk-based decisions including the selection of appropriate compensating security controls, when considering the use of these emerging mobile devices and technologies. The specialization of security plans using the tailoring guidance and overlays, together with a comprehensive set of technology- and policy-neutral security controls, promotes cost-effective, risk-based information security for organizations—in any sector, for any technology, and in any operating environment.

The security controls in the catalog are expected to change over time, as controls are withdrawn, revised, and added. In order to maintain stability in security plans and automated tools supporting the implementation of Special Publication 800-53, security controls will not be renumbered each time a control is withdrawn. Rather, notations of security controls that have been withdrawn are maintained in the catalog for historical purposes. Security controls are withdrawn for a variety of reasons including, for example: the security capability provided by the withdrawn control has been incorporated into another control; the security capability provided by the withdrawn control is redundant to an existing control; or the security control is deemed to be no longer necessary.

There may, on occasion, be repetition in requirements that appear in the security controls and control enhancements that are part of the security control catalog. This repetition in requirements is intended to reinforce the security requirements from the perspective of multiple controls and/or enhancements. For example, the requirement for strong identification and authentication when conducting remote maintenance activities appears in the MA family in the specific context of systems maintenance activities conducted by organizations. The identification and authentication requirement also appears in a more general context in the IA family. While these requirements appear to be redundant (i.e., overlapping), they are, in fact, mutually reinforcing and not intended to require additional effort on the part of organizations in the development and implementation of security programs.

Implementation Tip

New security controls and control enhancements will be developed on a regular basis using state-of-the-practice information from national-level threat and vulnerability databases as well as information on the tactics, techniques, and procedures employed by adversaries in launching cyber attacks. The proposed modifications to security controls and security control baselines will be carefully weighed during each revision cycle, considering the desire for stability of the security control catalog and the need to respond to changing threats, vulnerabilities, attack methods, and information technologies. The overall objective is to raise the basic level of information security over time. Organizations may choose to develop new security controls when there is a specific security capability required and the appropriate controls are not available in Appendices F or G.

SECURITY CONTROL CLASS DESIGNATIONS

MANAGEMENT, OPERATIONAL, AND TECHNICAL REFERENCES

Because many security controls within the security control families in Appendix F have various combinations of *management*, *operational*, and *technical* properties, the specific class designations have been removed from the security control families. Organizations may still find it useful to apply such designations to individual security controls and control enhancements or to individual sections within a particular control/enhancement. Organizations may find it beneficial to employ class designations as a way to group or refer to security controls. The class designations may also help organizations with the process of allocating security controls and control enhancements to: (i) responsible parties or information systems (e.g., as common or hybrid controls); (ii) specific roles; and/or (iii) specific components of a system. For example, organizations may determine that the responsibility for system-specific controls they have placed in the management class belong to the information system owner, controls placed in the operational class belong to the Information System Security Officer (ISSO), and controls placed in the technical class belong to one or more system administrators. This example is provided to illustrate the potential usefulness of designating classes for controls and/or control enhancements; it is not meant to suggest or require additional tasks for organizations.

CAUTIONARY NOTE

DEVELOPMENT OF SYSTEMS, COMPONENTS, AND SERVICES

With the renewed emphasis on trustworthy information systems and supply chain security, it is essential that organizations have the capability to express their information security requirements with clarity and specificity in order to engage the information technology industry and obtain the systems, components, and services necessary for mission and business success. To ensure that organizations have such capability, Special Publication 800-53 provides a set of security controls in the System and Services Acquisition family (i.e., SA family) addressing requirements for the development of information systems, information technology products, and information system services. Therefore, many of the controls in the SA family are directed at developers of those systems, components, and services. It is important for organizations to recognize that the scope of the security controls in the SA family includes all system/component/service development and the developers associated with such development whether the development is conducted by internal organizational personnel or by external developers through the contracting/acquisition process. Affected controls include SA-8, SA-10, SA-11, SA-15, SA-16, SA-17, SA-20, and SA-21.

Fundamentals of the Catalog

Security controls and control enhancements in Appendices F and G are generally designed to be policy-neutral and technology/implementation-independent. Organizations provide information about security controls and control enhancements in two ways:

- By specifying security control implementation details (e.g., platform dependencies) in the associated security plan for the information system or security program plan for the organization; and
- By establishing specific values in the variable sections of selected security controls through the use of *assignment* and *selection* statements.

Assignment and selection statements provide organizations with the capability to specialize security controls and control enhancements based on organizational security requirements or requirements originating in federal laws, Executive Orders, directives, policies, regulations, standards, or guidelines. Organization-defined parameters used in assignment and selection statements in the basic security controls apply also to all control enhancements associated with those controls. Control enhancements strengthen the fundamental security capability in the base control but are not a substitute for using assignment or selection statements to provide greater specificity to the control. Assignment statements for security controls and control enhancements do not contain minimum or maximum values (e.g., testing contingency plans *at least annually*). Organizations should consult specific federal laws, Executive Orders, directives, regulations, policies, standards, or guidelines as the definitive sources for such information. The absence of minimum and maximum values from the security controls and control enhancements does not obviate the need for organizations to comply with requirements in the controlling source publications.

The first security control in each family (i.e., the dash-1 control) generates requirements for specific policies and procedures that are needed for the effective implementation of the other security controls in the family. Therefore, individual controls and control enhancements in a particular family do not call for the development of such policies and procedures. Supplemental guidance sections of security controls and control enhancements do not contain any requirements or references to FIPS or NIST Special Publications. NIST publications are, however, included in a *references* section for each security control.

In support of the Joint Task Force initiative to develop a unified information security framework for the federal government, security controls and control enhancements for national security systems are included in this appendix. The inclusion of such controls and enhancements is not intended to impose security requirements on organizations that operate national security systems. Rather, organizations can use the security controls and control enhancements on a voluntary basis with the approval of federal officials exercising policy authority over national security systems. In addition, the security control priorities and security control baselines listed in Appendix D and in the priority and baseline allocation summary boxes below each security control in Appendix F, apply to non-national security systems *only* unless otherwise directed by the federal officials with national security policy authority.

Using the Catalog

Organizations employ security controls[107] in federal information systems and the environments in which those systems operate in accordance with FIPS Publication 199, FIPS Publication 200, and NIST Special Publications 800-37 and 800-39. Security categorization of federal information and information systems, as required by FIPS Publication 199, is the first step in the RMF.[108] Next, organizations select the appropriate security control baselines for their information systems by satisfying the minimum security requirements set forth in FIPS Publication 200. Appendix D includes three security control baselines that are associated with the designated impact levels of information systems as determined during the security categorization process.[109] After baseline selection, organizations tailor the baselines by: (i) identifying/designating common controls; (ii) applying scoping considerations; (iii) selecting compensating controls, if needed; (iv) assigning control parameter values in selection and assignment statements; (v) supplementing the baseline controls with additional controls and control enhancements from the security control catalog; and (vi) providing additional information for control implementation. Organizations can also use the baseline tailoring process with the overlay concept that is described in Section 3.2 and Appendix I. Risk assessments, as described in NIST Special Publication 800-30, guide and inform the security control selection process.[110]

CAUTIONARY NOTE

USE OF CRYPTOGRAPHY

If cryptography is required for the protection of information based on the selection of security controls in Appendix F and subsequently implemented by organizational information systems, the cryptographic mechanisms comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. This includes, for NSA-approved cryptography to protect classified information, FIPS-validated cryptography to protect unclassified information, and NSA-approved and FIPS-compliant key management technologies and processes. Security controls SC-12 and SC-13 provide specific information on the selection of appropriate cryptographic mechanisms, including the strength of such mechanisms.

[107] The security controls in Special Publication 800-53 are available online and can be downloaded in various formats from the NIST web site at: http://web.nvd.nist.gov/view/800-53/home.

[108] CNSS Instruction 1253 provides guidance for *security categorization* of national security systems.

[109] CNSS Instruction 1253 provides guidance on *security control baselines* for national security systems and specific tailoring requirements associated with such systems.

[110] There are additional security controls and control enhancements that appear in the catalog that are not used in any of the initial baselines. These additional controls and control enhancements are available to organizations and can be used in the tailoring process to achieve the needed level of protection in accordance with organizational risk assessments.

FAMILY: ACCESS CONTROL

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

   1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the access control policy and associated access controls; and

b. Reviews and updates the current:

   1. Access control policy [*Assignment: organization-defined frequency*]; and

   2. Access control procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** AC-1	**MOD** AC-1	**HIGH** AC-1

AC-2 ACCOUNT MANAGEMENT

Control: The organization:

a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [*Assignment: organization-defined information system account types*];

b. Assigns account managers for information system accounts;

c. Establishes conditions for group and role membership;

d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;

e. Requires approvals by [*Assignment: organization-defined personnel or roles*] for requests to create information system accounts;

f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [*Assignment: organization-defined procedures or conditions*];

g. Monitors the use of information system accounts;

h. Notifies account managers:

1. When accounts are no longer required;

2. When users are terminated or transferred; and

3. When individual information system usage or need-to-know changes;

i. Authorizes access to the information system based on:

1. A valid access authorization;

2. Intended system usage; and

3. Other attributes as required by the organization or associated missions/business functions;

j. Reviews accounts for compliance with account management requirements [*Assignment: organization-defined frequency*]; and

k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

Supplemental Guidance: Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information systems. The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability. Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local logon accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example: (i) when shared/group, emergency, or temporary accounts are no longer required; or (ii) when individuals are transferred or terminated. Some types of information system accounts may require specialized training. Related controls: AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-2, IA-4, IA-5, IA-8, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PL-4, SC-13.

Control Enhancements:

(1) *ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT*

The organization employs automated mechanisms to support the management of information system accounts.

Supplemental Guidance: The use of automated mechanisms can include, for example: using email or text messaging to automatically notify account managers when users are terminated or transferred; using the information system to monitor account usage; and using telephonic notification to report atypical system account usage.

(2) *ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS*

The information system automatically [*Selection: removes; disables*] temporary and emergency accounts after [*Assignment: organization-defined time period for each type of account*].

Supplemental Guidance: This control enhancement requires the removal of both temporary and emergency accounts automatically after a predefined period of time has elapsed, rather than at the convenience of the systems administrator.

(3) *ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS*

The information system automatically disables inactive accounts after [*Assignment: organization-defined time period*].

(4) *ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS*

The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: Related controls: AU-2, AU-12.

(5) *ACCOUNT MANAGEMENT | INACTIVITY LOGOUT*

The organization requires that users log out when [*Assignment: organization-defined time-period of expected inactivity or description of when to log out*].

Supplemental Guidance: Related control: SC-23.

(6) *ACCOUNT MANAGEMENT | DYNAMIC PRIVILEGE MANAGEMENT*

The information system implements the following dynamic privilege management capabilities: [*Assignment: organization-defined list of dynamic privilege management capabilities*].

Supplemental Guidance: In contrast to conventional access control approaches which employ static information system accounts and predefined sets of user privileges, dynamic access control approaches (e.g., service-oriented architectures) rely on run time access control decisions facilitated by dynamic privilege management. While user identities may remain relatively constant over time, user privileges may change more frequently based on ongoing mission/business requirements and operational needs of organizations. Dynamic privilege management can include, for example, the immediate revocation of privileges from users, as opposed to requiring that users terminate and restart their sessions to reflect any changes in privileges. Dynamic privilege management can also refer to mechanisms that change the privileges of users based on dynamic rules as opposed to editing specific user profiles. This type of privilege management includes, for example, automatic adjustments of privileges if users are operating out of their normal work times, or if information systems are under duress or in emergency maintenance situations. This control enhancement also includes the ancillary effects of privilege changes, for example, the potential changes to encryption keys used for communications. Dynamic privilege management can support requirements for information system resiliency. Related control: AC-16.

(7) *ACCOUNT MANAGEMENT | ROLE-BASED SCHEMES*

The organization:

(a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles;

(b) Monitors privileged role assignments; and

(c) Takes [*Assignment: organization-defined actions*] when privileged role assignments are no longer appropriate.

Supplemental Guidance: Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, key management, account management, network and system administration, database administration, and web administration.

(8) *ACCOUNT MANAGEMENT | DYNAMIC ACCOUNT CREATION*

The information system creates [*Assignment: organization-defined information system accounts*] dynamically.

Supplemental Guidance: Dynamic approaches for creating information system accounts (e.g., as implemented within service-oriented architectures) rely on establishing accounts (identities) at

run time for entities that were previously unknown. Organizations plan for dynamic creation of information system accounts by establishing trust relationships and mechanisms with the appropriate authorities to validate related authorizations and privileges. Related control: AC-16.

(9) *ACCOUNT MANAGEMENT | RESTRICTIONS ON USE OF SHARED GROUPS / ACCOUNTS*

The organization only permits the use of shared/group accounts that meet [*Assignment: organization-defined conditions for establishing shared/group accounts*].

(10) *ACCOUNT MANAGEMENT | SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION*

The information system terminates shared/group account credentials when members leave the group.

(11) *ACCOUNT MANAGEMENT | USAGE CONDITIONS*

The information system enforces [*Assignment: organization-defined circumstances and/or usage conditions*] for [*Assignment: organization-defined information system accounts*].

Supplemental Guidance: Organizations can describe the specific conditions or circumstances under which information system accounts can be used, for example, by restricting usage to certain days of the week, time of day, or specific durations of time.

(12) *ACCOUNT MANAGEMENT | ACCOUNT MONITORING / ATYPICAL USAGE*

The organization:

(a) Monitors information system accounts for [*Assignment: organization-defined atypical use*]; and

(b) Reports atypical usage of information system accounts to [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: Atypical usage includes, for example, accessing information systems at certain times of the day and from locations that are not consistent with the normal usage patterns of individuals working in organizations. Related control: CA-7.

(13) *ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS*

The organization disables accounts of users posing a significant risk within [*Assignment: organization-defined time period*] of discovery of the risk.

Supplemental Guidance: Users posing a significant risk to organizations include individuals for whom reliable evidence or intelligence indicates either the intention to use authorized access to information systems to cause harm or through whom adversaries will cause harm. Harm includes potential adverse impacts to organizational operations and assets, individuals, other organizations, or the Nation. Close coordination between authorizing officials, information system administrators, and human resource managers is essential in order for timely execution of this control enhancement. Related control: PS-4.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AC-2	**MOD** AC-2 (1) (2) (3) (4)	**HIGH** AC-2 (1) (2) (3) (4) (5) (11) (12) (13)

AC-3 ACCESS ENFORCEMENT

Control: The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Supplemental Guidance: Access control policies (e.g., identity-based policies, role-based policies, control matrices, cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, domains) in information systems. In addition to enforcing authorized access at the information system level and recognizing that information systems can host many applications and services in support of organizational missions and business operations, access enforcement mechanisms can also be employed at the application and service level to provide increased information security.

Related controls: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PE-3.

Control Enhancements:

(1) *ACCESS ENFORCEMENT | RESTRICTED ACCESS TO PRIVILEGED FUNCTIONS*

[Withdrawn: Incorporated into AC-6].

(2) *ACCESS ENFORCEMENT | DUAL AUTHORIZATION*

The information system enforces dual authorization for [*Assignment: organization-defined privileged commands and/or other organization-defined actions*].

Supplemental Guidance: Dual authorization mechanisms require the approval of two authorized individuals in order to execute. Organizations do not require dual authorization mechanisms when immediate responses are necessary to ensure public and environmental safety. Dual authorization may also be known as two-person control. Related controls: CP-9, MP-6.

(3) *ACCESS ENFORCEMENT | MANDATORY ACCESS CONTROL*

The information system enforces [*Assignment: organization-defined mandatory access control policies*] over all subjects and objects where the policy specifies that:

(a) The policy is uniformly enforced across all subjects and objects within the boundary of the information system;

(b) A subject that has been granted access to information is constrained from doing any of the following;

(1) Passing the information to unauthorized subjects or objects;

(2) Granting its privileges to other subjects;

(3) Changing one or more security attributes on subjects, objects, the information system, or information system components;

(4) Choosing the security attributes and attribute values to be associated with newly created or modified objects; or

(5) Changing the rules governing access control; and

(c) [*Assignment: Organized-defined subjects*] may explicitly be granted [*Assignment: organization-defined privileges (i.e., they are trusted subjects)*] such that they are not limited by some or all of the above constraints.

Supplemental Guidance: Mandatory access control as defined in this control enhancement is synonymous with nondiscretionary access control, and is not constrained only to certain historical uses (e.g., implementations using the Bell-LaPadula Model). The above class of mandatory access control policies constrains what actions subjects can take with information obtained from data objects for which they have already been granted access, thus preventing the subjects from passing the information to unauthorized subjects and objects. This class of mandatory access control policies also constrains what actions subjects can take with respect to the propagation of access control privileges; that is, a subject with a privilege cannot pass that privilege to other subjects. The policy is uniformly enforced over all subjects and objects to which the information system has control. Otherwise, the access control policy can be circumvented. This enforcement typically is provided via an implementation that meets the reference monitor concept (see AC-25). The policy is bounded by the information system boundary (i.e., once the information is passed outside of the control of the system, additional means may be required to ensure that the constraints on the information remain in effect). The trusted subjects described above are granted privileges consistent with the concept of least privilege (see AC-6). Trusted subjects are only given the minimum privileges relative to the above policy necessary for satisfying organizational mission/business needs. The control is most applicable when there is some policy mandate (e.g., law, Executive Order, directive, or regulation) that establishes a policy regarding access to sensitive/classified information and some users of the information system are not authorized access to all sensitive/classified information resident in the information system. This control can operate in conjunction with AC-3 (4). A subject that is constrained in its operation by policies governed by this control is still able to operate under the less rigorous constraints of AC-3 (4), but policies governed by this control take precedence over the less rigorous constraints of AC-3 (4). For example,

while a mandatory access control policy imposes a constraint preventing a subject from passing information to another subject operating at a different sensitivity label, AC-3 (4) permits the subject to pass the information to any subject with the same sensitivity label as the subject. Related controls: AC-25, SC-11.

(4) *ACCESS ENFORCEMENT | DISCRETIONARY ACCESS CONTROL*

The information system enforces [*Assignment: organization-defined discretionary access control policies*] over defined subjects and objects where the policy specifies that a subject that has been granted access to information can do one or more of the following:

(a) Pass the information to any other subjects or objects;

(b) Grant its privileges to other subjects;

(c) Change security attributes on subjects, objects, the information system, or the information system's components;

(d) Choose the security attributes to be associated with newly created or revised objects; or

(e) Change the rules governing access control.

Supplemental Guidance: When discretionary access control policies are implemented, subjects are not constrained with regard to what actions they can take with information for which they have already been granted access. Thus, subjects that have been granted access to information are not prevented from passing (i.e., the subjects have the discretion to pass) the information to other subjects or objects. This control enhancement can operate in conjunction with AC-3 (3). A subject that is constrained in its operation by policies governed by AC-3 (3) is still able to operate under the less rigorous constraints of this control enhancement. Thus, while AC-3 (3) imposes constraints preventing a subject from passing information to another subject operating at a different sensitivity level, AC-3 (4) permits the subject to pass the information to any subject at the same sensitivity level. The policy is bounded by the information system boundary. Once the information is passed outside of the control of the information system, additional means may be required to ensure that the constraints remain in effect. While the older, more traditional definitions of discretionary access control require identity-based access control, that limitation is not required for this use of discretionary access control.

(5) *ACCESS ENFORCEMENT | SECURITY-RELEVANT INFORMATION*

The information system prevents access to [*Assignment: organization-defined security-relevant information*] except during secure, non-operable system states.

Supplemental Guidance: Security-relevant information is any information within information systems that can potentially impact the operation of security functions or the provision of security services in a manner that could result in failure to enforce system security policies or maintain the isolation of code and data. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Secure, non-operable system states include the times in which information systems are not performing mission/business-related processing (e.g., the system is off-line for maintenance, troubleshooting, boot-up, shut down). Related control: CM-3.

(6) *ACCESS ENFORCEMENT | PROTECTION OF USER AND SYSTEM INFORMATION*

[Withdrawn: Incorporated into MP-4 and SC-28].

(7) *ACCESS ENFORCEMENT | ROLE-BASED ACCESS CONTROL*

The information system enforces a role-based access control policy over defined subjects and objects and controls access based upon [*Assignment: organization-defined roles and users authorized to assume such roles*].

Supplemental Guidance: Role-based access control (RBAC) is an access control policy that restricts information system access to authorized users. Organizations can create specific roles based on job functions and the authorizations (i.e., privileges) to perform needed operations on organizational information systems associated with the organization-defined roles. When users are assigned to the organizational roles, they inherit the authorizations or privileges defined for those roles. RBAC simplifies privilege administration for organizations because privileges are not assigned directly to every user (which can be a significant number of

individuals for mid- to large-size organizations) but are instead acquired through role assignments. RBAC can be implemented either as a mandatory or discretionary form of access control. For organizations implementing RBAC with mandatory access controls, the requirements in AC-3 (3) define the scope of the subjects and objects covered by the policy.

(8) *ACCESS ENFORCEMENT | REVOCATION OF ACCESS AUTHORIZATIONS*

The information system enforces the revocation of access authorizations resulting from changes to the security attributes of subjects and objects based on [*Assignment: organization-defined rules governing the timing of revocations of access authorizations*].

Supplemental Guidance: Revocation of access rules may differ based on the types of access revoked. For example, if a subject (i.e., user or process) is removed from a group, access may not be revoked until the next time the object (e.g., file) is opened or until the next time the subject attempts a new access to the object. Revocation based on changes to security labels may take effect immediately. Organizations can provide alternative approaches on how to make revocations immediate if information systems cannot provide such capability and immediate revocation is necessary.

(9) *ACCESS ENFORCEMENT | CONTROLLED RELEASE*

The information system does not release information outside of the established system boundary unless:

(a) The receiving [*Assignment: organization-defined information system or system component*] provides [*Assignment: organization-defined security safeguards*]; and

(b) [*Assignment: organization-defined security safeguards*] are used to validate the appropriateness of the information designated for release.

Supplemental Guidance: Information systems can only protect organizational information within the confines of established system boundaries. Additional security safeguards may be needed to ensure that such information is adequately protected once it is passed beyond the established information system boundaries. Examples of information leaving the system boundary include transmitting information to an external information system or printing the information on one of its printers. In cases where the information system is unable to make a determination of the adequacy of the protections provided by entities outside its boundary, as a mitigating control, organizations determine procedurally whether the external information systems are providing adequate security. The means used to determine the adequacy of the security provided by external information systems include, for example, conducting inspections or periodic testing, establishing agreements between the organization and its counterpart organizations, or some other process. The means used by external entities to protect the information received need not be the same as those used by the organization, but the means employed are sufficient to provide consistent adjudication of the security policy to protect the information. This control enhancement requires information systems to employ technical or procedural means to validate the information prior to releasing it to external systems. For example, if the information system passes information to another system controlled by another organization, technical means are employed to validate that the security attributes associated with the exported information are appropriate for the receiving system. Alternatively, if the information system passes information to a printer in organization-controlled space, procedural means can be employed to ensure that only appropriately authorized individuals gain access to the printer. This control enhancement is most applicable when there is some policy mandate (e.g., law, Executive Order, directive, or regulation) that establishes policy regarding access to the information, and that policy applies beyond the realm of a particular information system or organization.

(10) *ACCESS ENFORCEMENT | AUDITED OVERRIDE OF ACCESS CONTROL MECHANISMS*

The organization employs an audited override of automated access control mechanisms under [*Assignment: organization-defined conditions*].

Supplemental Guidance: Related controls: AU-2, AU-6.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AC-3	**MOD** AC-3	**HIGH** AC-3

AC-4 INFORMATION FLOW ENFORCEMENT

Control: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [*Assignment: organization-defined information flow control policies*].

Supplemental Guidance: Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include, for example, keeping export-controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, restricting web requests to the Internet that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between information systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes, for example: (i) prohibiting information transfers between interconnected systems (i.e., allowing access only); (ii) employing hardware mechanisms to enforce one-way information flows; and (iii) implementing trustworthy regrading mechanisms to reassign security attributes and security labels.

Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering/inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 3 through 22 primarily address cross-domain solution needs which focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, for example, high-assurance guards. Such capabilities are generally not available in commercial off-the-shelf information technology products. Related controls: AC-3, AC-17, AC-19, AC-21, CM-6, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18.

Control Enhancements:

(1) *INFORMATION FLOW ENFORCEMENT | OBJECT SECURITY ATTRIBUTES*

The information system uses [*Assignment: organization-defined security attributes*] associated with [*Assignment: organization-defined information, source, and destination objects*] to enforce [*Assignment: organization-defined information flow control policies*] as a basis for flow control decisions.

Supplemental Guidance: Information flow enforcement mechanisms compare security attributes associated with information (data content and data structure) and source/destination objects, and respond appropriately (e.g., block, quarantine, alert administrator) when the mechanisms encounter information flows not explicitly allowed by information flow policies. For example, an information object labeled *Secret* would be allowed to flow to a destination object labeled *Secret*, but an information object labeled *Top Secret* would not be allowed to flow to a

destination object labeled *Secret*. Security attributes can also include, for example, source and destination addresses employed in traffic filter firewalls. Flow enforcement using explicit security attributes can be used, for example, to control the release of certain types of information. Related control: AC-16.

(2) *INFORMATION FLOW ENFORCEMENT | PROCESSING DOMAINS*

The information system uses protected processing domains to enforce [*Assignment: organization-defined information flow control policies*] as a basis for flow control decisions.

Supplemental Guidance: Within information systems, protected processing domains are processing spaces that have controlled interactions with other processing spaces, thus enabling control of information flows between these spaces and to/from data/information objects. A protected processing domain can be provided, for example, by implementing domain and type enforcement. In domain and type enforcement, information system processes are assigned to domains; information is identified by types; and information flows are controlled based on allowed information accesses (determined by domain and type), allowed signaling among domains, and allowed process transitions to other domains.

(3) *INFORMATION FLOW ENFORCEMENT | DYNAMIC INFORMATION FLOW CONTROL*

The information system enforces dynamic information flow control based on [*Assignment: organization-defined policies*].

Supplemental Guidance: Organizational policies regarding dynamic information flow control include, for example, allowing or disallowing information flows based on changing conditions or mission/operational considerations. Changing conditions include, for example, changes in organizational risk tolerance due to changes in the immediacy of mission/business needs, changes in the threat environment, and detection of potentially harmful or adverse events. Related control: SI-4.

(4) *INFORMATION FLOW ENFORCEMENT | CONTENT CHECK ENCRYPTED INFORMATION*

The information system prevents encrypted information from bypassing content-checking mechanisms by [*Selection (one or more): decrypting the information; blocking the flow of the encrypted information; terminating communications sessions attempting to pass encrypted information;* [*Assignment: organization-defined procedure or method*]].

Supplemental Guidance: Related control: SI-4.

(5) *INFORMATION FLOW ENFORCEMENT | EMBEDDED DATA TYPES*

The information system enforces [*Assignment: organization-defined limitations*] on embedding data types within other data types.

Supplemental Guidance: Embedding data types within other data types may result in reduced flow control effectiveness. Data type embedding includes, for example, inserting executable files as objects within word processing files, inserting references or descriptive information into a media file, and compressed or archived data types that may include multiple embedded data types. Limitations on data type embedding consider the levels of embedding and prohibit levels of data type embedding that are beyond the capability of the inspection tools.

(6) *INFORMATION FLOW ENFORCEMENT | METADATA*

The information system enforces information flow control based on [*Assignment: organization-defined metadata*].

Supplemental Guidance: Metadata is information used to describe the characteristics of data. Metadata can include structural metadata describing data structures (e.g., data format, syntax, and semantics) or descriptive metadata describing data contents (e.g., age, location, telephone number). Enforcing allowed information flows based on metadata enables simpler and more effective flow control. Organizations consider the trustworthiness of metadata with regard to data accuracy (i.e., knowledge that the metadata values are correct with respect to the data), data integrity (i.e., protecting against unauthorized changes to metadata tags), and the binding of metadata to the data payload (i.e., ensuring sufficiently strong binding techniques with appropriate levels of assurance). Related controls: AC-16, SI-7.

(7) *INFORMATION FLOW ENFORCEMENT | ONE-WAY FLOW MECHANISMS*

The information system enforces [*Assignment: organization-defined one-way flows*] using hardware mechanisms.

(8) *INFORMATION FLOW ENFORCEMENT | SECURITY POLICY FILTERS*

The information system enforces information flow control using [*Assignment: organization-defined security policy filters*] as a basis for flow control decisions for [*Assignment: organization-defined information flows*].

Supplemental Guidance: Organization-defined security policy filters can address data structures and content. For example, security policy filters for data structures can check for maximum file lengths, maximum field sizes, and data/file types (for structured and unstructured data). Security policy filters for data content can check for specific words (e.g., dirty/clean word filters), enumerated values or data value ranges, and hidden content. Structured data permits the interpretation of data content by applications. Unstructured data typically refers to digital information without a particular data structure or with a data structure that does not facilitate the development of rule sets to address the particular sensitivity of the information conveyed by the data or the associated flow enforcement decisions. Unstructured data consists of: (i) bitmap objects that are inherently non language-based (i.e., image, video, or audio files); and (ii) textual objects that are based on written or printed languages (e.g., commercial off-the-shelf word processing documents, spreadsheets, or emails). Organizations can implement more than one security policy filter to meet information flow control objectives (e.g., employing clean word lists in conjunction with dirty word lists may help to reduce false positives).

(9) *INFORMATION FLOW ENFORCEMENT | HUMAN REVIEWS*

The information system enforces the use of human reviews for [*Assignment: organization-defined information flows*] under the following conditions: [*Assignment: organization-defined conditions*].

Supplemental Guidance: Organizations define security policy filters for all situations where automated flow control decisions are possible. When a fully automated flow control decision is not possible, then a human review may be employed in lieu of, or as a complement to, automated security policy filtering. Human reviews may also be employed as deemed necessary by organizations.

(10) *INFORMATION FLOW ENFORCEMENT | ENABLE / DISABLE SECURITY POLICY FILTERS*

The information system provides the capability for privileged administrators to enable/disable [*Assignment: organization-defined security policy filters*] under the following conditions: [*Assignment: organization-defined conditions*].

Supplemental Guidance: For example, as allowed by the information system authorization, administrators can enable security policy filters to accommodate approved data types.

(11) *INFORMATION FLOW ENFORCEMENT | CONFIGURATION OF SECURITY POLICY FILTERS*

The information system provides the capability for privileged administrators to configure [*Assignment: organization-defined security policy filters*] to support different security policies.

Supplemental Guidance: For example, to reflect changes in security policies, administrators can change the list of "dirty words" that security policy mechanisms check in accordance with the definitions provided by organizations.

(12) *INFORMATION FLOW ENFORCEMENT | DATA TYPE IDENTIFIERS*

The information system, when transferring information between different security domains, uses [*Assignment: organization-defined data type identifiers*] to validate data essential for information flow decisions.

Supplemental Guidance: Data type identifiers include, for example, filenames, file types, file signatures/tokens, and multiple internal file signatures/tokens. Information systems may allow transfer of data only if compliant with data type format specifications.

(13) *INFORMATION FLOW ENFORCEMENT | DECOMPOSITION INTO POLICY-RELEVANT SUBCOMPONENTS*

The information system, when transferring information between different security domains, decomposes information into [Assignment: organization-defined policy-relevant subcomponents] for submission to policy enforcement mechanisms.

Supplemental Guidance: Policy enforcement mechanisms apply filtering, inspection, and/or sanitization rules to the policy-relevant subcomponents of information to facilitate flow enforcement prior to transferring such information to different security domains. Parsing transfer files facilitates policy decisions on source, destination, certificates, classification, attachments, and other security-related component differentiators.

(14) *INFORMATION FLOW ENFORCEMENT | SECURITY POLICY FILTER CONSTRAINTS*

The information system, when transferring information between different security domains, implements [*Assignment: organization-defined security policy filters*] requiring fully enumerated formats that restrict data structure and content.

Supplemental Guidance: Data structure and content restrictions reduce the range of potential malicious and/or unsanctioned content in cross-domain transactions. Security policy filters that restrict data structures include, for example, restricting file sizes and field lengths. Data content policy filters include, for example: (i) encoding formats for character sets (e.g., Universal Character Set Transformation Formats, American Standard Code for Information Interchange); (ii) restricting character data fields to only contain alpha-numeric characters; (iii) prohibiting special characters; and (iv) validating schema structures.

(15) *INFORMATION FLOW ENFORCEMENT | DETECTION OF UNSANCTIONED INFORMATION*

The information system, when transferring information between different security domains, examines the information for the presence of [*Assignment: organized-defined unsanctioned information*] and prohibits the transfer of such information in accordance with the [*Assignment: organization-defined security policy*].

Supplemental Guidance: Detection of unsanctioned information includes, for example, checking all information to be transferred for malicious code and dirty words. Related control: SI-3.

(16) *INFORMATION FLOW ENFORCEMENT | INFORMATION TRANSFERS ON INTERCONNECTED SYSTEMS*

[Withdrawn: Incorporated into AC-4].

(17) *INFORMATION FLOW ENFORCEMENT | DOMAIN AUTHENTICATION*

The information system uniquely identifies and authenticates source and destination points by [*Selection (one or more): organization, system, application, individual*] for information transfer.

Supplemental Guidance: Attribution is a critical component of a security concept of operations. The ability to identify source and destination points for information flowing in information systems, allows the forensic reconstruction of events when required, and encourages policy compliance by attributing policy violations to specific organizations/individuals. Successful domain authentication requires that information system labels distinguish among systems, organizations, and individuals involved in preparing, sending, receiving, or disseminating information. Related controls: IA-2, IA-3, IA-4, IA-5.

(18) *INFORMATION FLOW ENFORCEMENT | SECURITY ATTRIBUTE BINDING*

The information system binds security attributes to information using [*Assignment: organization-defined binding techniques*] to facilitate information flow policy enforcement.

Supplemental Guidance: Binding techniques implemented by information systems affect the strength of security attribute binding to information. Binding strength and the assurance associated with binding techniques play an important part in the trust organizations have in the information flow enforcement process. The binding techniques affect the number and degree of additional reviews required by organizations. Related controls: AC-16, SC-16.

(19) *INFORMATION FLOW ENFORCEMENT | VALIDATION OF METADATA*

The information system, when transferring information between different security domains, applies the same security policy filtering to metadata as it applies to data payloads.

Supplemental Guidance: This control enhancement requires the validation of metadata and the data to which the metadata applies. Some organizations distinguish between metadata and data payloads (i.e., only the data to which the metadata is bound). Other organizations do not make such distinctions, considering metadata and the data to which the metadata applies as part of the payload. All information (including metadata and the data to which the metadata applies) is subject to filtering and inspection.

(20) *INFORMATION FLOW ENFORCEMENT | APPROVED SOLUTIONS*

The organization employs [*Assignment: organization-defined solutions in approved configurations*] to control the flow of [*Assignment: organization-defined information*] across security domains.

Supplemental Guidance: Organizations define approved solutions and configurations in cross-domain policies and guidance in accordance with the types of information flows across

classification boundaries. The Unified Cross Domain Management Office (UCDMO) provides a baseline listing of approved cross-domain solutions.

(21) *INFORMATION FLOW ENFORCEMENT | PHYSICAL / LOGICAL SEPARATION OF INFORMATION FLOWS*

The information system separates information flows logically or physically using [*Assignment: organization-defined mechanisms and/or techniques*] to accomplish [*Assignment: organization-defined required separations by types of information*].

Supplemental Guidance: Enforcing the separation of information flows by type can enhance protection by ensuring that information is not commingled while in transit and by enabling flow control by transmission paths perhaps not otherwise achievable. Types of separable information include, for example, inbound and outbound communications traffic, service requests and responses, and information of differing security categories.

(22) *INFORMATION FLOW ENFORCEMENT | ACCESS ONLY*

The information system provides access from a single device to computing platforms, applications, or data residing on multiple different security domains, while preventing any information flow between the different security domains.

Supplemental Guidance: The information system, for example, provides a desktop for users to access each connected security domain without providing any mechanisms to allow transfer of information between the different security domains.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** AC-4	**HIGH** AC-4

AC-5 SEPARATION OF DUTIES

Control: The organization:

a. Separates [*Assignment: organization-defined duties of individuals*];

b. Documents separation of duties of individuals; and

c. Defines information system access authorizations to support separation of duties.

Supplemental Guidance: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Related controls: AC-3, AC-6, PE-3, PE-4, PS-2.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** AC-5	**HIGH** AC-5

AC-6 LEAST PRIVILEGE

Control: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Supplemental Guidance: Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.

Control Enhancements:

(1) *LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS*

The organization explicitly authorizes access to [*Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information*].

Supplemental Guidance: Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. Related controls: AC-17, AC-18, AC-19.

(2) *LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS*

The organization requires that users of information system accounts, or roles, with access to [*Assignment: organization-defined security functions or security-relevant information*], use non-privileged accounts or roles, when accessing nonsecurity functions.

Supplemental Guidance: This control enhancement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Related control: PL-4.

(3) *LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS*

The organization authorizes network access to [*Assignment: organization-defined privileged commands*] only for [*Assignment: organization-defined compelling operational needs*] and documents the rationale for such access in the security plan for the information system.

Supplemental Guidance: Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device). Related control: AC-17.

(4) *LEAST PRIVILEGE | SEPARATE PROCESSING DOMAINS*

The information system provides separate processing domains to enable finer-grained allocation of user privileges.

Supplemental Guidance: Providing separate processing domains for finer-grained allocation of user privileges includes, for example: (i) using virtualization techniques to allow additional privileges within a virtual machine while restricting privileges to other virtual machines or to the underlying actual machine; (ii) employing hardware and/or software domain separation mechanisms; and (iii) implementing separate physical domains. Related controls: AC-4, SC-3, SC-30, SC-32.

(5) *LEAST PRIVILEGE | PRIVILEGED ACCOUNTS*

The organization restricts privileged accounts on the information system to [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions. Organizations may differentiate in the application of this control enhancement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control information

system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk. Related control: CM-6.

(6) *LEAST PRIVILEGE | PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS*

The organization prohibits privileged access to the information system by non-organizational users.

Supplemental Guidance: Related control: IA-8.

(7) *LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES*

The organization:

(a) Reviews [*Assignment: organization-defined frequency*] the privileges assigned to [*Assignment: organization-defined roles or classes of users*] to validate the need for such privileges; and

(b) Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.

Supplemental Guidance: The need for certain assigned user privileges may change over time reflecting changes in organizational missions/business function, environments of operation, technologies, or threat. Periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions. Related control: CA-7.

(8) *LEAST PRIVILEGE | PRIVILEGE LEVELS FOR CODE EXECUTION*

The information system prevents [*Assignment: organization-defined software*] from executing at higher privilege levels than users executing the software.

Supplemental Guidance: In certain situations, software applications/programs need to execute with elevated privileges to perform required functions. However, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such applications/programs, those users are indirectly provided with greater privileges than assigned by organizations.

(9) *LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS*

The information system audits the execution of privileged functions.

Supplemental Guidance: Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat (APT). Related control: AU-2.

(10) *LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS*

The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Supplemental Guidance: Privileged functions include, for example, establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** AC-6 (1) (2) (5) (9) (10)	**HIGH** AC-6 (1) (2) (3) (5) (9) (10)

AC-7 UNSUCCESSFUL LOGON ATTEMPTS

Control: The information system:

a. Enforces a limit of [*Assignment: organization-defined number*] consecutive invalid logon attempts by a user during a [*Assignment: organization-defined time period*]; and

b. Automatically [*Selection: locks the account/node for an* [*Assignment: organization-defined time period*]; *locks the account/node until released by an administrator; delays next logon prompt according to* [*Assignment: organization-defined delay algorithm*]] when the maximum number of unsuccessful attempts is exceeded.

Supplemental Guidance: This control applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by information systems are usually temporary and automatically release after a predetermined time period established by organizations. If a delay algorithm is selected, organizations may choose to employ different algorithms for different information system components based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels. Related controls: AC-2, AC-9, AC-14, IA-5.

Control Enhancements:

(1) *UNSUCCESSFUL LOGON ATTEMPTS | AUTOMATIC ACCOUNT LOCK*

[Withdrawn: Incorporated into AC-7].

(2) *UNSUCCESSFUL LOGON ATTEMPTS | PURGE / WIPE MOBILE DEVICE*

The information system purges/wipes information from [*Assignment: organization-defined mobile devices*] based on [*Assignment: organization-defined purging/wiping requirements/techniques*] after [*Assignment: organization-defined number*] consecutive, unsuccessful device logon attempts.

Supplemental Guidance: This control enhancement applies only to mobile devices for which a logon occurs (e.g., personal digital assistants, smart phones, tablets). The logon is to the mobile device, not to any one account on the device. Therefore, successful logons to any accounts on mobile devices reset the unsuccessful logon count to zero. Organizations define information to be purged/wiped carefully in order to avoid over purging/wiping which may result in devices becoming unusable. Purging/wiping may be unnecessary if the information on the device is protected with sufficiently strong encryption mechanisms. Related controls: AC-19, MP-5, MP-6, SC-13.

References: None.

Priority and Baseline Allocation:

P2	**LOW** AC-7	**MOD** AC-7	**HIGH** AC-7

AC-8 SYSTEM USE NOTIFICATION

Control: The information system:

a. Displays to users [*Assignment: organization-defined system use notification message or banner*] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:

1. Users are accessing a U.S. Government information system;

2. Information system usage may be monitored, recorded, and subject to audit;

3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and

4. Use of the information system indicates consent to monitoring and recording;

b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and

c. For publicly accessible systems:

1. Displays system use information [*Assignment: organization-defined conditions*], before granting further access;

2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and

3. Includes a description of the authorized uses of the system.

Supplemental Guidance: System use notifications can be implemented using messages or warning banners displayed before individuals log in to information systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. Organizations consider system use notification messages/banners displayed in multiple languages based on specific organizational needs and the demographics of information system users. Organizations also consult with the Office of the General Counsel for legal review and approval of warning banner content.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AC-8	**MOD** AC-8	**HIGH** AC-8

AC-9 PREVIOUS LOGON (ACCESS) NOTIFICATION

Control: The information system notifies the user, upon successful logon (access) to the system, of the date and time of the last logon (access).

Supplemental Guidance: This control is applicable to logons to information systems via human user interfaces and logons to systems that occur in other types of architectures (e.g., service-oriented architectures). Related controls: AC-7, PL-4.

Control Enhancements:

(1) *PREVIOUS LOGON NOTIFICATION | UNSUCCESSFUL LOGONS*

The information system notifies the user, upon successful logon/access, of the number of unsuccessful logon/access attempts since the last successful logon/access.

(2) *PREVIOUS LOGON NOTIFICATION | SUCCESSFUL / UNSUCCESSFUL LOGONS*

The information system notifies the user of the number of [*Selection: successful logons/accesses; unsuccessful logon/access attempts; both*] during [*Assignment: organization-defined time period*].

(3) *PREVIOUS LOGON NOTIFICATION | NOTIFICATION OF ACCOUNT CHANGES*

The information system notifies the user of changes to [*Assignment: organization-defined security-related characteristics/parameters of the user's account*] during [*Assignment: organization-defined time period*].

(4) *PREVIOUS LOGON NOTIFICATION | ADDITIONAL LOGON INFORMATION*

The information system notifies the user, upon successful logon (access), of the following additional information: [*Assignment: organization-defined information to be included in addition to the date and time of the last logon (access)*].

Supplemental Guidance: This control enhancement permits organizations to specify additional information to be provided to users upon logon including, for example, the location of last logon. User location is defined as that information which can be determined by information systems, for example, IP addresses from which network logons occurred, device identifiers, or notifications of local logons.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

AC-10 CONCURRENT SESSION CONTROL

Control: The information system limits the number of concurrent sessions for each [*Assignment: organization-defined account and/or account type*] to [*Assignment: organization-defined number*].

Supplemental Guidance: Organizations may define the maximum number of concurrent sessions for information system accounts globally, by account type (e.g., privileged user, non-privileged user, domain, specific application), by account, or a combination. For example, organizations may limit the number of concurrent sessions for system administrators or individuals working in particularly sensitive domains or mission-critical applications. This control addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P3	**LOW** Not Selected	**MOD** Not Selected	**HIGH** AC-10

AC-11 SESSION LOCK

Control: The information system:

a. Prevents further access to the system by initiating a session lock after [*Assignment: organization-defined time period*] of inactivity or upon receiving a request from a user; and

b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

Supplemental Guidance: Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. This is typically at the operating system level, but can also be at the application level. Session locks are not an acceptable substitute for logging out of information systems, for example, if organizations require users to log out at the end of workdays. Related control: AC-7.

Control Enhancements:

(1) *SESSION LOCK | PATTERN-HIDING DISPLAYS*

The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

Supplemental Guidance: Publicly viewable images can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the images convey sensitive information.

References: OMB Memorandum 06-16.

Priority and Baseline Allocation:

P3	**LOW** Not Selected	**MOD** AC-11 (1)	**HIGH** AC-11 (1)

AC-12 SESSION TERMINATION

Control: The information system automatically terminates a user session after [*Assignment: organization-defined conditions or trigger events requiring session disconnect*].

Supplemental Guidance: This control addresses the termination of user-initiated logical sessions in contrast to SC-10 which addresses the termination of network connections that are associated with communications sessions (i.e., network disconnect). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational information system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, time-of-day restrictions on information system use. Related controls: SC-10, SC-23.

Control Enhancements:

(1) *SESSION TERMINATION | USER-INITIATED LOGOUTS / MESSAGE DISPLAYS*

The information system:

(a) Provides a logout capability for user-initiated communications sessions whenever authentication is used to gain access to [*Assignment: organization-defined information resources*]; and

(b) Displays an explicit logout message to users indicating the reliable termination of authenticated communications sessions.

Supplemental Guidance: Information resources to which users gain access via authentication include, for example, local workstations, databases, and password-protected websites/web-based services. Logout messages for web page access, for example, can be displayed after authenticated sessions have been terminated. However, for some types of interactive sessions including, for example, file transfer protocol (FTP) sessions, information systems typically send logout messages as final messages prior to terminating sessions.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** AC-12	**HIGH** AC-12

AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL

[Withdrawn: Incorporated into AC-2 and AU-6].

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

Control: The organization:

a. Identifies [*Assignment: organization-defined user actions*] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and

b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

Supplemental Guidance: This control addresses situations in which organizations determine that no identification or authentication is required in organizational information systems. Organizations may allow a limited number of user actions without identification or authentication including, for example, when individuals access public websites or other publicly accessible federal information systems, when individuals use mobile phones to receive calls, or when facsimiles are received. Organizations also identify actions that normally require identification or authentication but may under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed. Such bypasses may occur, for example, via a software-readable physical switch that commands bypass of the logon functionality and is protected from accidental or unmonitored use. This control does not apply to situations where identification and authentication have already occurred and are not repeated, but rather to situations where identification and authentication have not yet occurred. Organizations may decide that there are no user actions that can be performed on organizational information systems without identification and authentication and thus, the values for assignment statements can be *none*. Related controls: CP-2, IA-2.

Control Enhancements: None.

(1) *PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION | NECESSARY USES*
[Withdrawn: Incorporated into AC-14].

References: None.

Priority and Baseline Allocation:

P3	**LOW** AC-14	**MOD** AC-14	**HIGH** AC-14

AC-15 AUTOMATED MARKING

[Withdrawn: Incorporated into MP-3].

AC-16 SECURITY ATTRIBUTES

Control: The organization:

a. Provides the means to associate [*Assignment: organization-defined types of security attributes*] having [*Assignment: organization-defined security attribute values*] with information in storage, in process, and/or in transmission;

b. Ensures that the security attribute associations are made and retained with the information;

c. Establishes the permitted [*Assignment: organization-defined security attributes*] for [*Assignment: organization-defined information systems*]; and

d. Determines the permitted [*Assignment: organization-defined values or ranges*] for each of the established security attributes.

Supplemental Guidance: Information is represented internally within information systems using abstractions known as data structures. Internal data structures can represent different types of entities, both active and passive. Active entities, also known as *subjects*, are typically associated with individuals, devices, or processes acting on behalf of individuals. Passive entities, also known as *objects*, are typically associated with data structures such as records, buffers, tables, files, inter-process pipes, and communications ports. Security attributes, a form of metadata, are abstractions representing the basic properties or characteristics of active and passive entities with respect to safeguarding information. These attributes may be associated with active entities (i.e., subjects) that have the potential to send or receive information, to cause information to flow among objects,

or to change the information system state. These attributes may also be associated with passive entities (i.e., objects) that contain or receive information. The association of security attributes to subjects and objects is referred to as *binding* and is typically inclusive of setting the attribute value and the attribute type. Security attributes when bound to data/information, enables the enforcement of information security policies for access control and information flow control, either through organizational processes or information system functions or mechanisms. The content or assigned values of security attributes can directly affect the ability of individuals to access organizational information.

Organizations can define the types of attributes needed for selected information systems to support missions/business functions. There is potentially a wide range of values that can be assigned to any given security attribute. Release markings could include, for example, US only, NATO, or NOFORN (not releasable to foreign nationals). By specifying permitted attribute ranges and values, organizations can ensure that the security attribute values are meaningful and relevant. The term *security labeling* refers to the association of security attributes with subjects and objects represented by internal data structures within organizational information systems, to enable information system-based enforcement of information security policies. Security labels include, for example, access authorizations, data life cycle protection (i.e., encryption and data expiration), nationality, affiliation as contractor, and classification of information in accordance with legal and compliance requirements. The term security marking refers to the association of security attributes with objects in a human-readable form, to enable organizational process-based enforcement of information security policies. The AC-16 base control represents the requirement for user-based attribute association (marking). The enhancements to AC-16 represent additional requirements including information system-based attribute association (labeling). Types of attributes include, for example, classification level for objects and clearance (access authorization) level for subjects. An example of a value for both of these attribute types is *Top Secret*. Related controls: AC-3, AC-4, AC-6, AC-21, AU-2, AU-10, SC-16, MP-3.

Control Enhancements:

(1) *SECURITY ATTRIBUTES | DYNAMIC ATTRIBUTE ASSOCIATION*

The information system dynamically associates security attributes with [*Assignment: organization-defined subjects and objects*] in accordance with [*Assignment: organization-defined security policies*] as information is created and combined.

Supplemental Guidance: Dynamic association of security attributes is appropriate whenever the security characteristics of information changes over time. Security attributes may change, for example, due to information aggregation issues (i.e., the security characteristics of individual information elements are different from the combined elements), changes in individual access authorizations (i.e., privileges), and changes in the security category of information. Related control: AC-4.

(2) *SECURITY ATTRIBUTES | ATTRIBUTE VALUE CHANGES BY AUTHORIZED INDIVIDUALS*

The information system provides authorized individuals (or processes acting on behalf of individuals) the capability to define or change the value of associated security attributes.

Supplemental Guidance: The content or assigned values of security attributes can directly affect the ability of individuals to access organizational information. Therefore, it is important for information systems to be able to limit the ability to create or modify security attributes to authorized individuals. Related controls: AC-6, AU-2.

(3) *SECURITY ATTRIBUTES | MAINTENANCE OF ATTRIBUTE ASSOCIATIONS BY INFORMATION SYSTEM*

The information system maintains the association and integrity of [*Assignment: organization-defined security attributes*] to [*Assignment: organization-defined subjects and objects*].

Supplemental Guidance: Maintaining the association and integrity of security attributes to subjects and objects with sufficient assurance helps to ensure that the attribute associations can be used as the basis of automated policy actions. Automated policy actions include, for example, access control decisions or information flow control decisions.

(4) *SECURITY ATTRIBUTES | ASSOCIATION OF ATTRIBUTES BY AUTHORIZED INDIVIDUALS*

The information system supports the association of [*Assignment: organization-defined security attributes*] with [*Assignment: organization-defined subjects and objects*] by authorized individuals (or processes acting on behalf of individuals).

Supplemental Guidance: The support provided by information systems can vary to include: (i) prompting users to select specific security attributes to be associated with specific information objects; (ii) employing automated mechanisms for categorizing information with appropriate attributes based on defined policies; or (iii) ensuring that the combination of selected security attributes selected is valid. Organizations consider the creation, deletion, or modification of security attributes when defining auditable events.

(5) *SECURITY ATTRIBUTES | ATTRIBUTE DISPLAYS FOR OUTPUT DEVICES*

The information system displays security attributes in human-readable form on each object that the system transmits to output devices to identify [*Assignment: organization-identified special dissemination, handling, or distribution instructions*] using [*Assignment: organization-identified human-readable, standard naming conventions*].

Supplemental Guidance: Information system outputs include, for example, pages, screens, or equivalent. Information system output devices include, for example, printers and video displays on computer workstations, notebook computers, and personal digital assistants.

(6) *SECURITY ATTRIBUTES | MAINTENANCE OF ATTRIBUTE ASSOCIATION BY ORGANIZATION*

The organization allows personnel to associate, and maintain the association of [*Assignment: organization-defined security attributes*] with [*Assignment: organization-defined subjects and objects*] in accordance with [*Assignment: organization-defined security policies*].

Supplemental Guidance: This control enhancement requires individual users (as opposed to the information system) to maintain associations of security attributes with subjects and objects.

(7) *SECURITY ATTRIBUTES | CONSISTENT ATTRIBUTE INTERPRETATION*

The organization provides a consistent interpretation of security attributes transmitted between distributed information system components.

Supplemental Guidance: In order to enforce security policies across multiple components in distributed information systems (e.g., distributed database management systems, cloud-based systems, and service-oriented architectures), organizations provide a consistent interpretation of security attributes that are used in access enforcement and flow enforcement decisions. Organizations establish agreements and processes to ensure that all distributed information system components implement security attributes with consistent interpretations in automated access/flow enforcement actions.

(8) *SECURITY ATTRIBUTES | ASSOCIATION TECHNIQUES / TECHNOLOGIES*

The information system implements [*Assignment: organization-defined techniques or technologies*] with [*Assignment: organization-defined level of assurance*] in associating security attributes to information.

Supplemental Guidance: The association (i.e., binding) of security attributes to information within information systems is of significant importance with regard to conducting automated access enforcement and flow enforcement actions. The association of such security attributes can be accomplished with technologies/techniques providing different levels of assurance. For example, information systems can cryptographically bind security attributes to information using digital signatures with the supporting cryptographic keys protected by hardware devices (sometimes known as hardware roots of trust).

(9) *SECURITY ATTRIBUTES | ATTRIBUTE REASSIGNMENT*

The organization ensures that security attributes associated with information are reassigned only via re-grading mechanisms validated using [*Assignment: organization-defined techniques or procedures*].

Supplemental Guidance: Validated re-grading mechanisms are employed by organizations to provide the requisite levels of assurance for security attribute reassignment activities. The validation is facilitated by ensuring that re-grading mechanisms are single purpose and of limited function. Since security attribute reassignments can affect security policy enforcement actions (e.g., access/flow enforcement decisions), using trustworthy re-grading mechanisms is necessary to ensure that such mechanisms perform in a consistent/correct mode of operation.

(10) *SECURITY ATTRIBUTES | ATTRIBUTE CONFIGURATION BY AUTHORIZED INDIVIDUALS*

The information system provides authorized individuals the capability to define or change the type and value of security attributes available for association with subjects and objects.

Supplemental Guidance: The content or assigned values of security attributes can directly affect the ability of individuals to access organizational information. Therefore, it is important for information systems to be able to limit the ability to create or modify security attributes to authorized individuals only.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

AC-17 REMOTE ACCESS

Control: The organization:

a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

b. Authorizes remote access to the information system prior to allowing such connections.

Supplemental Guidance: Remote access is access to organizational information systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include, for example, dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality and integrity over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate security controls (e.g., employing appropriate encryption techniques for confidentiality and integrity protection) may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. Also, VPNs with encrypted tunnels can affect the organizational capability to adequately monitor network communications traffic for malicious code. Remote access controls apply to information systems other than public web servers or systems designed for public access. This control addresses authorization prior to allowing remote access without specifying the formats for such authorization. While organizations may use interconnection security agreements to authorize remote access connections, such agreements are not required by this control. Enforcing access restrictions for remote connections is addressed in AC-3. Related controls: AC-2, AC-3, AC-18, AC-19, AC-20, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, MA-4, PE-17, PL-4, SC-10, SI-4.

Control Enhancements:

(1) *REMOTE ACCESS | AUTOMATED MONITORING / CONTROL*

The information system monitors and controls remote access methods.

Supplemental Guidance: Automated monitoring and control of remote access sessions allows organizations to detect cyber attacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of information system components (e.g., servers, workstations, notebook computers, smart phones, and tablets). Related controls: AU-2, AU-12.

(2) *REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION*

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Supplemental Guidance: The encryption strength of mechanism is selected based on the security categorization of the information. Related controls: SC-8, SC-12, SC-13.

(3) *REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS*

The information system routes all remote accesses through [*Assignment: organization-defined number*] managed network access control points.

Supplemental Guidance: Limiting the number of access control points for remote accesses reduces the attack surface for organizations. Organizations consider the Trusted Internet Connections (TIC) initiative requirements for external network connections. Related control: SC-7.

(4) *REMOTE ACCESS | PRIVILEGED COMMANDS / ACCESS*

The organization:

(a) Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [*Assignment: organization-defined needs*]; and

(b) Documents the rationale for such access in the security plan for the information system.

Supplemental Guidance: Related control: AC-6.

(5) *REMOTE ACCESS | MONITORING FOR UNAUTHORIZED CONNECTIONS*

[Withdrawn: Incorporated into SI-4].

(6) *REMOTE ACCESS | PROTECTION OF INFORMATION*

The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.

Supplemental Guidance: Related controls: AT-2, AT-3, PS-6.

(7) *REMOTE ACCESS | ADDITIONAL PROTECTION FOR SECURITY FUNCTION ACCESS*

[Withdrawn: Incorporated into AC-3 (10)].

(8) *REMOTE ACCESS | DISABLE NONSECURE NETWORK PROTOCOLS*

[Withdrawn: Incorporated into CM-7].

(9) *REMOTE ACCESS | DISCONNECT / DISABLE ACCESS*

The organization provides the capability to expeditiously disconnect or disable remote access to the information system within [*Assignment: organization-defined time period*].

Supplemental Guidance: This control enhancement requires organizations to have the capability to rapidly disconnect current users remotely accessing the information system and/or disable further remote access. The speed of disconnect or disablement varies based on the criticality of missions/business functions and the need to eliminate immediate or future remote access to organizational information systems.

References: NIST Special Publications 800-46, 800-77, 800-113, 800-114, 800-121.

Priority and Baseline Allocation:

P1	**LOW** AC-17	**MOD** AC-17 (1) (2) (3) (4)	**HIGH** AC-17 (1) (2) (3) (4)

AC-18 WIRELESS ACCESS

Control: The organization:

a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and

b. Authorizes wireless access to the information system prior to allowing such connections.

Supplemental Guidance: Wireless technologies include, for example, microwave, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication. Related controls: AC-2, AC-3, AC-17, AC-19, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, PL-4, SI-4.

Control Enhancements:

(1) *WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION*

The information system protects wireless access to the system using authentication of [*Selection (one or more): users; devices*] and encryption.

Supplemental Guidance: Related controls: SC-8, SC-13.

(2) *WIRELESS ACCESS | MONITORING UNAUTHORIZED CONNECTIONS*

[Withdrawn: Incorporated into SI-4].

(3) *WIRELESS ACCESS | DISABLE WIRELESS NETWORKING*

The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.

Supplemental Guidance: Related control: AC-19.

(4) *WIRELESS ACCESS | RESTRICT CONFIGURATIONS BY USERS*

The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.

Supplemental Guidance: Organizational authorizations to allow selected users to configure wireless networking capability are enforced in part, by the access enforcement mechanisms employed within organizational information systems. Related controls: AC-3, SC-15.

(5) *WIRELESS ACCESS | ANTENNAS / TRANSMISSION POWER LEVELS*

The organization selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.

Supplemental Guidance: Actions that may be taken by organizations to limit unauthorized use of wireless communications outside of organization-controlled boundaries include, for example: (i) reducing the power of wireless transmissions so that the transmissions are less likely to emit a signal that can be used by adversaries outside of the physical perimeters of organizations; (ii) employing measures such as TEMPEST to control wireless emanations; and (iii) using directional/beam forming antennas that reduce the likelihood that unintended receivers will be able to intercept signals. Prior to taking such actions, organizations can conduct periodic wireless surveys to understand the radio frequency profile of organizational information systems as well as other systems that may be operating in the area. Related control: PE-19.

References: NIST Special Publications 800-48, 800-94, 800-97.

Priority and Baseline Allocation:

P1	**LOW** AC-18	**MOD** AC-18 (1)	**HIGH** AC-18 (1) (4) (5)

AC-19 ACCESS CONTROL FOR MOBILE DEVICES

Control: The organization:

a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and

b. Authorizes the connection of mobile devices to organizational information systems.

Supplemental Guidance: A mobile device is a computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, E-readers, and tablets. Mobile devices are typically associated with a single individual and the device is usually in close proximity to the individual; however, the degree of proximity can vary depending upon on the form factor and size of the device. The

processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of desktop systems, depending upon the nature and intended purpose of the device. Due to the large variety of mobile devices with different technical characteristics and capabilities, organizational restrictions may vary for the different classes/types of such devices. Usage restrictions and specific implementation guidance for mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Organizations are cautioned that the need to provide adequate security for mobile devices goes beyond the requirements in this control. Many safeguards and countermeasures for mobile devices are reflected in other security controls in the catalog allocated in the initial control baselines as starting points for the development of security plans and overlays using the tailoring process. There may also be some degree of overlap in the requirements articulated by the security controls within the different families of controls. AC-20 addresses mobile devices that are not organization-controlled. Related controls: AC-3, AC-7, AC-18, AC-20, CA-9, CM-2, IA-2, IA-3, MP-2, MP-4, MP-5, PL-4, SC-7, SC-43, SI-3, SI-4.

Control Enhancements:

(1) *ACCESS CONTROL FOR MOBILE DEVICES | USE OF WRITABLE / PORTABLE STORAGE DEVICES*

[Withdrawn: Incorporated into MP-7].

(2) *ACCESS CONTROL FOR MOBILE DEVICES | USE OF PERSONALLY OWNED PORTABLE STORAGE DEVICES*

[Withdrawn: Incorporated into MP-7].

(3) *ACCESS CONTROL FOR MOBILE DEVICES | USE OF PORTABLE STORAGE DEVICES WITH NO IDENTIFIABLE OWNER*

[Withdrawn: Incorporated into MP-7].

(4) *ACCESS CONTROL FOR MOBILE DEVICES | RESTRICTIONS FOR CLASSIFIED INFORMATION*

The organization:

(a) Prohibits the use of unclassified mobile devices in facilities containing information systems processing, storing, or transmitting classified information unless specifically permitted by the authorizing official; and

(b) Enforces the following restrictions on individuals permitted by the authorizing official to use unclassified mobile devices in facilities containing information systems processing, storing, or transmitting classified information:

(1) Connection of unclassified mobile devices to classified information systems is prohibited;

(2) Connection of unclassified mobile devices to unclassified information systems requires approval from the authorizing official;

(3) Use of internal or external modems or wireless interfaces within the unclassified mobile devices is prohibited; and

(4) Unclassified mobile devices and the information stored on those devices are subject to random reviews and inspections by [*Assignment: organization-defined security officials*], and if classified information is found, the incident handling policy is followed.

(c) Restricts the connection of classified mobile devices to classified information systems in accordance with [*Assignment: organization-defined security policies*].

Supplemental Guidance: Related controls: CA-6, IR-4.

(5) *ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE / CONTAINER-BASED ENCRYPTION*

The organization employs [*Selection: full-device encryption; container encryption*] to protect the confidentiality and integrity of information on [*Assignment: organization-defined mobile devices*].

Supplemental Guidance: Container-based encryption provides a more fine-grained approach to the encryption of data/information on mobile devices, including for example, encrypting selected data structures such as files, records, or fields. Related controls: MP-5, SC-13, SC-28.

References: OMB Memorandum 06-16; NIST Special Publications 800-114, 800-124, 800-164.

Priority and Baseline Allocation:

P1	**LOW** AC-19	**MOD** AC-19 (5)	**HIGH** AC-19 (5)

AC-20 USE OF EXTERNAL INFORMATION SYSTEMS

Control: The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

a. Access the information system from external information systems; and

b. Process, store, or transmit organization-controlled information using external information systems.

Supplemental Guidance: External information systems are information systems or components of information systems that are outside of the authorization boundary established by organizations and for which organizations typically have no direct supervision and authority over the application of required security controls or the assessment of control effectiveness. External information systems include, for example: (i) personally owned information systems/devices (e.g., notebook computers, smart phones, tablets, personal digital assistants); (ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, train stations, convention centers, shopping malls, or airports); (iii) information systems owned or controlled by nonfederal governmental organizations; and (iv) federal information systems that are not owned by, operated by, or under the direct supervision and authority of organizations. This control also addresses the use of external information systems for the processing, storage, or transmission of organizational information, including, for example, accessing cloud services (e.g., infrastructure as a service, platform as a service, or software as a service) from organizational information systems.

For some external information systems (i.e., information systems operated by other federal agencies, including organizations subordinate to those agencies), the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. Information systems within these organizations would not be considered external. These situations occur when, for example, there are pre-existing sharing/trust agreements (either implicit or explicit) established between federal agencies or organizations subordinate to those agencies, or when such trust agreements are specified by applicable laws, Executive Orders, directives, or policies. Authorized individuals include, for example, organizational personnel, contractors, or other individuals with authorized access to organizational information systems and over which organizations have the authority to impose rules of behavior with regard to system access. Restrictions that organizations impose on authorized individuals need not be uniform, as those restrictions may vary depending upon the trust relationships between organizations. Therefore, organizations may choose to impose different security restrictions on contractors than on state, local, or tribal governments.

This control does not apply to the use of external information systems to access public interfaces to organizational information systems (e.g., individuals accessing federal information through www.usa.gov). Organizations establish terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. Terms and conditions address as a minimum: types of applications that can be accessed on organizational information systems from external information systems; and the highest security category of information that can be processed, stored, or transmitted on external information systems. If terms and conditions with the owners of external information systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems. Related controls: AC-3, AC-17, AC-19, CA-3, PL-4, SA-9.

Control Enhancements:

(1) *USE OF EXTERNAL INFORMATION SYSTEMS | LIMITS ON AUTHORIZED USE*

The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:

(a) Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or

(b) Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

Supplemental Guidance: This control enhancement recognizes that there are circumstances where individuals using external information systems (e.g., contractors, coalition partners) need to access organizational information systems. In those situations, organizations need confidence that the external information systems contain the necessary security safeguards (i.e., security controls), so as not to compromise, damage, or otherwise harm organizational information systems. Verification that the required security controls have been implemented can be achieved, for example, by third-party, independent assessments, attestations, or other means, depending on the confidence level required by organizations. Related control: CA-2.

(2) *USE OF EXTERNAL INFORMATION SYSTEMS | PORTABLE STORAGE DEVICES*

The organization [*Selection: restricts; prohibits*] the use of organization-controlled portable storage devices by authorized individuals on external information systems.

Supplemental Guidance: Limits on the use of organization-controlled portable storage devices in external information systems include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used.

(3) *USE OF EXTERNAL INFORMATION SYSTEMS | NON-ORGANIZATIONALLY OWNED SYSTEMS / COMPONENTS / DEVICES*

The organization [*Selection: restricts; prohibits*] the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit organizational information.

Supplemental Guidance: Non-organizationally owned devices include devices owned by other organizations (e.g., federal/state agencies, contractors) and personally owned devices. There are risks to using non-organizationally owned devices. In some cases, the risk is sufficiently high as to prohibit such use. In other cases, it may be such that the use of non-organizationally owned devices is allowed but restricted in some way. Restrictions include, for example: (i) requiring the implementation of organization-approved security controls prior to authorizing such connections; (ii) limiting access to certain types of information, services, or applications; (iii) using virtualization techniques to limit processing and storage activities to servers or other system components provisioned by the organization; and (iv) agreeing to terms and conditions for usage. For personally owned devices, organizations consult with the Office of the General Counsel regarding legal issues associated with using such devices in operational environments, including, for example, requirements for conducting forensic analyses during investigations after an incident.

(4) *USE OF EXTERNAL INFORMATION SYSTEMS | NETWORK ACCESSIBLE STORAGE DEVICES*

The organization prohibits the use of [*Assignment: organization-defined network accessible storage devices*] in external information systems.

Supplemental Guidance: Network accessible storage devices in external information systems include, for example, online storage devices in public, hybrid, or community cloud-based systems.

References: FIPS Publication 199.

Priority and Baseline Allocation:

P1	**LOW** AC-20	**MOD** AC-20 (1) (2)	**HIGH** AC-20 (1) (2)

AC-21 INFORMATION SHARING

Control: The organization:

a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [*Assignment: organization-defined information sharing circumstances where user discretion is required*]; and

b. Employs [*Assignment: organization-defined automated mechanisms or manual processes*] to assist users in making information sharing/collaboration decisions.

Supplemental Guidance: This control applies to information that may be restricted in some manner (e.g., privileged medical information, contract-sensitive information, proprietary information, personally identifiable information, classified information related to special access programs or compartments) based on some formal or administrative determination. Depending on the particular information-sharing circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program/compartment. Related control: AC-3.

Control Enhancements:

(1) *INFORMATION SHARING | AUTOMATED DECISION SUPPORT*

The information system enforces information-sharing decisions by authorized users based on access authorizations of sharing partners and access restrictions on information to be shared.

(2) *INFORMATION SHARING | INFORMATION SEARCH AND RETRIEVAL*

The information system implements information search and retrieval services that enforce [*Assignment: organization-defined information sharing restrictions*].

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** AC-21	**HIGH** AC-21

AC-22 PUBLICLY ACCESSIBLE CONTENT

Control: The organization:

a. Designates individuals authorized to post information onto a publicly accessible information system;

b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and

d. Reviews the content on the publicly accessible information system for nonpublic information [*Assignment: organization-defined frequency*] and removes such information, if discovered.

Supplemental Guidance: In accordance with federal laws, Executive Orders, directives, policies, regulations, standards, and/or guidance, the general public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act and proprietary information). This control addresses information systems that are controlled by the organization and accessible to the general public, typically without identification or authentication. The posting of information on non-organization information systems is covered by organizational policy. Related controls: AC-3, AC-4, AT-2, AT-3, AU-13.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P3	**LOW** AC-22	**MOD** AC-22	**HIGH** AC-22

AC-23 DATA MINING PROTECTION

Control: The organization employs [*Assignment: organization-defined data mining prevention and detection techniques*] for [*Assignment: organization-defined data storage objects*] to adequately detect and protect against data mining.

Supplemental Guidance: Data storage objects include, for example, databases, database records, and database fields. Data mining prevention and detection techniques include, for example: (i) limiting the types of responses provided to database queries; (ii) limiting the number/frequency of database queries to increase the work factor needed to determine the contents of such databases; and (iii) notifying organizational personnel when atypical database queries or accesses occur. This control focuses on the protection of organizational information from data mining while such information resides in organizational data stores. In contrast, AU-13 focuses on monitoring for organizational information that may have been mined or otherwise obtained from data stores and is now available as open source information residing on external sites, for example, through social networking or social media websites.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

AC-24 ACCESS CONTROL DECISIONS

Control: The organization establishes procedures to ensure [*Assignment: organization-defined access control decisions*] are applied to each access request prior to access enforcement.

Supplemental Guidance: Access control decisions (also known as authorization decisions) occur when authorization information is applied to specific accesses. In contrast, access enforcement occurs when information systems enforce access control decisions. While it is very common to have access control decisions and access enforcement implemented by the same entity, it is not required and it is not always an optimal implementation choice. For some architectures and distributed information systems, different entities may perform access control decisions and access enforcement.

Control Enhancements:

(1) *ACCESS CONTROL DECISIONS | TRANSMIT ACCESS AUTHORIZATION INFORMATION*

The information system transmits [*Assignment: organization-defined access authorization information*] using [*Assignment: organization-defined security safeguards*] to [*Assignment: organization-defined information systems*] that enforce access control decisions.

Supplemental Guidance: In distributed information systems, authorization processes and access control decisions may occur in separate parts of the systems. In such instances, authorization information is transmitted securely so timely access control decisions can be enforced at the appropriate locations. To support the access control decisions, it may be necessary to transmit as part of the access authorization information, supporting security attributes. This is due to the fact that in distributed information systems, there are various access control decisions that need to be made and different entities (e.g., services) make these decisions in a serial fashion, each requiring some security attributes to make the decisions. Protecting access authorization

information (i.e., access control decisions) ensures that such information cannot be altered, spoofed, or otherwise compromised during transmission.

(2) *ACCESS CONTROL DECISIONS | NO USER OR PROCESS IDENTITY*

The information system enforces access control decisions based on [*Assignment: organization-defined security attributes*] that do not include the identity of the user or process acting on behalf of the user.

Supplemental Guidance: In certain situations, it is important that access control decisions can be made without information regarding the identity of the users issuing the requests. These are generally instances where preserving individual privacy is of paramount importance. In other situations, user identification information is simply not needed for access control decisions and, especially in the case of distributed information systems, transmitting such information with the needed degree of assurance may be very expensive or difficult to accomplish.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

AC-25 REFERENCE MONITOR

Control: The information system implements a reference monitor for [*Assignment: organization-defined access control policies*] that is tamperproof, always invoked, and small enough to be subject to analysis and testing, the completeness of which can be assured.

Supplemental Guidance: Information is represented internally within information systems using abstractions known as data structures. Internal data structures can represent different types of entities, both active and passive. Active entities, also known as *subjects*, are typically associated with individuals, devices, or processes acting on behalf of individuals. Passive entities, also known as *objects*, are typically associated with data structures such as records, buffers, tables, files, inter-process pipes, and communications ports. Reference monitors typically enforce mandatory access control policies—a type of access control that restricts access to objects based on the identity of subjects or groups to which the subjects belong. The access controls are mandatory because subjects with certain privileges (i.e., access permissions) are restricted from passing those privileges on to any other subjects, either directly or indirectly—that is, the information system strictly enforces the access control policy based on the rule set established by the policy. The *tamperproof* property of the reference monitor prevents adversaries from compromising the functioning of the mechanism. The *always invoked* property prevents adversaries from bypassing the mechanism and hence violating the security policy. The *smallness* property helps to ensure the completeness in the analysis and testing of the mechanism to detect weaknesses or deficiencies (i.e., latent flaws) that would prevent the enforcement of the security policy. Related controls: AC-3, AC-16, SC-3, SC-39.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: AWARENESS AND TRAINING

AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

   1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and

b. Reviews and updates the current:

   1. Security awareness and training policy [*Assignment: organization-defined frequency*]; and

   2. Security awareness and training procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AT family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-16, 800-50, 800-100.

Priority and Baseline Allocation:

P1	**LOW** AT-1	**MOD** AT-1	**HIGH** AT-1

AT-2 SECURITY AWARENESS TRAINING

Control: The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):

a. As part of initial training for new users;

b. When required by information system changes; and

c. [*Assignment: organization-defined frequency*] thereafter.

Supplemental Guidance: Organizations determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from

senior organizational officials, displaying logon screen messages, and conducting information security awareness events. Related controls: AT-3, AT-4, PL-4.

Control Enhancements:

(1) *SECURITY AWARENESS | PRACTICAL EXERCISES*

The organization includes practical exercises in security awareness training that simulate actual cyber attacks.

Supplemental Guidance: Practical exercises may include, for example, no-notice social engineering attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking, via spear phishing attacks, malicious web links. Related controls: CA-2, CA-7, CP-4, IR-3.

(2) *SECURITY AWARENESS | INSIDER THREAT*

The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.

Supplemental Guidance: Potential indicators and possible precursors of insider threat can include behaviors such as inordinate, long-term job dissatisfaction, attempts to gain access to information not required for job performance, unexplained access to financial resources, bullying or sexual harassment of fellow employees, workplace violence, and other serious violations of organizational policies, procedures, directives, rules, or practices. Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures. Related controls: PL-4, PM-12, PS-3, PS-6.

References: C.F.R. Part 5 Subpart C (5 C.F.R. 930.301); Executive Order 13587; NIST Special Publication 800-50.

Priority and Baseline Allocation:

P1	**LOW** AT-2	**MOD** AT-2 (2)	**HIGH** AT-2 (2)

AT-3 ROLE-BASED SECURITY TRAINING

Control: The organization provides role-based security training to personnel with assigned security roles and responsibilities:

a. Before authorizing access to the information system or performing assigned duties;

b. When required by information system changes; and

c. [*Assignment: organization-defined frequency*] thereafter.

Supplemental Guidance: Organizations determine the appropriate content of security training based on the assigned roles and responsibilities of individuals and the specific security requirements of organizations and the information systems to which personnel have authorized access. In addition, organizations provide enterprise architects, information system developers, software developers, acquisition/procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training specifically tailored for their assigned duties. Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Such training can include for example, policies, procedures, tools, and artifacts for the organizational security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs. Role-

based security training also applies to contractors providing services to federal agencies. Related controls: AT-2, AT-4, PL-4, PS-7, SA-3, SA-12, SA-16.

Control Enhancements:

(1) *SECURITY TRAINING | ENVIRONMENTAL CONTROLS*

The organization provides [*Assignment: organization-defined personnel or roles*] with initial and [*Assignment: organization-defined frequency*] training in the employment and operation of environmental controls.

Supplemental Guidance: Environmental controls include, for example, fire suppression and detection devices/systems, sprinkler systems, handheld fire extinguishers, fixed fire hoses, smoke detectors, temperature/humidity, HVAC, and power within the facility. Organizations identify personnel with specific roles and responsibilities associated with environmental controls requiring specialized training. Related controls: PE-1, PE-13, PE-14, PE-15.

(2) *SECURITY TRAINING | PHYSICAL SECURITY CONTROLS*

The organization provides [*Assignment: organization-defined personnel or roles*] with initial and [*Assignment: organization-defined frequency*] training in the employment and operation of physical security controls.

Supplemental Guidance: Physical security controls include, for example, physical access control devices, physical intrusion alarms, monitoring/surveillance equipment, and security guards (deployment and operating procedures). Organizations identify personnel with specific roles and responsibilities associated with physical security controls requiring specialized training. Related controls: PE-2, PE-3, PE-4, PE-5.

(3) *SECURITY TRAINING | PRACTICAL EXERCISES*

The organization includes practical exercises in security training that reinforce training objectives.

Supplemental Guidance: Practical exercises may include, for example, security training for software developers that includes simulated cyber attacks exploiting common software vulnerabilities (e.g., buffer overflows), or spear/whale phishing attacks targeted at senior leaders/executives. These types of practical exercises help developers better understand the effects of such vulnerabilities and appreciate the need for security coding standards and processes.

(4) *SECURITY TRAINING | SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR*

The organization provides training to its personnel on [*Assignment: organization-defined indicators of malicious code*] to recognize suspicious communications and anomalous behavior in organizational information systems.

Supplemental Guidance: A well-trained workforce provides another organizational safeguard that can be employed as part of a defense-in-depth strategy to protect organizations against malicious code coming in to organizations via email or the web applications. Personnel are trained to look for indications of potentially suspicious email (e.g., receiving an unexpected email, receiving an email containing strange or poor grammar, or receiving an email from an unfamiliar sender but who appears to be from a known sponsor or contractor). Personnel are also trained on how to respond to such suspicious email or web communications (e.g., not opening attachments, not clicking on embedded web links, and checking the source of email addresses). For this process to work effectively, all organizational personnel are trained and made aware of what constitutes suspicious communications. Training personnel on how to recognize anomalous behaviors in organizational information systems can potentially provide early warning for the presence of malicious code. Recognition of such anomalous behavior by organizational personnel can supplement automated malicious code detection and protection tools and systems employed by organizations.

References: C.F.R. Part 5 Subpart C (5 C.F.R. 930.301); NIST Special Publications 800-16, 800-50.

Priority and Baseline Allocation:

P1	**LOW** AT-3	**MOD** AT-3	**HIGH** AT-3

AT-4 SECURITY TRAINING RECORDS

Control: The organization:

a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and

b. Retains individual training records for [*Assignment: organization-defined time period*].

Supplemental Guidance: Documentation for specialized training may be maintained by individual supervisors at the option of the organization. Related controls: AT-2, AT-3, PM-14.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P3	**LOW** AT-4	**MOD** AT-4	**HIGH** AT-4

AT-5 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS

[Withdrawn: Incorporated into PM-15].

FAMILY: AUDIT AND ACCOUNTABILITY

AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

   1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and

b. Reviews and updates the current:

   1. Audit and accountability policy [*Assignment: organization-defined frequency*]; and

   2. Audit and accountability procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AU family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** AU-1	**MOD** AU-1	**HIGH** AU-1

AU-2 AUDIT EVENTS

Control: The organization:

a. Determines that the information system is capable of auditing the following events: [*Assignment: organization-defined auditable events*];

b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;

c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and

d. Determines that the following events are to be audited within the information system: [*Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event*].

Supplemental Guidance: An event is any observable occurrence in an organizational information system. Organizations identify audit events as those events which are significant and relevant to

the security of information systems and the environments in which those systems operate in order to meet specific and ongoing audit needs. Audit events can include, for example, password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, PIV credential usage, or third-party credential usage. In determining the set of auditable events, organizations consider the auditing appropriate for each of the security controls to be implemented. To balance auditing requirements with other information system needs, this control also requires identifying that subset of *auditable* events that are *audited* at a given point in time. For example, organizations may determine that information systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. Auditing requirements, including the need for auditable events, may be referenced in other security controls and control enhancements. Organizations also include auditable events that are required by applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of auditable events, the auditing necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented architectures. Related controls: AC-6, AC-17, AU-3, AU-12, MA-4, MP-2, MP-4, SI-4.

Control Enhancements:

(1) *AUDIT EVENTS | COMPILATION OF AUDIT RECORDS FROM MULTIPLE SOURCES*

[Withdrawn: Incorporated into AU-12].

(2) *AUDIT EVENTS | SELECTION OF AUDIT EVENTS BY COMPONENT*

[Withdrawn: Incorporated into AU-12].

(3) *AUDIT EVENTS | REVIEWS AND UPDATES*

The organization reviews and updates the audited events [*Assignment: organization-defined frequency*].

Supplemental Guidance: Over time, the events that organizations believe should be audited may change. Reviewing and updating the set of audited events periodically is necessary to ensure that the current set is still necessary and sufficient.

(4) *AUDIT EVENTS | PRIVILEGED FUNCTIONS*

[Withdrawn: Incorporated into AC-6 (9)].

References: NIST Special Publication 800-92; Web: http://idmanagement.gov.

Priority and Baseline Allocation:

P1	**LOW** AU-2	**MOD** AU-2 (3)	**HIGH** AU-2 (3)

AU-3 CONTENT OF AUDIT RECORDS

Control: The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Supplemental Guidance: Audit record content that may be necessary to satisfy the requirement of this control, includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the information system after the event occurred). Related controls: AU-2, AU-8, AU-12, SI-11.

Control Enhancements:

(1) *CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION*

The information system generates audit records containing the following additional information: [*Assignment: organization-defined additional, more detailed information*].

Supplemental Guidance: Detailed information that organizations may consider in audit records includes, for example, full text recording of privileged commands or the individual identities of group account users. Organizations consider limiting the additional audit information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest.

(2) *CONTENT OF AUDIT RECORDS | CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT*

The information system provides centralized management and configuration of the content to be captured in audit records generated by [*Assignment: organization-defined information system components*].

Supplemental Guidance: This control enhancement requires that the content to be captured in audit records be configured from a central location (necessitating automation). Organizations coordinate the selection of required audit content to support the centralized management and configuration capability provided by the information system. Related controls: AU-6, AU-7.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AU-3	**MOD** AU-3 (1)	**HIGH** AU-3 (1) (2)

AU-4 AUDIT STORAGE CAPACITY

Control: The organization allocates audit record storage capacity in accordance with [*Assignment: organization-defined audit record storage requirements*].

Supplemental Guidance: Organizations consider the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Allocating sufficient audit storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of auditing capability. Related controls: AU-2, AU-5, AU-6, AU-7, AU-11, SI-4.

Control Enhancements:

(1) *AUDIT STORAGE CAPACITY | TRANSFER TO ALTERNATE STORAGE*

The information system off-loads audit records [*Assignment: organization-defined frequency*] onto a different system or media than the system being audited.

Supplemental Guidance: Off-loading is a process designed to preserve the confidentiality and integrity of audit records by moving the records from the primary information system to a secondary or alternate system. It is a common process in information systems with limited audit storage capacity; the audit storage is used only in a transitory fashion until the system can communicate with the secondary or alternate system designated for storing the audit records, at which point the information is transferred.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AU-4	**MOD** AU-4	**HIGH** AU-4

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Control: The information system:

a. Alerts [*Assignment: organization-defined personnel or roles*] in the event of an audit processing failure; and

b. Takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].

Supplemental Guidance: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Organizations may choose to define additional actions for different audit processing failures (e.g., by type, by location, by severity, or a combination of such factors). This control applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the total audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both. Related controls: AU-4, SI-12.

Control Enhancements:

(1) *RESPONSE TO AUDIT PROCESSING FAILURES | AUDIT STORAGE CAPACITY*

The information system provides a warning to [*Assignment: organization-defined personnel, roles, and/or locations*] within [*Assignment: organization-defined time period*] when allocated audit record storage volume reaches [*Assignment: organization-defined percentage*] of repository maximum audit record storage capacity.

Supplemental Guidance: Organizations may have multiple audit data storage repositories distributed across multiple information system components, with each repository having different storage volume capacities.

(2) *RESPONSE TO AUDIT PROCESSING FAILURES | REAL-TIME ALERTS*

The information system provides an alert in [*Assignment: organization-defined real-time period*] to [*Assignment: organization-defined personnel, roles, and/or locations*] when the following audit failure events occur: [*Assignment: organization-defined audit failure events requiring real-time alerts*].

Supplemental Guidance: Alerts provide organizations with urgent messages. Real-time alerts provide these messages at information technology speed (i.e., the time from event detection to alert occurs in seconds or less).

(3) *RESPONSE TO AUDIT PROCESSING FAILURES | CONFIGURABLE TRAFFIC VOLUME THRESHOLDS*

The information system enforces configurable network communications traffic volume thresholds reflecting limits on auditing capacity and [*Selection: rejects; delays*] network traffic above those thresholds.

Supplemental Guidance: Organizations have the capability to reject or delay the processing of network communications traffic if auditing such traffic is determined to exceed the storage capacity of the information system audit function. The rejection or delay response is triggered by the established organizational traffic volume thresholds which can be adjusted based on changes to audit storage capacity.

(4) *RESPONSE TO AUDIT PROCESSING FAILURES | SHUTDOWN ON FAILURE*

The information system invokes a [*Selection: full system shutdown; partial system shutdown; degraded operational mode with limited mission/business functionality available*] in the event of [*Assignment: organization-defined audit failures*], unless an alternate audit capability exists.

Supplemental Guidance: Organizations determine the types of audit failures that can trigger automatic information system shutdowns or degraded operations. Because of the importance of ensuring mission/business continuity, organizations may determine that the nature of the audit failure is not so severe that it warrants a complete shutdown of the information system supporting the core organizational missions/business operations. In those instances, partial information system shutdowns or operating in a degraded mode with reduced capability may be viable alternatives. Related control: AU-15.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AU-5	**MOD** AU-5	**HIGH** AU-5 (1) (2)

AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING

Control: The organization:

a. Reviews and analyzes information system audit records [*Assignment: organization-defined frequency*] for indications of [*Assignment: organization-defined inappropriate or unusual activity*]; and

b. Reports findings to [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: Audit review, analysis, and reporting covers information security-related auditing performed by organizations including, for example, auditing that results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, and use of VoIP. Findings can be reported to organizational entities that include, for example, incident response team, help desk, information security group/department. If organizations are prohibited from reviewing and analyzing audit information or unable to conduct such activities (e.g., in certain national security applications or systems), the review/analysis may be carried out by other organizations granted such authority. Related controls: AC-2, AC-3, AC-6, AC-17, AT-3, AU-7, AU-16, CA-7, CM-5, CM-10, CM-11, IA-3, IA-5, IR-5, IR-6, MA-4, MP-4, PE-3, PE-6, PE-14, PE-16, RA-5, SC-7, SC-18, SC-19, SI-3, SI-4, SI-7.

Control Enhancements:

(1) *AUDIT REVIEW, ANALYSIS, AND REPORTING | PROCESS INTEGRATION*

The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

Supplemental Guidance: Organizational processes benefiting from integrated audit review, analysis, and reporting include, for example, incident response, continuous monitoring, contingency planning, and Inspector General audits. Related controls: AU-12, PM-7.

(2) *AUDIT REVIEW, ANALYSIS, AND REPORTING | AUTOMATED SECURITY ALERTS*

[Withdrawn: Incorporated into SI-4].

(3) *AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT REPOSITORIES*

The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

Supplemental Guidance: Organization-wide situational awareness includes awareness across all three tiers of risk management (i.e., organizational, mission/business process, and information system) and supports cross-organization awareness. Related controls: AU-12, IR-4.

(4) *AUDIT REVIEW, ANALYSIS, AND REPORTING | CENTRAL REVIEW AND ANALYSIS*

The information system provides the capability to centrally review and analyze audit records from multiple components within the system.

Supplemental Guidance: Automated mechanisms for centralized reviews and analyses include, for example, Security Information Management products. Related controls: AU-2, AU-12.

(5) *AUDIT REVIEW, ANALYSIS, AND REPORTING | INTEGRATION / SCANNING AND MONITORING CAPABILITIES*

The organization integrates analysis of audit records with analysis of [*Selection (one or more): vulnerability scanning information; performance data; information system monitoring information;* [*Assignment: organization-defined data/information collected from other sources*]] to further enhance the ability to identify inappropriate or unusual activity.

Supplemental Guidance: This control enhancement does not require vulnerability scanning, the generation of performance data, or information system monitoring. Rather, the enhancement requires that the analysis of information being otherwise produced in these areas is integrated with the analysis of audit information. Security Event and Information Management System tools can facilitate audit record aggregation/consolidation from multiple information system components as well as audit record correlation and analysis. The use of standardized audit record analysis scripts developed by organizations (with localized script adjustments, as necessary) provides more cost-effective approaches for analyzing audit record information collected. The correlation of audit record information with vulnerability scanning information is important in determining the veracity of vulnerability scans and correlating attack detection events with scanning results. Correlation with performance data can help uncover denial of service attacks or cyber attacks resulting in unauthorized use of resources. Correlation with system monitoring information can assist in uncovering attacks and in better relating audit information to operational situations. Related controls: AU-12, IR-4, RA-5.

(6) *AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH PHYSICAL MONITORING*

The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

Supplemental Guidance: The correlation of physical audit information and audit logs from information systems may assist organizations in identifying examples of suspicious behavior or supporting evidence of such behavior. For example, the correlation of an individual's identity for logical access to certain information systems with the additional physical security information that the individual was actually present at the facility when the logical access occurred, may prove to be useful in investigations.

(7) *AUDIT REVIEW, ANALYSIS, AND REPORTING | PERMITTED ACTIONS*

The organization specifies the permitted actions for each [*Selection (one or more): information system process; role; user*] associated with the review, analysis, and reporting of audit information.

Supplemental Guidance: Organizations specify permitted actions for information system processes, roles, and/or users associated with the review, analysis, and reporting of audit records through account management techniques. Specifying permitted actions on audit information is a way to enforce the principle of least privilege. Permitted actions are enforced by the information system and include, for example, read, write, execute, append, and delete.

(8) *AUDIT REVIEW, ANALYSIS, AND REPORTING | FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS*

The organization performs a full text analysis of audited privileged commands in a physically distinct component or subsystem of the information system, or other information system that is dedicated to that analysis.

Supplemental Guidance: This control enhancement requires a distinct environment for the dedicated analysis of audit information related to privileged users without compromising such information on the information system where the users have elevated privileges including the capability to execute privileged commands. Full text analysis refers to analysis that considers the full text of privileged commands (i.e., commands and all parameters) as opposed to analysis that considers only the name of the command. Full text analysis includes, for example, the use of pattern matching and heuristics. Related controls: AU-3, AU-9, AU-11, AU-12.

(9) *AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH INFORMATION FROM NONTECHNICAL SOURCES*

The organization correlates information from nontechnical sources with audit information to enhance organization-wide situational awareness.

Supplemental Guidance: Nontechnical sources include, for example, human resources records documenting organizational policy violations (e.g., sexual harassment incidents, improper use of organizational information assets). Such information can lead organizations to a more directed analytical effort to detect potential malicious insider activity. Due to the sensitive nature of the information available from nontechnical sources, organizations limit access to such information to minimize the potential for the inadvertent release of privacy-related information to individuals that do not have a need to know. Thus, correlation of information

from nontechnical sources with audit information generally occurs only when individuals are suspected of being involved in a security incident. Organizations obtain legal advice prior to initiating such actions. Related control: AT-2.

(10) *AUDIT REVIEW, ANALYSIS, AND REPORTING | AUDIT LEVEL ADJUSTMENT*

The organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

Supplemental Guidance: The frequency, scope, and/or depth of the audit review, analysis, and reporting may be adjusted to meet organizational needs based on new information received.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AU-6	**MOD** AU-6 (1) (3)	**HIGH** AU-6 (1) (3) (5) (6)

AU-7 AUDIT REDUCTION AND REPORT GENERATION

Control: The information system provides an audit reduction and report generation capability that:

a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and

b. Does not alter the original content or time ordering of audit records.

Supplemental Guidance: Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Audit reduction and report generation capabilities do not always emanate from the same information system or from the same organizational entities conducting auditing activities. Audit reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the information system can generate customizable reports. Time ordering of audit records can be a significant issue if the granularity of the timestamp in the record is insufficient. Related control: AU-6.

Control Enhancements:

(1) *AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING*

The information system provides the capability to process audit records for events of interest based on [*Assignment: organization-defined audit fields within audit records*].

Supplemental Guidance: Events of interest can be identified by the content of specific audit record fields including, for example, identities of individuals, event types, event locations, event times, event dates, system resources involved, IP addresses involved, or information objects accessed. Organizations may define audit event criteria to any degree of granularity required, for example, locations selectable by general networking location (e.g., by network or subnetwork) or selectable by specific information system component. Related controls: AU-2, AU-12.

(2) *AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC SORT AND SEARCH*

The information system provides the capability to sort and search audit records for events of interest based on the content of [*Assignment: organization-defined audit fields within audit records*].

Supplemental Guidance: Sorting and searching of audit records may be based upon the contents of audit record fields, for example: (i) date/time of events; (ii) user identifiers; (iii) Internet Protocol (IP) addresses involved in the event; (iv) type of event; or (v) event success/failure.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** AU-7 (1)	**HIGH** AU-7 (1)

AU-8 TIME STAMPS

Control: The information system:

a. Uses internal system clocks to generate time stamps for audit records; and

b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [*Assignment: organization-defined granularity of time measurement*].

Supplemental Guidance: Time stamps generated by the information system include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. Granularity of time measurements refers to the degree of synchronization between information system clocks and reference clocks, for example, clocks synchronizing within hundreds of milliseconds or within tens of milliseconds. Organizations may define different time granularities for different system components. Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities. Related controls: AU-3, AU-12.

Control Enhancements:

(1) *TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE*

The information system:

(a) Compares the internal information system clocks [*Assignment: organization-defined frequency*] with [*Assignment: organization-defined authoritative time source*]; and

(b) Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than [*Assignment: organization-defined time period*].

Supplemental Guidance: This control enhancement provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

(2) *TIME STAMPS | SECONDARY AUTHORITATIVE TIME SOURCE*

The information system identifies a secondary authoritative time source that is located in a different geographic region than the primary authoritative time source.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AU-8	**MOD** AU-8 (1)	**HIGH** AU-8 (1)

AU-9 PROTECTION OF AUDIT INFORMATION

Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Supplemental Guidance: Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity. This control focuses on technical protection of audit information. Physical protection of audit information is addressed by media protection controls and physical and environmental protection controls. Related controls: AC-3, AC-6, MP-2, MP-4, PE-2, PE-3, PE-6.

Control Enhancements:

(1) *PROTECTION OF AUDIT INFORMATION | HARDWARE WRITE-ONCE* MEDIA

The information system writes audit trails to hardware-enforced, write-once media.

Supplemental Guidance: This control enhancement applies to the initial generation of audit trails (i.e., the collection of audit records that represents the audit information to be used for detection, analysis, and reporting purposes) and to the backup of those audit trails. The enhancement does not apply to the initial generation of audit records prior to being written to an audit trail. Write-once, read-many (WORM) media includes, for example, Compact Disk-Recordable (CD-R) and Digital Video Disk-Recordable (DVD-R). In contrast, the use of switchable write-protection media such as on tape cartridges or Universal Serial Bus (USB) drives results in write-protected, but not write-once, media. Related controls: AU-4, AU-5.

(2) *PROTECTION OF AUDIT INFORMATION | AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS*

The information system backs up audit records [*Assignment: organization-defined frequency*] onto a physically different system or system component than the system or component being audited.

Supplemental Guidance: This control enhancement helps to ensure that a compromise of the information system being audited does not also result in a compromise of the audit records. Related controls: AU-4, AU-5, AU-11.

(3) *PROTECTION OF AUDIT INFORMATION | CRYPTOGRAPHIC PROTECTION*

The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools.

Supplemental Guidance: Cryptographic mechanisms used for protecting the integrity of audit information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash. Related controls: AU-10, SC-12, SC-13.

(4) *PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS*

The organization authorizes access to management of audit functionality to only [*Assignment: organization-defined subset of privileged users*].

Supplemental Guidance: Individuals with privileged access to an information system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit activities or modifying audit records. This control enhancement requires that privileged access be further defined between audit-related privileges and other privileges, thus limiting the users with audit-related privileges. Related control: AC-5.

(5) *PROTECTION OF AUDIT INFORMATION | DUAL AUTHORIZATION*

The organization enforces dual authorization for [*Selection (one or more): movement; deletion*] of [*Assignment: organization-defined audit information*].

Supplemental Guidance: Organizations may choose different selection options for different types of audit information. Dual authorization mechanisms require the approval of two authorized individuals in order to execute. Dual authorization may also be known as two-person control. Related controls: AC-3, MP-2.

(6) *PROTECTION OF AUDIT INFORMATION | READ ONLY ACCESS*

The organization authorizes read-only access to audit information to [*Assignment: organization-defined subset of privileged users*].

Supplemental Guidance: Restricting privileged user authorizations to read-only helps to limit the potential damage to organizations that could be initiated by such users (e.g., deleting audit records to cover up malicious activity).

References: None.

Priority and Baseline Allocation:

P1	**LOW** AU-9	**MOD** AU-9 (4)	**HIGH** AU-9 (2) (3) (4)

AU-10 NON-REPUDIATION

Control: The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed [*Assignment: organization-defined actions to be covered by non-repudiation*].

Supplemental Guidance: Types of individual actions covered by non-repudiation include, for example, creating information, sending and receiving messages, approving information (e.g., indicating concurrence or signing a contract). Non-repudiation protects individuals against later claims by: (i) authors of not having authored particular documents; (ii) senders of not having transmitted messages; (iii) receivers of not having received messages; or (iv) signatories of not having signed documents. Non-repudiation services can be used to determine if information originated from a particular individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Organizations obtain non-repudiation services by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts). Related controls: SC-12, SC-8, SC-13, SC-16, SC-17, SC-23.

Control Enhancements:

(1) *NON-REPUDIATION | ASSOCIATION OF IDENTITIES*

The information system:

(a) Binds the identity of the information producer with the information to [*Assignment: organization-defined strength of binding*]; and

(b) Provides the means for authorized individuals to determine the identity of the producer of the information.

Supplemental Guidance: This control enhancement supports audit requirements that provide organizational personnel with the means to identify who produced specific information in the event of an information transfer. Organizations determine and approve the strength of the binding between the information producer and the information based on the security category of the information and relevant risk factors. Related controls: AC-4, AC-16.

(2) *NON-REPUDIATION | VALIDATE BINDING OF INFORMATION PRODUCER IDENTITY*

The information system:

(a) Validates the binding of the information producer identity to the information at [*Assignment: organization-defined frequency*]; and

(b) Performs [*Assignment: organization-defined actions*] in the event of a validation error.

Supplemental Guidance: This control enhancement prevents the modification of information between production and review. The validation of bindings can be achieved, for example, by the use of cryptographic checksums. Organizations determine if validations are in response to user requests or generated automatically. Related controls: AC-3, AC-4, AC-16.

(3) *NON-REPUDIATION | CHAIN OF CUSTODY*

The information system maintains reviewer/releaser identity and credentials within the established chain of custody for all information reviewed or released.

Supplemental Guidance: Chain of custody is a process that tracks the movement of evidence through its collection, safeguarding, and analysis life cycle by documenting each person who handled the evidence, the date and time it was collected or transferred, and the purpose for the transfer. If the reviewer is a human or if the review function is automated but separate from the release/transfer function, the information system associates the identity of the reviewer of the information to be released with the information and the information label. In the case of human reviews, this control enhancement provides organizational officials the means to identify who reviewed and released the information. In the case of automated reviews, this control enhancement ensures that only approved review functions are employed. Related controls: AC-4, AC-16.

(4) *NON-REPUDIATION | VALIDATE BINDING OF INFORMATION REVIEWER IDENTITY*

The information system:

(a) Validates the binding of the information reviewer identity to the information at the transfer or release points prior to release/transfer between [*Assignment: organization-defined security domains*]; and

(b) Performs [*Assignment: organization-defined actions*] in the event of a validation error.

Supplemental Guidance: This control enhancement prevents the modification of information between review and transfer/release. The validation of bindings can be achieved, for example, by the use of cryptographic checksums. Organizations determine validations are in response to user requests or generated automatically. Related controls: AC-4, AC-16.

(5) *NON-REPUDIATION | DIGITAL SIGNATURES*

[Withdrawn: Incorporated into SI-7].

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** Not Selected	**HIGH** AU-10

AU-11 AUDIT RECORD RETENTION

Control: The organization retains audit records for [*Assignment: organization-defined time period consistent with records retention policy*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Supplemental Guidance: Organizations retain audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action. The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on record retention. Related controls: AU-4, AU-5, AU-9, MP-6.

Control Enhancements:

(1) *AUDIT RECORD RETENTION | LONG-TERM RETRIEVAL CAPABILITY*

The organization employs [*Assignment: organization-defined measures*] to ensure that long-term audit records generated by the information system can be retrieved.

Supplemental Guidance: Measures employed by organizations to help facilitate the retrieval of audit records include, for example, converting records to newer formats, retaining equipment capable of reading the records, and retaining necessary documentation to help organizational personnel understand how to interpret the records.

References: None.

Priority and Baseline Allocation:

P3	**LOW** AU-11	**MOD** AU-11	**HIGH** AU-11

AU-12 AUDIT GENERATION

Control: The information system:

a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [*Assignment: organization-defined information system components*];

b. Allows [*Assignment: organization-defined personnel or roles*] to select which auditable events are to be audited by specific components of the information system; and

c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

Supplemental Guidance: Audit records can be generated from many different information system components. The list of audited events is the set of events for which audits are to be generated. These events are typically a subset of all events for which the information system is capable of generating audit records. Related controls: AC-3, AU-2, AU-3, AU-6, AU-7.

Control Enhancements:

(1) *AUDIT GENERATION | SYSTEM-WIDE / TIME-CORRELATED AUDIT TRAIL*

The information system compiles audit records from [*Assignment: organization-defined information system components*] into a system-wide (logical or physical) audit trail that is time-correlated to within [*Assignment: organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail*].

Supplemental Guidance: Audit trails are time-correlated if the time stamps in the individual audit records can be reliably related to the time stamps in other audit records to achieve a time ordering of the records within organizational tolerances. Related controls: AU-8, AU-12.

(2) *AUDIT GENERATION | STANDARDIZED FORMATS*

The information system produces a system-wide (logical or physical) audit trail composed of audit records in a standardized format.

Supplemental Guidance: Audit information that is normalized to common standards promotes interoperability and exchange of such information between dissimilar devices and information systems. This facilitates production of event information that can be more readily analyzed and correlated. Standard formats for audit records include, for example, system log records and audit records compliant with Common Event Expressions (CEE). If logging mechanisms within information systems do not conform to standardized formats, systems may convert individual audit records into standardized formats when compiling system-wide audit trails.

(3) *AUDIT GENERATION | CHANGES BY AUTHORIZED INDIVIDUALS*

The information system provides the capability for [*Assignment: organization-defined individuals or roles*] to change the auditing to be performed on [*Assignment: organization-defined information system components*] based on [*Assignment: organization-defined selectable event criteria*] within [*Assignment: organization-defined time thresholds*].

Supplemental Guidance: This control enhancement enables organizations to extend or limit auditing as necessary to meet organizational requirements. Auditing that is limited to conserve information system resources may be extended to address certain threat situations. In addition, auditing may be limited to a specific set of events to facilitate audit reduction, analysis, and reporting. Organizations can establish time thresholds in which audit actions are changed, for example, near real-time, within minutes, or within hours. Related control: AU-7.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AU-12	**MOD** AU-12	**HIGH** AU-12 (1) (3)

AU-13 MONITORING FOR INFORMATION DISCLOSURE

Control: The organization monitors [*Assignment: organization-defined open source information and/or information sites*] [*Assignment: organization-defined frequency*] for evidence of unauthorized disclosure of organizational information.

Supplemental Guidance: Open source information includes, for example, social networking sites. Related controls: PE-3, SC-7.

Control Enhancements:

(1) *MONITORING FOR INFORMATION DISCLOSURE | USE OF AUTOMATED TOOLS*

The organization employs automated mechanisms to determine if organizational information has been disclosed in an unauthorized manner.

Supplemental Guidance: Automated mechanisms can include, for example, automated scripts to monitor new posts on selected websites, and commercial services providing notifications and alerts to organizations.

(2) *MONITORING FOR INFORMATION DISCLOSURE | REVIEW OF MONITORED SITES*

The organization reviews the open source information sites being monitored [*Assignment: organization-defined frequency*].

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

AU-14 SESSION AUDIT

Control: The information system provides the capability for authorized users to select a user session to capture/record or view/hear.

Supplemental Guidance: Session audits include, for example, monitoring keystrokes, tracking websites visited, and recording information and/or file transfers. Session auditing activities are developed, integrated, and used in consultation with legal counsel in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, or standards. Related controls: AC-3, AU-4, AU-5, AU-9, AU-11.

Control Enhancements:

(1) *SESSION AUDIT | SYSTEM START-UP*

The information system initiates session audits at system start-up.

(2) *SESSION AUDIT | CAPTURE/RECORD AND LOG CONTENT*

The information system provides the capability for authorized users to capture/record and log content related to a user session.

(3) *SESSION AUDIT | REMOTE VIEWING / LISTENING*

The information system provides the capability for authorized users to remotely view/hear all content related to an established user session in real time.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

AU-15 ALTERNATE AUDIT CAPABILITY

Control: The organization provides an alternate audit capability in the event of a failure in primary audit capability that provides [*Assignment: organization-defined alternate audit functionality*].

Supplemental Guidance: Since an alternate audit capability may be a short-term protection employed until the failure in the primary auditing capability is corrected, organizations may determine that the alternate audit capability need only provide a subset of the primary audit functionality that is impacted by the failure. Related control: AU-5.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

AU-16 CROSS-ORGANIZATIONAL AUDITING

Control: The organization employs [*Assignment: organization-defined methods*] for coordinating [*Assignment: organization-defined audit information*] among external organizations when audit information is transmitted across organizational boundaries.

Supplemental Guidance: When organizations use information systems and/or services of external organizations, the auditing capability necessitates a coordinated approach across organizations. For example, maintaining the identity of individuals that requested particular services across organizational boundaries may often be very difficult, and doing so may prove to have significant performance ramifications. Therefore, it is often the case that cross-organizational auditing (e.g., the type of auditing capability provided by service-oriented architectures) simply captures the identity of individuals issuing requests at the initial information system, and subsequent systems record that the requests emanated from authorized individuals. Related control: AU-6.

Control Enhancements:

(1) *CROSS-ORGANIZATIONAL AUDITING | IDENTITY PRESERVATION*

The organization requires that the identity of individuals be preserved in cross-organizational audit trails.

Supplemental Guidance: This control enhancement applies when there is a need to be able to trace actions that are performed across organizational boundaries to a specific individual.

(2) *CROSS-ORGANIZATIONAL AUDITING | SHARING OF AUDIT INFORMATION*

The organization provides cross-organizational audit information to [*Assignment: organization-defined organizations*] based on [*Assignment: organization-defined cross-organizational sharing agreements*].

Supplemental Guidance: Because of the distributed nature of the audit information, cross-organization sharing of audit information may be essential for effective analysis of the auditing being performed. For example, the audit records of one organization may not provide sufficient information to determine the appropriate or inappropriate use of organizational information resources by individuals in other organizations. In some instances, only the home organizations of individuals have the appropriate knowledge to make such determinations, thus requiring the sharing of audit information among organizations.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: SECURITY ASSESSMENT AND AUTHORIZATION

CA-1 SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and

b. Reviews and updates the current:

1. Security assessment and authorization policy [*Assignment: organization-defined frequency*]; and

2. Security assessment and authorization procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-37, 800-53A, 800-100.

Priority and Baseline Allocation:

P1	**LOW** CA-1	**MOD** CA-1	**HIGH** CA-1

CA-2 SECURITY ASSESSMENTS

Control: The organization:

a. Develops a security assessment plan that describes the scope of the assessment including:

1. Security controls and control enhancements under assessment;

2. Assessment procedures to be used to determine security control effectiveness; and

3. Assessment environment, assessment team, and assessment roles and responsibilities;

b. Assesses the security controls in the information system and its environment of operation [*Assignment: organization-defined frequency*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;

c. Produces a security assessment report that documents the results of the assessment; and

d. Provides the results of the security control assessment to [*Assignment: organization-defined individuals or roles*].

Supplemental Guidance: Organizations assess security controls in organizational information systems and the environments in which those systems operate as part of: (i) initial and ongoing security authorizations; (ii) FISMA annual assessments; (iii) continuous monitoring; and (iv) system development life cycle activities. Security assessments: (i) ensure that information security is built into organizational information systems; (ii) identify weaknesses and deficiencies early in the development process; (iii) provide essential information needed to make risk-based decisions as part of security authorization processes; and (iv) ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls from Appendix F (main catalog) and Appendix G (Program Management controls) as documented in System Security Plans and Information Security Program Plans. Organizations can use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of information systems during the entire life cycle. Security assessment reports document assessment results in sufficient detail as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. The FISMA requirement for assessing security controls at least annually does not require additional assessment activities to those activities already in place in organizational security authorization processes. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of security authorization decisions are provided to authorizing officials or authorizing official designated representatives.

To satisfy annual assessment requirements, organizations can use assessment results from the following sources: (i) initial or ongoing information system authorizations; (ii) continuous monitoring; or (iii) system development life cycle activities. Organizations ensure that security assessment results are current, relevant to the determination of security control effectiveness, and obtained with the appropriate level of assessor independence. Existing security control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. Subsequent to initial authorizations and in accordance with OMB policy, organizations assess security controls during continuous monitoring. Organizations establish the frequency for ongoing security control assessments in accordance with organizational continuous monitoring strategies. Information Assurance Vulnerability Alerts provide useful examples of vulnerability mitigation procedures. External audits (e.g., audits by external entities such as regulatory agencies) are outside the scope of this control. Related controls: CA-5, CA-6, CA-7, PM-9, RA-5, SA-11, SA-12, SI-4.

Control Enhancements:

(1) *SECURITY ASSESSMENTS | INDEPENDENT ASSESSORS*

The organization employs assessors or assessment teams with [*Assignment: organization-defined level of independence*] to conduct security control assessments.

Supplemental Guidance: Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of organizational information systems. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the organizational information systems under assessment or to the determination of security control effectiveness. To achieve impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in positions of advocacy for the organizations acquiring their services. Independent assessments can be obtained from elements within organizations or can be contracted to public or private sector entities outside of organizations. Authorizing officials determine the required level of independence based on the security categories of information systems and/or the ultimate risk to organizational operations, organizational assets, or individuals. Authorizing officials also determine if the level of assessor independence provides sufficient assurance that the results

are sound and can be used to make credible, risk-based decisions. This includes determining whether contracted security assessment services have sufficient independence, for example, when information system owners are not directly involved in contracting processes or cannot unduly influence the impartiality of assessors conducting assessments. In special situations, for example, when organizations that own the information systems are small or organizational structures require that assessments are conducted by individuals that are in the developmental, operational, or management chain of system owners, independence in assessment processes can be achieved by ensuring that assessment results are carefully reviewed and analyzed by independent teams of experts to validate the completeness, accuracy, integrity, and reliability of the results. Organizations recognize that assessments performed for purposes other than direct support to authorization decisions are, when performed by assessors with sufficient independence, more likely to be useable for such decisions, thereby reducing the need to repeat assessments.

(2) *SECURITY ASSESSMENTS | SPECIALIZED ASSESSMENTS*

The organization includes as part of security control assessments, [*Assignment: organization-defined frequency*], [*Selection: announced; unannounced*], [*Selection (one or more): in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing;* [*Assignment: organization-defined other forms of security assessment*]].

Supplemental Guidance: Organizations can employ information system monitoring, insider threat assessments, malicious user testing, and other forms of testing (e.g., verification and validation) to improve readiness by exercising organizational capabilities and indicating current performance levels as a means of focusing actions to improve security. Organizations conduct assessment activities in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Authorizing officials approve the assessment methods in coordination with the organizational risk executive function. Organizations can incorporate vulnerabilities uncovered during assessments into vulnerability remediation processes. Related controls: PE-3, SI-2.

(3) *SECURITY ASSESSMENTS | EXTERNAL ORGANIZATIONS*

The organization accepts the results of an assessment of [*Assignment: organization-defined information system*] performed by [*Assignment: organization-defined external organization*] when the assessment meets [*Assignment: organization-defined requirements*].

Supplemental Guidance: Organizations may often rely on assessments of specific information systems by other (external) organizations. Utilizing such existing assessments (i.e., reusing existing assessment evidence) can significantly decrease the time and resources required for organizational assessments by limiting the amount of independent assessment activities that organizations need to perform. The factors that organizations may consider in determining whether to accept assessment results from external organizations can vary. Determinations for accepting assessment results can be based on, for example, past assessment experiences one organization has had with another organization, the reputation that organizations have with regard to assessments, the level of detail of supporting assessment documentation provided, or mandates imposed upon organizations by federal legislation, policies, or directives.

References: Executive Order 13587; FIPS Publication 199; NIST Special Publications 800-37, 800-39, 800-53A, 800-115, 800-137.

Priority and Baseline Allocation:

P2	**LOW** CA-2	**MOD** CA-2 (1)	**HIGH** CA-2 (1) (2)

CA-3 SYSTEM INTERCONNECTIONS

Control: The organization:

a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;

b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and

c. Reviews and updates Interconnection Security Agreements [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control applies to dedicated connections between information systems (i.e., system interconnections) and does not apply to transitory, user-controlled connections such as email and website browsing. Organizations carefully consider the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within organizations and external to organizations. Authorizing officials determine the risk associated with information system connections and the appropriate controls employed. If interconnecting systems have the same authorizing official, organizations do not need to develop Interconnection Security Agreements. Instead, organizations can describe the interface characteristics between those interconnecting systems in their respective security plans. If interconnecting systems have different authorizing officials within the same organization, organizations can either develop Interconnection Security Agreements or describe the interface characteristics between systems in the security plans for the respective systems. Organizations may also incorporate Interconnection Security Agreement information into formal contracts, especially for interconnections established between federal agencies and nonfederal (i.e., private sector) organizations. Risk considerations also include information systems sharing the same networks. For certain technologies (e.g., space, unmanned aerial vehicles, and medical devices), there may be specialized connections in place during preoperational testing. Such connections may require Interconnection Security Agreements and be subject to additional security controls. Related controls: AC-3, AC-4, AC-20, AU-2, AU-12, AU-16, CA-7, IA-3, SA-9, SC-7, SI-4.

Control Enhancements:

(1) *SYSTEM INTERCONNECTIONS | UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS*

The organization prohibits the direct connection of an [*Assignment: organization-defined unclassified, national security system*] to an external network without the use of [*Assignment: organization-defined boundary protection device*].

Supplemental Guidance: Organizations typically do not have control over external networks (e.g., the Internet). Approved boundary protection devices (e.g., routers, firewalls) mediate communications (i.e., information flows) between unclassified national security systems and external networks. This control enhancement is required for organizations processing, storing, or transmitting Controlled Unclassified Information (CUI).

(2) *SYSTEM INTERCONNECTIONS | CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS*

The organization prohibits the direct connection of a classified, national security system to an external network without the use of [*Assignment: organization-defined boundary protection device*].

Supplemental Guidance: Organizations typically do not have control over external networks (e.g., the Internet). Approved boundary protection devices (e.g., routers, firewalls) mediate communications (i.e., information flows) between classified national security systems and external networks. In addition, approved boundary protection devices (typically managed interface/cross-domain systems) provide information flow enforcement from information systems to external networks.

(3) *SYSTEM INTERCONNECTIONS | UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS*

The organization prohibits the direct connection of an [*Assignment: organization-defined unclassified, non-national security system*] to an external network without the use of [*Assignment; organization-defined boundary protection device*].

Supplemental Guidance: Organizations typically do not have control over external networks (e.g., the Internet). Approved boundary protection devices (e.g., routers, firewalls) mediate communications (i.e., information flows) between unclassified non-national security systems and external networks. This control enhancement is required for organizations processing, storing, or transmitting Controlled Unclassified Information (CUI).

(4) *SYSTEM INTERCONNECTIONS | CONNECTIONS TO PUBLIC NETWORKS*

The organization prohibits the direct connection of an [*Assignment: organization-defined information system*] to a public network.

Supplemental Guidance: A public network is any network accessible to the general public including, for example, the Internet and organizational extranets with public access.

(5) *SYSTEM INTERCONNECTIONS | RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS*

The organization employs [*Selection: allow-all, deny-by-exception; deny-all, permit-by-exception*] policy for allowing [*Assignment: organization-defined information systems*] to connect to external information systems.

Supplemental Guidance: Organizations can constrain information system connectivity to external domains (e.g., websites) by employing one of two policies with regard to such connectivity: (i) allow-all, deny by exception, also known as *blacklisting* (the weaker of the two policies); or (ii) deny-all, allow by exception, also known as *whitelisting* (the stronger of the two policies). For either policy, organizations determine what exceptions, if any, are acceptable. Related control: CM-7.

References: FIPS Publication 199; NIST Special Publication 800-47.

Priority and Baseline Allocation:

P1	**LOW** CA-3	**MOD** CA-3 (5)	**HIGH** CA-3 (5)

CA-4 SECURITY CERTIFICATION

[Withdrawn: Incorporated into CA-2].

CA-5 PLAN OF ACTION AND MILESTONES

Control: The organization:

a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and

b. Updates existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Supplemental Guidance: Plans of action and milestones are key documents in security authorization packages and are subject to federal reporting requirements established by OMB. Related controls: CA-2, CA-7, CM-4, PM-4.

Control Enhancements:

(1) *PLAN OF ACTION AND MILESTONES | AUTOMATION SUPPORT FOR ACCURACY / CURRENCY*

The organization employs automated mechanisms to help ensure that the plan of action and milestones for the information system is accurate, up to date, and readily available.

References: OMB Memorandum 02-01; NIST Special Publication 800-37.

Priority and Baseline Allocation:

P3	**LOW** CA-5	**MOD** CA-5	**HIGH** CA-5

CA-6 SECURITY AUTHORIZATION

Control: The organization:

a. Assigns a senior-level executive or manager as the authorizing official for the information system;

b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and

c. Updates the security authorization [*Assignment: organization-defined frequency*].

Supplemental Guidance: Security authorizations are official management decisions, conveyed through authorization decision documents, by senior organizational officials or executives (i.e., authorizing officials) to authorize operation of information systems and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of agreed-upon security controls. Authorizing officials provide budgetary oversight for organizational information systems or assume responsibility for the mission/business operations supported by those systems. The security authorization process is an inherently federal responsibility and therefore, authorizing officials must be federal employees. Through the security authorization process, authorizing officials assume responsibility and are accountable for security risks associated with the operation and use of organizational information systems. Accordingly, authorizing officials are in positions with levels of authority commensurate with understanding and accepting such information security-related risks. OMB policy requires that organizations conduct ongoing authorizations of information systems by implementing continuous monitoring programs. Continuous monitoring programs can satisfy three-year reauthorization requirements, so separate reauthorization processes are not necessary. Through the employment of comprehensive continuous monitoring processes, critical information contained in authorization packages (i.e., security plans, security assessment reports, and plans of action and milestones) is updated on an ongoing basis, providing authorizing officials and information system owners with an up-to-date status of the security state of organizational information systems and environments of operation. To reduce the administrative cost of security reauthorization, authorizing officials use the results of continuous monitoring processes to the maximum extent possible as the basis for rendering reauthorization decisions. Related controls: CA-2, CA-7, PM-9, PM-10.

Control Enhancements: None.

References: OMB Circular A-130; OMB Memorandum 11-33; NIST Special Publications 800-37, 800-137.

Priority and Baseline Allocation:

P2	**LOW** CA-6	**MOD** CA-6	**HIGH** CA-6

CA-7 CONTINUOUS MONITORING

Control: The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

a. Establishment of [*Assignment: organization-defined metrics*] to be monitored;

b. Establishment of [*Assignment: organization-defined freq*uencies] for monitoring and [*Assignment: organization-defined freq*uencies] for assessments supporting such monitoring;

c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;

d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;

e. Correlation and analysis of security-related information generated by assessments and monitoring;

f. Response actions to address results of the analysis of security-related information; and

g. Reporting the security status of organization and the information system to [*Assignment: organization-defined personnel or roles*] [*Assignment: organization-defined frequency*].

Supplemental Guidance: Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms *continuous* and *ongoing* imply that organizations assess/analyze security controls and information security-related risks at a frequency sufficient to support organizational risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Continuous monitoring programs also allow organizations to maintain the security authorizations of information systems and common controls over time in highly dynamic environments of operation with changing mission/business needs, threats, vulnerabilities, and technologies. Having access to security-related information on a continuing basis through reports/dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions. Automation supports more frequent updates to security authorization packages, hardware/software/firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of information systems. Related controls: CA-2, CA-5, CA-6, CM-3, CM-4, PM-6, PM-9, RA-5, SA-11, SA-12, SI-2, SI-4.

Control Enhancements:

(1) *CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT*

The organization employs assessors or assessment teams with [*Assignment: organization-defined level of independence*] to monitor the security controls in the information system on an ongoing basis.

Supplemental Guidance: Organizations can maximize the value of assessments of security controls during the continuous monitoring process by requiring that such assessments be conducted by assessors or assessment teams with appropriate levels of independence based on continuous monitoring strategies. Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in advocacy positions for the organizations acquiring their services.

(2) *CONTINUOUS MONITORING | TYPES OF ASSESSMENTS*

[Withdrawn: Incorporated into CA-2.]

(3) *CONTINUOUS MONITORING | TREND ANALYSES*

The organization employs trend analyses to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data.

Supplemental Guidance: Trend analyses can include, for example, examining recent threat information regarding the types of threat events that have occurred within the organization or across the federal government, success rates of certain types of cyber attacks, emerging vulnerabilities in information technologies, evolving social engineering techniques, results from multiple security control assessments, the effectiveness of configuration settings, and findings from Inspectors General or auditors.

References: OMB Memorandum 11-33; NIST Special Publications 800-37, 800-39, 800-53A, 800-115, 800-137; US-CERT Technical Cyber Security Alerts; DoD Information Assurance Vulnerability Alerts.

Priority and Baseline Allocation:

P2	**LOW** CA-7	**MOD** CA-7 (1)	**HIGH** CA-7 (1)

CA-8 PENETRATION TESTING

Control: The organization conducts penetration testing [*Assignment: organization-defined frequency*] on [*Assignment: organization-defined information systems or system components*].

Supplemental Guidance: Penetration testing is a specialized type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Such testing can be used to either validate vulnerabilities or determine the degree of resistance organizational information systems have to adversaries within a set of specified constraints (e.g., time, resources, and/or skills). Penetration testing attempts to duplicate the actions of adversaries in carrying out hostile cyber attacks against organizations and provides a more in-depth analysis of security-related weaknesses/deficiencies. Organizations can also use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted on the hardware, software, or firmware components of an information system and can exercise both physical and technical security controls. A standard method for penetration testing includes, for example: (i) pretest analysis based on full knowledge of the target system; (ii) pretest identification of potential vulnerabilities based on pretest analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. All parties agree to the rules of engagement before the commencement of penetration testing scenarios. Organizations correlate the penetration testing rules of engagement with the tools, techniques, and procedures that are anticipated to be employed by adversaries carrying out attacks. Organizational risk assessments guide decisions on the level of independence required for personnel conducting penetration testing. Related control: SA-12.

Control Enhancements:

(1) *PENETRATION TESTING | INDEPENDENT PENETRATION AGENT OR TEAM*

The organization employs an independent penetration agent or penetration team to perform penetration testing on the information system or system components.

Supplemental Guidance: Independent penetration agents or teams are individuals or groups who conduct impartial penetration testing of organizational information systems. Impartiality implies that penetration agents or teams are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the information systems that are the targets of the penetration testing. Supplemental guidance for CA-2 (1) provides additional information regarding independent assessments that can be applied to penetration testing. Related control: CA-2.

(2) *PENETRATION TESTING | RED TEAM EXERCISES*

The organization employs [*Assignment: organization-defined red team exercises*] to simulate attempts by adversaries to compromise organizational information systems in accordance with [*Assignment: organization-defined rules of engagement*].

Supplemental Guidance: Red team exercises extend the objectives of penetration testing by examining the security posture of organizations and their ability to implement effective cyber defenses. As such, red team exercises reflect simulated adversarial attempts to compromise organizational mission/business functions and provide a comprehensive assessment of the security state of information systems and organizations. Simulated adversarial attempts to compromise organizational missions/business functions and the information systems that support those missions/functions may include technology-focused attacks (e.g., interactions with hardware, software, or firmware components and/or mission/business processes) and social engineering-based attacks (e.g., interactions via email, telephone, shoulder surfing, or personal conversations). While penetration testing may be largely laboratory-based testing, organizations use red team exercises to provide more comprehensive assessments that reflect

real-world conditions. Red team exercises can be used to improve security awareness and training and to assess levels of security control effectiveness.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** Not Selected	**HIGH** CA-8

CA-9 INTERNAL SYSTEM CONNECTIONS

Control: The organization:

a. Authorizes internal connections of [*Assignment: organization-defined information system components or classes of components*] to the information system; and

b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

Supplemental Guidance: This control applies to connections between organizational information systems and (separate) constituent system components (i.e., intra-system connections) including, for example, system connections with mobile devices, notebook/desktop computers, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each individual internal connection, organizations can authorize internal connections for a class of components with common characteristics and/or configurations, for example, all digital printers, scanners, and copiers with a specified processing, storage, and transmission capability or all smart phones with a specific baseline configuration. Related controls: AC-3, AC-4, AC-18, AC-19, AU-2, AU-12, CA-7, CM-2, IA-3, SC-7, SI-4.

Control Enhancements:

(1) *INTERNAL SYSTEM CONNECTIONS | SECURITY COMPLIANCE CHECKS*

The information system performs security compliance checks on constituent system components prior to the establishment of the internal connection.

Supplemental Guidance: Security compliance checks may include, for example, verification of the relevant baseline configuration. Related controls: CM-6.

References: None.

Priority and Baseline Allocation:

P2	**LOW** CA-9	**MOD** CA-9	**HIGH** CA-9

FAMILY: CONFIGURATION MANAGEMENT

CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

   1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and

b. Reviews and updates the current:

   1. Configuration management policy [*Assignment: organization-defined frequency*]; and

   2. Configuration management procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CM family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** CM-1	**MOD** CM-1	**HIGH** CM-1

CM-2 BASELINE CONFIGURATION

Control: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

Supplemental Guidance: This control establishes baseline configurations for information systems and system components including communications and connectivity-related aspects of systems. Baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for information systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. Baseline configurations include information about information system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture. Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture. Related controls: CM-3, CM-6, CM-8, CM-9, SA-10, PM-5, PM-7.

Control Enhancements:

(1) *BASELINE CONFIGURATION | REVIEWS AND UPDATES*

The organization reviews and updates the baseline configuration of the information system:

(a) [*Assignment: organization-defined frequency*];

(b) When required due to [*Assignment organization-defined circumstances*]; and

(c) As an integral part of information system component installations and upgrades.

Supplemental Guidance: Related control: CM-5.

(2) *BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY / CURRENCY*

The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

Supplemental Guidance: Automated mechanisms that help organizations maintain consistent baseline configurations for information systems include, for example, hardware and software inventory tools, configuration management tools, and network management tools. Such tools can be deployed and/or allocated as common controls, at the information system level, or at the operating system or component level (e.g., on workstations, servers, notebook computers, network components, or mobile devices). Tools can be used, for example, to track version numbers on operating system applications, types of software installed, and current patch levels. This control enhancement can be satisfied by the implementation of CM-8 (2) for organizations that choose to combine information system component inventory and baseline configuration activities. Related controls: CM-7, RA-5.

(3) *BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS*

The organization retains [*Assignment: organization-defined previous versions of baseline configurations of the information system*] to support rollback.

Supplemental Guidance: Retaining previous versions of baseline configurations to support rollback may include, for example, hardware, software, firmware, configuration files, and configuration records.

(4) *BASELINE CONFIGURATION | UNAUTHORIZED SOFTWARE*

[Withdrawn: Incorporated into CM-7].

(5) *BASELINE CONFIGURATION | AUTHORIZED SOFTWARE*

[Withdrawn: Incorporated into CM-7].

(6) *BASELINE CONFIGURATION | DEVELOPMENT AND TEST ENVIRONMENTS*

The organization maintains a baseline configuration for information system development and test environments that is managed separately from the operational baseline configuration.

Supplemental Guidance: Establishing separate baseline configurations for development, testing, and operational environments helps protect information systems from unplanned/unexpected events related to development and testing activities. Separate baseline configurations allow organizations to apply the configuration management that is most appropriate for each type of configuration. For example, management of operational configurations typically emphasizes the need for stability, while management of development/test configurations requires greater flexibility. Configurations in the test environment mirror the configurations in the operational environment to the extent practicable so that the results of the testing are representative of the proposed changes to the operational systems. This control enhancement requires separate configurations but not necessarily separate physical environments. Related controls: CM-4, SC-3, SC-7.

(7) *BASELINE CONFIGURATION | CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS*

The organization:

(a) Issues [*Assignment: organization-defined information systems, system components, or devices*] with [*Assignment: organization-defined configurations*] to individuals traveling to locations that the organization deems to be of significant risk; and

(b) Applies [*Assignment: organization-defined security safeguards*] to the devices when the individuals return.

Supplemental Guidance: When it is known that information systems, system components, or devices (e.g., notebook computers, mobile devices) will be located in high-risk areas, additional security controls may be implemented to counter the greater threat in such areas coupled with the lack of physical security relative to organizational-controlled areas. For example, organizational policies and procedures for notebook computers used by individuals departing on and returning from travel include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific safeguards to the device after travel is completed. Specially configured notebook computers include, for example, computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified safeguards applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering and purging/reimaging the hard disk drive. Protecting information residing on mobile devices is covered in the media protection family.

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P1	**LOW** CM-2	**MOD** CM-2 (1) (3) (7)	**HIGH** CM-2 (1) (2) (3) (7)

CM-3 CONFIGURATION CHANGE CONTROL

Control: The organization:

a. Determines the types of changes to the information system that are configuration-controlled;

b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;

c. Documents configuration change decisions associated with the information system;

d. Implements approved configuration-controlled changes to the information system;

e. Retains records of configuration-controlled changes to the information system for [*Assignment: organization-defined time period*];

f. Audits and reviews activities associated with configuration-controlled changes to the information system; and

g. Coordinates and provides oversight for configuration change control activities through [*Assignment: organization-defined configuration change control element (e.g., committee, board)*] that convenes [*Selection (one or more):* [*Assignment: organization-defined frequency*]; [*Assignment: organization-defined configuration change conditions*]].

Supplemental Guidance: Configuration change controls for organizational information systems involve the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of information systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled/unauthorized changes, and changes to remediate vulnerabilities. Typical processes for managing configuration changes to information systems include, for example, Configuration Control Boards that approve proposed changes to systems. For new development information systems or systems undergoing major upgrades, organizations consider including representatives from development organizations on the Configuration Control Boards. Auditing of changes includes activities before and after changes are made to organizational information systems and the auditing activities required to implement such changes. Related controls: CA-7, CM-2, CM-4, CM-5, CM-6, CM-9, SA-10, SI-2, SI-12.

Control Enhancements:

(1) *CONFIGURATION CHANGE CONTROL | AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES*

The organization employs automated mechanisms to:

(a) Document proposed changes to the information system;

(b) Notify [*Assignment: organized-defined approval authorities*] of proposed changes to the information system and request change approval;

(c) Highlight proposed changes to the information system that have not been approved or disapproved by [*Assignment: organization-defined time period*];

(d) Prohibit changes to the information system until designated approvals are received;

(e) Document all changes to the information system; and

(f) Notify [*Assignment: organization-defined personnel*] when approved changes to the information system are completed.

(2) *CONFIGURATION CHANGE CONTROL | TEST / VALIDATE / DOCUMENT CHANGES*

The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

Supplemental Guidance: Changes to information systems include modifications to hardware, software, or firmware components and configuration settings defined in CM-6. Organizations ensure that testing does not interfere with information system operations. Individuals/groups conducting tests understand organizational security policies and procedures, information system security policies and procedures, and the specific health, safety, and environmental risks associated with particular facilities/processes. Operational systems may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If information systems must be taken off-line for testing, the tests are scheduled to occur during planned system outages whenever possible. If testing cannot be conducted on operational systems, organizations employ compensating controls (e.g., testing on replicated systems).

(3) *CONFIGURATION CHANGE CONTROL | AUTOMATED CHANGE IMPLEMENTATION*

The organization employs automated mechanisms to implement changes to the current information system baseline and deploys the updated baseline across the installed base.

(4) *CONFIGURATION CHANGE CONTROL | SECURITY REPRESENTATIVE*

The organization requires an information security representative to be a member of the [*Assignment: organization-defined configuration change control element*].

Supplemental Guidance: Information security representatives can include, for example, senior agency information security officers, information system security officers, or information system security managers. Representation by personnel with information security expertise is important because changes to information system configurations can have unintended side effects, some of which may be security-relevant. Detecting such changes early in the process can help avoid unintended, negative consequences that could ultimately affect the security state of organizational information systems. The configuration change control element in this control enhancement reflects the change control elements defined by organizations in CM-3.

(5) *CONFIGURATION CHANGE CONTROL | AUTOMATED SECURITY RESPONSE*

The information system implements [*Assignment: organization-defined security responses*] automatically if baseline configurations are changed in an unauthorized manner.

Supplemental Guidance: Security responses include, for example, halting information system processing, halting selected system functions, or issuing alerts/notifications to organizational personnel when there is an unauthorized modification of a configuration item.

(6) *CONFIGURATION CHANGE CONTROL | CRYPTOGRAPHY MANAGEMENT*

The organization ensures that cryptographic mechanisms used to provide [*Assignment: organization-defined security safeguards*] are under configuration management.

Supplemental Guidance: Regardless of the cryptographic means employed (e.g., public key, private key, shared secrets), organizations ensure that there are processes and procedures in place to effectively manage those means. For example, if devices use certificates as a basis for

identification and authentication, there needs to be a process in place to address the expiration of those certificates. Related control: SC-13.

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** CM-3 (2)	**HIGH** CM-3 (1) (2)

CM-4 SECURITY IMPACT ANALYSIS

Control: The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

Supplemental Guidance: Organizational personnel with information security responsibilities (e.g., Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills/technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis may include, for example, reviewing security plans to understand security control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls. Security impact analyses may also include assessments of risk to better understand the impact of the changes and to determine if additional security controls are required. Security impact analyses are scaled in accordance with the security categories of the information systems. Related controls: CA-2, CA-7, CM-3, CM-9, SA-4, SA-5, SA-10, SI-2.

Control Enhancements:

(1) *SECURITY IMPACT ANALYSIS | SEPARATE TEST ENVIRONMENTS*

The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.

Supplemental Guidance: Separate test environment in this context means an environment that is physically or logically isolated and distinct from the operational environment. The separation is sufficient to ensure that activities in the test environment do not impact activities in the operational environment, and information in the operational environment is not inadvertently transmitted to the test environment. Separate environments can be achieved by physical or logical means. If physically separate test environments are not used, organizations determine the strength of mechanism required when implementing logical separation (e.g., separation achieved through virtual machines). Related controls: SA-11, SC-3, SC-7.

(2) *SECURITY IMPACT ANALYSIS | VERIFICATION OF SECURITY FUNCTIONS*

The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.

Supplemental Guidance: Implementation is this context refers to installing changed code in the operational information system. Related control: SA-11.

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P2	**LOW** CM-4	**MOD** CM-4	**HIGH** CM-4 (1)

CM-5 ACCESS RESTRICTIONS FOR CHANGE

Control: The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

Supplemental Guidance: Any changes to the hardware, software, and/or firmware components of information systems can potentially have significant effects on the overall security of the systems. Therefore, organizations permit only qualified and authorized individuals to access information systems for purposes of initiating changes, including upgrades and modifications. Organizations maintain records of access to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes. Access restrictions for change also include software libraries. Access restrictions include, for example, physical and logical access controls (see AC-3 and PE-3), workflow automation, media libraries, abstract layers (e.g., changes implemented into third-party interfaces rather than directly into information systems), and change windows (e.g., changes occur only during specified times, making unauthorized changes easy to discover). Related controls: AC-3, AC-6, PE-3.

Control Enhancements:

(1) *ACCESS RESTRICTIONS FOR CHANGE | AUTOMATED ACCESS ENFORCEMENT / AUDITING*

The information system enforces access restrictions and supports auditing of the enforcement actions.

Supplemental Guidance: Related controls: AU-2, AU-12, AU-6, CM-3, CM-6.

(2) *ACCESS RESTRICTIONS FOR CHANGE | REVIEW SYSTEM CHANGES*

The organization reviews information system changes [*Assignment: organization-defined frequency*] and [*Assignment: organization-defined circumstances*] to determine whether unauthorized changes have occurred.

Supplemental Guidance: Indications that warrant review of information system changes and the specific circumstances justifying such reviews may be obtained from activities carried out by organizations during the configuration change process. Related controls: AU-6, AU-7, CM-3, CM-5, PE-6, PE-8.

(3) *ACCESS RESTRICTIONS FOR CHANGE | SIGNED COMPONENTS*

The information system prevents the installation of [*Assignment: organization-defined software and firmware components*] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

Supplemental Guidance: Software and firmware components prevented from installation unless signed with recognized and approved certificates include, for example, software and firmware version updates, patches, service packs, device drivers, and basic input output system (BIOS) updates. Organizations can identify applicable software and firmware components by type, by specific items, or a combination of both. Digital signatures and organizational verification of such signatures, is a method of code authentication. Related controls: CM-7, SC-13, SI-7.

(4) *ACCESS RESTRICTIONS FOR CHANGE | DUAL AUTHORIZATION*

The organization enforces dual authorization for implementing changes to [*Assignment: organization-defined information system components and system-level information*].

Supplemental Guidance: Organizations employ dual authorization to ensure that any changes to selected information system components and information cannot occur unless two qualified individuals implement such changes. The two individuals possess sufficient skills/expertise to determine if the proposed changes are correct implementations of approved changes. Dual authorization may also be known as two-person control. Related controls: AC-5, CM-3.

(5) *ACCESS RESTRICTIONS FOR CHANGE | LIMIT PRODUCTION / OPERATIONAL PRIVILEGES*

The organization:

(a) Limits privileges to change information system components and system-related information within a production or operational environment; and

(b) Reviews and reevaluates privileges [*Assignment: organization-defined frequency*].

Supplemental Guidance: In many organizations, information systems support multiple core missions/business functions. Limiting privileges to change information system components with respect to operational systems is necessary because changes to a particular information

system component may have far-reaching effects on mission/business processes supported by the system where the component resides. The complex, many-to-many relationships between systems and mission/business processes are in some cases, unknown to developers. Related control: AC-2.

(6) *ACCESS RESTRICTIONS FOR CHANGE | LIMIT LIBRARY PRIVILEGES*

The organization limits privileges to change software resident within software libraries.

Supplemental Guidance: Software libraries include privileged programs. Related control: AC-2.

(7) *ACCESS RESTRICTIONS FOR CHANGE | AUTOMATIC IMPLEMENTATION OF SECURITY SAFEGUARDS*

[Withdrawn: Incorporated into SI-7].

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** CM-5	**HIGH** CM-5 (1) (2) (3)

CM-6 CONFIGURATION SETTINGS

Control: The organization:

a. Establishes and documents configuration settings for information technology products employed within the information system using [*Assignment: organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements;

b. Implements the configuration settings;

c. Identifies, documents, and approves any deviations from established configuration settings for [*Assignment: organization-defined information system components*] based on [*Assignment: organization-defined operational requirements*]; and

d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

Supplemental Guidance: Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system. Information technology products for which security-related configuration settings can be defined include, for example, mainframe computers, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications. Security-related parameters are those parameters impacting the security state of information systems including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: (i) registry settings; (ii) account, file, directory permission settings; and (iii) settings for functions, ports, protocols, services, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific settings for information systems. The established settings become part of the systems configuration baseline.

Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those information system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations including, for example, information technology product developers, manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors. Common secure configurations include the

United States Government Configuration Baseline (USGCB) which affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol (e.g., Common Configuration Enumeration) provide an effective method to uniquely identify, track, and control configuration settings. OMB establishes federal policy on configuration requirements for federal information systems. Related controls: AC-19, CM-2, CM-3, CM-7, SI-4.

Control Enhancements:

(1) *CONFIGURATION SETTINGS | AUTOMATED CENTRAL MANAGEMENT / APPLICATION / VERIFICATION*

The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [*Assignment: organization-defined information system components*].

Supplemental Guidance: Related controls: CA-7, CM-4.

(2) *CONFIGURATION SETTINGS | RESPOND TO UNAUTHORIZED CHANGES*

The organization employs [*Assignment: organization-defined security safeguards*] to respond to unauthorized changes to [*Assignment: organization-defined configuration settings*].

Supplemental Guidance: Responses to unauthorized changes to configuration settings can include, for example, alerting designated organizational personnel, restoring established configuration settings, or in extreme cases, halting affected information system processing. Related controls: IR-4, SI-7.

(3) *CONFIGURATION SETTINGS | UNAUTHORIZED CHANGE DETECTION*

[Withdrawn: Incorporated into SI-7].

(4) *CONFIGURATION SETTINGS | CONFORMANCE DEMONSTRATION*

[Withdrawn: Incorporated into CM-4].

References: OMB Memoranda 07-11, 07-18, 08-22; NIST Special Publications 800-70, 800-128; Web: http://nvd.nist.gov, http://checklists.nist.gov, http://www.nsa.gov.

Priority and Baseline Allocation:

P1	**LOW** CM-6	**MOD** CM-6	**HIGH** CM-6 (1) (2)

CM-7 LEAST FUNCTIONALITY

Control: The organization:

a. Configures the information system to provide only essential capabilities; and

b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [*Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services*].

Supplemental Guidance: Information systems can provide a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from single information system components, but doing so increases risk over limiting the services provided by any one component. Where feasible, organizations limit component functionality to a single function per device (e.g., email servers or web servers, but not both). Organizations review functions and services provided by information systems or individual components of information systems, to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, and file sharing). Organizations consider disabling unused or unnecessary physical and logical ports/protocols (e.g., Universal Serial Bus, File Transfer Protocol, and Hyper Text Transfer Protocol) on information systems to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection

systems to identify and prevent the use of prohibited functions, ports, protocols, and services. Related controls: AC-6, CM-2, RA-5, SA-5, SC-7.

Control Enhancements:

(1) *LEAST FUNCTIONALITY | PERIODIC REVIEW*

The organization:

(a) Reviews the information system [*Assignment: organization-defined frequency*] to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and

(b) Disables [*Assignment: organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure*].

Supplemental Guidance: The organization can either make a determination of the relative security of the function, port, protocol, and/or service or base the security decision on the assessment of other entities. Bluetooth, FTP, and peer-to-peer networking are examples of less than secure protocols. Related controls: AC-18, CM-7, IA-2.

(2) *LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION*

The information system prevents program execution in accordance with [*Selection (one or more): [Assignment: organization-defined policies regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage*].

Supplemental Guidance: Related controls: CM-8, PM-5.

(3) *LEAST FUNCTIONALITY | REGISTRATION COMPLIANCE*

The organization ensures compliance with [*Assignment: organization-defined registration requirements for functions, ports, protocols, and services*].

Supplemental Guidance: Organizations use the registration process to manage, track, and provide oversight for information systems and implemented functions, ports, protocols, and services.

(4) *LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE / BLACKLISTING*

The organization:

(a) Identifies [*Assignment: organization-defined software programs not authorized to execute on the information system*];

(b) Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and

(c) Reviews and updates the list of unauthorized software programs [*Assignment: organization-defined frequency*].

Supplemental Guidance: The process used to identify software programs that are not authorized to execute on organizational information systems is commonly referred to as *blacklisting*. Organizations can implement CM-7 (5) instead of this control enhancement if whitelisting (the stronger of the two policies) is the preferred approach for restricting software program execution. Related controls: CM-6, CM-8, PM-5.

(5) *LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE / WHITELISTING*

The organization:

(a) Identifies [*Assignment: organization-defined software programs authorized to execute on the information system*];

(b) Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and

(c) Reviews and updates the list of authorized software programs [*Assignment: organization-defined frequency*].

Supplemental Guidance: The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as *whitelisting*. In addition to whitelisting, organizations consider verifying the integrity of white-listed software programs using, for example, cryptographic checksums, digital signatures, or hash functions. Verification of white-listed software can occur either prior to execution or at system startup. Related controls: CM-2, CM-6, CM-8, PM-5, SA-10, SC-34, SI-7.

References: DoD Instruction 8551.01.

Priority and Baseline Allocation:

P1	**LOW** CM-7	**MOD** CM-7 (1) (2) (4)	**HIGH** CM-7 (1) (2) (5)

CM-8 INFORMATION SYSTEM COMPONENT INVENTORY

Control: The organization:

a. Develops and documents an inventory of information system components that:

1. Accurately reflects the current information system;
2. Includes all components within the authorization boundary of the information system;
3. Is at the level of granularity deemed necessary for tracking and reporting; and
4. Includes [*Assignment: organization-defined information deemed necessary to achieve effective information system component accountability*]; and

b. Reviews and updates the information system component inventory [*Assignment: organization-defined frequency*].

Supplemental Guidance: Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner). Information deemed necessary for effective accountability of information system components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location. Related controls: CM-2, CM-6, PM-5.

Control Enhancements:

(1) *INFORMATION SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATIONS / REMOVALS*

The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

(2) *INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE*

The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

Supplemental Guidance: Organizations maintain information system inventories to the extent feasible. Virtual machines, for example, can be difficult to monitor because such machines are not visible to the network when not in use. In such cases, organizations maintain as up-to-date, complete, and accurate an inventory as is deemed reasonable. This control enhancement can be satisfied by the implementation of CM-2 (2) for organizations that choose to combine information system component inventory and baseline configuration activities. Related control: SI-7.

(3) *INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION*

The organization:

(a) Employs automated mechanisms [*Assignment: organization-defined frequency*] to detect the presence of unauthorized hardware, software, and firmware components within the information system; and

(b) Takes the following actions when unauthorized components are detected: [*Selection (one or more): disables network access by such components; isolates the components; notifies* [*Assignment: organization-defined personnel or roles*]].

Supplemental Guidance: This control enhancement is applied in addition to the monitoring for unauthorized remote connections and mobile devices. Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms can be implemented within information systems or in other separate devices. Isolation can be achieved, for example, by placing unauthorized information system components in separate domains or subnets or otherwise quarantining such components. This type of component isolation is commonly referred to as sandboxing. Related controls: AC-17, AC-18, AC-19, CA-7, SI-3, SI-4, SI-7, RA-5.

(4) *INFORMATION SYSTEM COMPONENT INVENTORY | ACCOUNTABILITY INFORMATION*

The organization includes in the information system component inventory information, a means for identifying by [*Selection (one or more): name; position; role*], individuals responsible/accountable for administering those components.

Supplemental Guidance: Identifying individuals who are both responsible and accountable for administering information system components helps to ensure that the assigned components are properly administered and organizations can contact those individuals if some action is required (e.g., component is determined to be the source of a breach/compromise, component needs to be recalled/replaced, or component needs to be relocated).

(5) *INFORMATION SYSTEM COMPONENT INVENTORY | NO DUPLICATE ACCOUNTING OF COMPONENTS*

The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.

Supplemental Guidance: This control enhancement addresses the potential problem of duplicate accounting of information system components in large or complex interconnected systems.

(6) *INFORMATION SYSTEM COMPONENT INVENTORY | ASSESSED CONFIGURATIONS / APPROVED DEVIATIONS*

The organization includes assessed component configurations and any approved deviations to current deployed configurations in the information system component inventory.

Supplemental Guidance: This control enhancement focuses on configuration settings established by organizations for information system components, the specific components that have been assessed to determine compliance with the required configuration settings, and any approved deviations from established configuration settings. Related controls: CM-2, CM-6.

(7) *INFORMATION SYSTEM COMPONENT INVENTORY | CENTRALIZED REPOSITORY*

The organization provides a centralized repository for the inventory of information system components.

Supplemental Guidance: Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. Centralized repositories of information system component inventories provide opportunities for efficiencies in accounting for organizational hardware, software, and firmware assets. Such repositories may also help organizations rapidly identify the location and responsible individuals of system components that have been compromised, breached, or are otherwise in need of mitigation actions. Organizations ensure that the resulting centralized inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner).

(8) *INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED LOCATION TRACKING*

The organization employs automated mechanisms to support tracking of information system components by geographic location.

Supplemental Guidance: The use of automated mechanisms to track the location of information system components can increase the accuracy of component inventories. Such capability may also help organizations rapidly identify the location and responsible individuals of system components that have been compromised, breached, or are otherwise in need of mitigation actions.

(9) *INFORMATION SYSTEM COMPONENT INVENTORY | ASSIGNMENT OF COMPONENTS TO SYSTEMS*

The organization:

(a) Assigns [*Assignment: organization-defined acquired information system components*] to an information system; and

(b) Receives an acknowledgement from the information system owner of this assignment.

Supplemental Guidance: Organizations determine the criteria for or types of information system components (e.g., microprocessors, motherboards, software, programmable logic controllers, and network devices) that are subject to this control enhancement. Related control: SA-4.

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P1	**LOW** CM-8	**MOD** CM-8 (1) (3) (5)	**HIGH** CM-8 (1) (2) (3) (4) (5)

CM-9 CONFIGURATION MANAGEMENT PLAN

Control: The organization develops, documents, and implements a configuration management plan for the information system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;

b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;

c. Defines the configuration items for the information system and places the configuration items under configuration management; and

d. Protects the configuration management plan from unauthorized disclosure and modification.

Supplemental Guidance: Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual information systems. Such plans define detailed processes and procedures for how configuration management is used to support system development life cycle activities at the information system level. Configuration management plans are typically developed during the development/acquisition phase of the system development life cycle. The plans describe how to move changes through change management processes, how to update configuration settings and baselines, how to maintain information system component inventories, how to control development, test, and operational environments, and how to develop, release, and update key documents. Organizations can employ templates to help ensure consistent and timely development and implementation of configuration management plans. Such templates can represent a master configuration management plan for the organization at large with subsets of the plan implemented on a system by system basis. Configuration management approval processes include designation of key management stakeholders responsible for reviewing and approving proposed changes to information systems, and personnel that conduct security impact analyses prior to the implementation of changes to the systems. Configuration items are the information system items (hardware, software, firmware, and documentation) to be configuration-managed. As information systems continue through the system development life cycle, new configuration items may be identified and some existing configuration items may no longer need to be under configuration control. Related controls: CM-2, CM-3, CM-4, CM-5, CM-8, SA-10.

Control Enhancements:

(1) *CONFIGURATION MANAGEMENT PLAN | ASSIGNMENT OF RESPONSIBILITY*

The organization assigns responsibility for developing the configuration management process to organizational personnel that are not directly involved in information system development.

Supplemental Guidance: In the absence of dedicated configuration management teams assigned within organizations, system developers may be tasked to develop configuration management processes using personnel who are not directly involved in system development or integration. This separation of duties ensures that organizations establish and maintain a sufficient degree of independence between the information system development and integration processes and configuration management processes to facilitate quality control and more effective oversight.

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** CM-9	**HIGH** CM-9

CM-10 SOFTWARE USAGE RESTRICTIONS

Control: The organization:

a. Uses software and associated documentation in accordance with contract agreements and copyright laws;

b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and

c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Supplemental Guidance: Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs. Related controls: AC-17, CM-8, SC-7.

Control Enhancements:

(1) *SOFTWARE USAGE RESTRICTIONS | OPEN SOURCE SOFTWARE*

The organization establishes the following restrictions on the use of open source software: [*Assignment: organization-defined restrictions*].

Supplemental Guidance: Open source software refers to software that is available in source code form. Certain software rights normally reserved for copyright holders are routinely provided under software license agreements that permit individuals to study, change, and improve the software. From a security perspective, the major advantage of open source software is that it provides organizations with the ability to examine the source code. However, there are also various licensing issues associated with open source software including, for example, the constraints on derivative use of such software.

References: None.

Priority and Baseline Allocation:

P2	**LOW** CM-10	**MOD** CM-10	**HIGH** CM-10

CM-11 USER-INSTALLED SOFTWARE

Control: The organization:

a. Establishes [*Assignment: organization-defined policies*] governing the installation of software by users;
b. Enforces software installation policies through [*Assignment: organization-defined methods*]; and
c. Monitors policy compliance at [*Assignment: organization-defined frequency*].

Supplemental Guidance: If provided the necessary privileges, users have the ability to install software in organizational information systems. To maintain control over the types of software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations may include, for example, updates and security patches to existing software and downloading applications from organization-approved "app stores." Prohibited software installations may include, for example, software with unknown or suspect pedigrees or software that organizations consider potentially malicious. The policies organizations select

governing user-installed software may be organization-developed or provided by some external entity. Policy enforcement methods include procedural methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information systems), or both. Related controls: AC-3, CM-2, CM-3, CM-5, CM-6, CM-7, PL-4.

Control Enhancements:

(1) *USER-INSTALLED SOFTWARE | ALERTS FOR UNAUTHORIZED INSTALLATIONS*

The information system alerts [*Assignment: organization-defined personnel or roles*] when the unauthorized installation of software is detected.

Supplemental Guidance: Related controls: CA-7, SI-4.

(2) *USER-INSTALLED SOFTWARE | PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS*

The information system prohibits user installation of software without explicit privileged status.

Supplemental Guidance: Privileged status can be obtained, for example, by serving in the role of system administrator. Related control: AC-6.

References: None.

Priority and Baseline Allocation:

P1	**LOW** CM-11	**MOD** CM-11	**HIGH** CM-11

FAMILY: CONTINGENCY PLANNING

CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

   1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and

b. Reviews and updates the current:

   1. Contingency planning policy [*Assignment: organization-defined frequency*]; and

   2. Contingency planning procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CP family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: Federal Continuity Directive 1; NIST Special Publications 800-12, 800-34, 800-100.

Priority and Baseline Allocation:

P1	**LOW** CP-1	**MOD** CP-1	**HIGH** CP-1

CP-2 CONTINGENCY PLAN

Control: The organization:

a. Develops a contingency plan for the information system that:

   1. Identifies essential missions and business functions and associated contingency requirements;

   2. Provides recovery objectives, restoration priorities, and metrics;

   3. Addresses contingency roles, responsibilities, assigned individuals with contact information;

   4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;

   5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and

   6. Is reviewed and approved by [*Assignment: organization-defined personnel or roles*];

b. Distributes copies of the contingency plan to [*Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements*];

c. Coordinates contingency planning activities with incident handling activities;

d. Reviews the contingency plan for the information system [*Assignment: organization-defined frequency*];

e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

f. Communicates contingency plan changes to [*Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements*]; and

g. Protects the contingency plan from unauthorized disclosure and modification.

Supplemental Guidance: Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. The effectiveness of contingency planning is maximized by considering such planning throughout the phases of the system development life cycle. Performing contingency planning on hardware, software, and firmware development can be an effective means of achieving information system resiliency. Contingency plans reflect the degree of restoration required for organizational information systems since not all systems may need to fully recover to achieve the level of continuity of operations desired. Information system recovery objectives reflect applicable laws, Executive Orders, directives, policies, standards, regulations, and guidelines. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission and/or business effectiveness, such as malicious attacks compromising the confidentiality or integrity of information systems. Actions addressed in contingency plans include, for example, orderly/graceful degradation, information system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By closely coordinating contingency planning with incident handling activities, organizations can ensure that the necessary contingency planning activities are in place and activated in the event of a security incident. Related controls: AC-14, CP-6, CP-7, CP-8, CP-9, CP-10, IR-4, IR-8, MP-2, MP-4, MP-5, PM-8, PM-11.

Control Enhancements:

(1) *CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS*

The organization coordinates contingency plan development with organizational elements responsible for related plans.

Supplemental Guidance: Plans related to contingency plans for organizational information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation Plan, and Occupant Emergency Plans.

(2) *CONTINGENCY PLAN | CAPACITY PLANNING*

The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

Supplemental Guidance: Capacity planning is needed because different types of threats (e.g., natural disasters, targeted cyber attacks) can result in a reduction of the available processing, telecommunications, and support services originally intended to support the organizational missions/business functions. Organizations may need to anticipate degraded operations during contingency operations and factor such degradation into capacity planning.

(3) *CONTINGENCY PLAN | RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*

The organization plans for the resumption of essential missions and business functions within [*Assignment: organization-defined time period*] of contingency plan activation.

Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. The time period for resumption of essential missions/business functions may be dependent on the severity/extent of disruptions to the information system and its supporting infrastructure. Related control: PE-12.

(4) *CONTINGENCY PLAN | RESUME ALL MISSIONS / BUSINESS FUNCTIONS*

The organization plans for the resumption of all missions and business functions within [*Assignment: organization-defined time period*] of contingency plan activation.

Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. The time period for resumption of all missions/business functions may be dependent on the severity/extent of disruptions to the information system and its supporting infrastructure. Related control: PE-12.

(5) *CONTINGENCY PLAN | CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*

The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.

Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency (e.g., backup sites may become primary sites). Related control: PE-12.

(6) *CONTINGENCY PLAN | ALTERNATE PROCESSING / STORAGE SITE*

The organization plans for the transfer of essential missions and business functions to alternate processing and/or storage sites with little or no loss of operational continuity and sustains that continuity through information system restoration to primary processing and/or storage sites.

Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency (e.g., backup sites may become primary sites). Related control: PE-12.

(7) *CONTINGENCY PLAN | COORDINATE WITH EXTERNAL SERVICE PROVIDERS*

The organization coordinates its contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.

Supplemental Guidance: When the capability of an organization to successfully carry out its core missions/business functions is dependent on external service providers, developing a timely and comprehensive contingency plan may become more challenging. In this situation, organizations coordinate contingency planning activities with the external entities to ensure that the individual plans reflect the overall contingency needs of the organization. Related control: SA-9.

(8) *CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS*

The organization identifies critical information system assets supporting essential missions and business functions.

Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. Organizations identify critical information system assets so that additional safeguards and countermeasures can be employed (above and beyond those safeguards and countermeasures routinely implemented) to help ensure that organizational missions/business functions can continue to be conducted during contingency operations. In addition, the identification of critical information assets facilitates the prioritization of organizational resources. Critical information system assets include technical and operational aspects. Technical aspects include, for example, information

technology services, information system components, information technology products, and mechanisms. Operational aspects include, for example, procedures (manually executed operations) and personnel (individuals operating technical safeguards and/or executing manual procedures). Organizational program protection plans can provide assistance in identifying critical assets. Related controls: SA-14, SA-15.

References: Federal Continuity Directive 1; NIST Special Publication 800-34.

Priority and Baseline Allocation:

P1	**LOW** CP-2	**MOD** CP-2 (1) (3) (8)	**HIGH** CP-2 (1) (2) (3) (4) (5) (8)

CP-3 CONTINGENCY TRAINING

Control: The organization provides contingency training to information system users consistent with assigned roles and responsibilities:

a. Within [*Assignment: organization-defined time period*] of assuming a contingency role or responsibility;

b. When required by information system changes; and

c. [*Assignment: organization-defined frequency*] thereafter.

Supplemental Guidance: Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, regular users may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to set up information systems at alternate processing and storage sites; and managers/senior leaders may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activities. Training for contingency roles/responsibilities reflects the specific continuity requirements in the contingency plan. Related controls: AT-2, AT-3, CP-2, IR-2.

Control Enhancements:

(1) *CONTINGENCY TRAINING | SIMULATED EVENTS*

The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.

(2) *CONTINGENCY TRAINING | AUTOMATED TRAINING ENVIRONMENTS*

The organization employs automated mechanisms to provide a more thorough and realistic contingency training environment.

References: Federal Continuity Directive 1; NIST Special Publications 800-16, 800-50.

Priority and Baseline Allocation:

P2	**LOW** CP-3	**MOD** CP-3	**HIGH** CP-3 (1)

CP-4 CONTINGENCY PLAN TESTING

Control: The organization:

a. Tests the contingency plan for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests*] to determine the effectiveness of the plan and the organizational readiness to execute the plan;

b. Reviews the contingency plan test results; and

c. Initiates corrective actions, if needed.

Supplemental Guidance: Methods for testing contingency plans to determine the effectiveness of the plans and to identify potential weaknesses in the plans include, for example, walk-through and tabletop exercises, checklists, simulations (parallel, full interrupt), and comprehensive exercises. Organizations conduct testing based on the continuity requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals arising due to contingency operations. Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions. Related controls: CP-2, CP-3, IR-3.

Control Enhancements:

(1) *CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS*

The organization coordinates contingency plan testing with organizational elements responsible for related plans.

Supplemental Guidance: Plans related to contingency plans for organizational information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans. This control enhancement does not require organizations to create organizational elements to handle related plans or to align such elements with specific plans. It does require, however, that if such organizational elements are responsible for related plans, organizations should coordinate with those elements. Related controls: IR-8, PM-8.

(2) *CONTINGENCY PLAN TESTING | ALTERNATE PROCESSING SITE*

The organization tests the contingency plan at the alternate processing site:

(a) To familiarize contingency personnel with the facility and available resources; and

(b) To evaluate the capabilities of the alternate processing site to support contingency operations.

Supplemental Guidance: Related control: CP-7.

(3) *CONTINGENCY PLAN TESTING | AUTOMATED TESTING*

The organization employs automated mechanisms to more thoroughly and effectively test the contingency plan.

Supplemental Guidance: Automated mechanisms provide more thorough and effective testing of contingency plans, for example: (i) by providing more complete coverage of contingency issues; (ii) by selecting more realistic test scenarios and environments; and (iii) by effectively stressing the information system and supported missions.

(4) *CONTINGENCY PLAN TESTING | FULL RECOVERY / RECONSTITUTION*

The organization includes a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.

Supplemental Guidance: Related controls: CP-10, SC-24.

References: Federal Continuity Directive 1; FIPS Publication 199; NIST Special Publications 800-34, 800-84.

Priority and Baseline Allocation:

P2	**LOW** CP-4	**MOD** CP-4 (1)	**HIGH** CP-4 (1) (2)

CP-5 CONTINGENCY PLAN UPDATE

[Withdrawn: Incorporated into CP-2].

CP-6 ALTERNATE STORAGE SITE

Control: The organization:

a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and

b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

Supplemental Guidance: Alternate storage sites are sites that are geographically distinct from primary storage sites. An alternate storage site maintains duplicate copies of information and data in the event that the primary storage site is not available. Items covered by alternate storage site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination of delivery/retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems. Related controls: CP-2, CP-7, CP-9, CP-10, MP-4.

Control Enhancements:

(1) *ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE*

The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

Supplemental Guidance: Threats that affect alternate storage sites are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber attacks, and errors of omission/commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate storage sites based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber attack), the degree of separation between sites is less relevant. Related control: RA-3.

(2) *ALTERNATE STORAGE SITE | RECOVERY TIME / POINT OBJECTIVES*

The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

(3) *ALTERNATE STORAGE SITE | ACCESSIBILITY*

The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Supplemental Guidance: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage) with such determinations made by organizations based on organizational assessments of risk. Explicit mitigation actions include, for example: (i) duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites; or (ii) planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted. Related control: RA-3.

References: NIST Special Publication 800-34.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** CP-6 (1) (3)	**HIGH** CP-6 (1) (2) (3)

CP-7 ALTERNATE PROCESSING SITE

Control: The organization:

a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [*Assignment: organization-defined information system operations*] for essential missions/business functions within [*Assignment: organization-defined time period*

consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable;

b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and

c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.

Supplemental Guidance: Alternate processing sites are sites that are geographically distinct from primary processing sites. An alternate processing site provides processing capability in the event that the primary processing site is not available. Items covered by alternate processing site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination for the transfer/assignment of personnel. Requirements are specifically allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems. Related controls: CP-2, CP-6, CP-8, CP-9, CP-10, MA-6.

Control Enhancements:

(1) *ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE*

The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

Supplemental Guidance: Threats that affect alternate processing sites are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber attacks, and errors of omission/commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate processing sites based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber attack), the degree of separation between sites is less relevant. Related control: RA-3.

(2) *ALTERNATE PROCESSING SITE | ACCESSIBILITY*

The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Supplemental Guidance: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage) with such determinations made by organizations based on organizational assessments of risk. Related control: RA-3.

(3) *ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE*

The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).

Supplemental Guidance: Priority-of-service agreements refer to negotiated agreements with service providers that ensure that organizations receive priority treatment consistent with their availability requirements and the availability of information resources at the alternate processing site.

(4) *ALTERNATE PROCESSING SITE | PREPARATION FOR USE*

The organization prepares the alternate processing site so that the site is ready to be used as the operational site supporting essential missions and business functions.

Supplemental Guidance: Site preparation includes, for example, establishing configuration settings for information system components at the alternate processing site consistent with the requirements for such settings at the primary site and ensuring that essential supplies and other logistical considerations are in place. Related controls: CM-2, CM-6.

(5) *ALTERNATE PROCESSING SITE | EQUIVALENT INFORMATION SECURITY SAFEGUARDS*

[Withdrawn: Incorporated into CP-7].

(6) *ALTERNATE PROCESSING SITE | INABILITY TO RETURN TO PRIMARY SITE*

The organization plans and prepares for circumstances that preclude returning to the primary processing site.

References: NIST Special Publication 800-34.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** CP-7 (1) (2) (3)	**HIGH** CP-7 (1) (2) (3) (4)

CP-8 TELECOMMUNICATIONS SERVICES

Control: The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [*Assignment: organization-defined information system operations*] for essential missions and business functions within [*Assignment: organization-defined time period*] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Supplemental Guidance: This control applies to telecommunications services (data and voice) for primary and alternate processing and storage sites. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential missions/business functions despite the loss of primary telecommunications services. Organizations may specify different time periods for primary/alternate sites. Alternate telecommunications services include, for example, additional organizational or commercial ground-based circuits/lines or satellites in lieu of ground-based communications. Organizations consider factors such as availability, quality of service, and access when entering into alternate telecommunications agreements. Related controls: CP-2, CP-6, CP-7.

Control Enhancements:

(1) *TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS*

The organization:

(a) Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and

(b) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

Supplemental Guidance: Organizations consider the potential mission/business impact in situations where telecommunications service providers are servicing other organizations with similar priority-of-service provisions.

(2) *TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE*

The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

(3) *TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY / ALTERNATE PROVIDERS*

The organization obtains alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

Supplemental Guidance: Threats that affect telecommunications services are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber/physical attacks, and errors of omission/commission. Organizations seek to reduce common susceptibilities by, for example, minimizing shared infrastructure among telecommunications service providers and achieving sufficient geographic separation between services. Organizations may consider using a single service provider in situations where the service provider can provide alternate telecommunications services meeting the separation needs addressed in the risk assessment.

(4) *TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN*

The organization:

(a) Requires primary and alternate telecommunications service providers to have contingency plans;

(b) Reviews provider contingency plans to ensure that the plans meet organizational contingency requirements; and

(c) Obtains evidence of contingency testing/training by providers [*Assignment: organization-defined frequency*].

Supplemental Guidance: Reviews of provider contingency plans consider the proprietary nature of such plans. In some situations, a summary of provider contingency plans may be sufficient evidence for organizations to satisfy the review requirement. Telecommunications service providers may also participate in ongoing disaster recovery exercises in coordination with the Department of Homeland Security, state, and local governments. Organizations may use these types of activities to satisfy evidentiary requirements related to service provider contingency plan reviews, testing, and training.

(5) *TELECOMMUNICATIONS SERVICES | ALTERNATE TELECOMMUNICATION SERVICE TESTING*

The organization tests alternate telecommunication services [*Assignment: organization-defined frequency*].

References: NIST Special Publication 800-34; National Communications Systems Directive 3-10; Web: http://www.dhs.gov/telecommunications-service-priority-tsp.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** CP-8 (1) (2)	**HIGH** CP-8 (1) (2) (3) (4)

CP-9 INFORMATION SYSTEM BACKUP

Control: The organization:

a. Conducts backups of user-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*];

b. Conducts backups of system-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*];

c. Conducts backups of information system documentation including security-related documentation [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; and

d. Protects the confidentiality, integrity, and availability of backup information at storage locations.

Supplemental Guidance: System-level information includes, for example, system-state information, operating system and application software, and licenses. User-level information includes any information other than system-level information. Mechanisms employed by organizations to protect the integrity of information system backups include, for example, digital signatures and cryptographic hashes. Protection of system backup information while in transit is beyond the scope of this control. Information system backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information. Related controls: CP-2, CP-6, MP-4, MP-5, SC-13.

Control Enhancements:

(1) *INFORMATION SYSTEM BACKUP | TESTING FOR RELIABILITY / INTEGRITY*

The organization tests backup information [*Assignment: organization-defined frequency*] to verify media reliability and information integrity.

Supplemental Guidance: Related control: CP-4.

(2) *INFORMATION SYSTEM BACKUP | TEST RESTORATION USING SAMPLING*

The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.

Supplemental Guidance: Related control: CP-4.

(3) *INFORMATION SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION*

The organization stores backup copies of [*Assignment: organization-defined critical information system software and other security-related information*] in a separate facility or in a fire-rated container that is not collocated with the operational system.

Supplemental Guidance: Critical information system software includes, for example, operating systems, cryptographic key management systems, and intrusion detection/prevention systems. Security-related information includes, for example, organizational inventories of hardware, software, and firmware components. Alternate storage sites typically serve as separate storage facilities for organizations. Related controls: CM-2, CM-8.

(4) *INFORMATION SYSTEM BACKUP | PROTECTION FROM UNAUTHORIZED MODIFICATION*

[Withdrawn: Incorporated into CP-9].

(5) *INFORMATION SYSTEM BACKUP | TRANSFER TO ALTERNATE STORAGE SITE*

The organization transfers information system backup information to the alternate storage site [*Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives*].

Supplemental Guidance: Information system backup information can be transferred to alternate storage sites either electronically or by physical shipment of storage media.

(6) *INFORMATION SYSTEM BACKUP | REDUNDANT SECONDARY SYSTEM*

The organization accomplishes information system backup by maintaining a redundant secondary system that is not collocated with the primary system and that can be activated without loss of information or disruption to operations.

Supplemental Guidance: Related controls: CP-7, CP-10.

(7) *INFORMATION SYSTEM BACKUP | DUAL AUTHORIZATION*

The organization enforces dual authorization for the deletion or destruction of [*Assignment: organization-defined backup information*].

Supplemental Guidance: Dual authorization ensures that the deletion or destruction of backup information cannot occur unless two qualified individuals carry out the task. Individuals deleting/destroying backup information possess sufficient skills/expertise to determine if the proposed deletion/destruction of backup information reflects organizational policies and procedures. Dual authorization may also be known as two-person control. Related controls: AC-3, MP-2.

References: NIST Special Publication 800-34.

Priority and Baseline Allocation:

P1	**LOW** CP-9	**MOD** CP-9 (1)	**HIGH** CP-9 (1) (2) (3) (5)

CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

Control: The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

Supplemental Guidance: Recovery is executing information system contingency plan activities to restore organizational missions/business functions. Reconstitution takes place following recovery and includes activities for returning organizational information systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities, recovery point/time and reconstitution objectives, and established organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of any interim information system

capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored information system capabilities, reestablishment of continuous monitoring activities, potential information system reauthorizations, and activities to prepare the systems against future disruptions, compromises, or failures. Recovery/reconstitution capabilities employed by organizations can include both automated mechanisms and manual procedures. Related controls: CA-2, CA-6, CA-7, CP-2, CP-6, CP-7, CP-9, SC-24.

Control Enhancements:

(1) *INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | CONTINGENCY PLAN TESTING*
[Withdrawn: Incorporated into CP-4].

(2) *INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY*
The information system implements transaction recovery for systems that are transaction-based.

Supplemental Guidance: Transaction-based information systems include, for example, database management systems and transaction processing systems. Mechanisms supporting transaction recovery include, for example, transaction rollback and transaction journaling.

(3) *INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | COMPENSATING SECURITY CONTROLS*
[Withdrawn: Addressed through tailoring procedures].

(4) *INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME PERIOD*
The organization provides the capability to restore information system components within [*Assignment: organization-defined restoration time-periods*] from configuration-controlled and integrity-protected information representing a known, operational state for the components.

Supplemental Guidance: Restoration of information system components includes, for example, reimaging which restores components to known, operational states. Related control: CM-2.

(5) *INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | FAILOVER CAPABILITY*
[Withdrawn: Incorporated into SI-13].

(6) *INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | COMPONENT PROTECTION*
The organization protects backup and restoration hardware, firmware, and software.

Supplemental Guidance: Protection of backup and restoration hardware, firmware, and software components includes both physical and technical safeguards. Backup and restoration software includes, for example, router tables, compilers, and other security-relevant system software. Related controls: AC-3, AC-6, PE-3.

References: Federal Continuity Directive 1; NIST Special Publication 800-34.

Priority and Baseline Allocation:

P1	**LOW** CP-10	**MOD** CP-10 (2)	**HIGH** CP-10 (2) (4)

CP-11 ALTERNATE COMMUNICATIONS PROTOCOLS

Control: The information system provides the capability to employ [*Assignment: organization-defined alternative communications protocols*] in support of maintaining continuity of operations.

Supplemental Guidance: Contingency plans and the associated training and testing for those plans, incorporate an alternate communications protocol capability as part of increasing the resilience of organizational information systems. Alternate communications protocols include, for example, switching from Transmission Control Protocol/Internet Protocol (TCP/IP) Version 4 to TCP/IP Version 6. Switching communications protocols may affect software applications and therefore, the potential side effects of introducing alternate communications protocols are analyzed prior to implementation.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

CP-12 SAFE MODE

Control: The information system, when [*Assignment: organization-defined conditions*] are detected, enters a safe mode of operation with [*Assignment: organization-defined restrictions of safe mode of operation*].

Supplemental Guidance: For information systems supporting critical missions/business functions including, for example, military operations and weapons systems, civilian space operations, nuclear power plant operations, and air traffic control operations (especially real-time operational environments), organizations may choose to identify certain conditions under which those systems revert to a predefined safe mode of operation. The safe mode of operation, which can be activated automatically or manually, restricts the types of activities or operations information systems could execute when those conditions are encountered. Restriction includes, for example, allowing only certain functions that could be carried out under limited power or with reduced communications bandwidth.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

CP-13 ALTERNATIVE SECURITY MECHANISMS

Control: The organization employs [*Assignment: organization-defined alternative or supplemental security mechanisms*] for satisfying [*Assignment: organization-defined security functions*] when the primary means of implementing the security function is unavailable or compromised.

Supplemental Guidance: This control supports information system resiliency and contingency planning/continuity of operations. To ensure mission/business continuity, organizations can implement alternative or supplemental security mechanisms. These mechanisms may be less effective than the primary mechanisms (e.g., not as easy to use, not as scalable, or not as secure). However, having the capability to readily employ these alternative/supplemental mechanisms enhances overall mission/business continuity that might otherwise be adversely impacted if organizational operations had to be curtailed until the primary means of implementing the functions was restored. Given the cost and level of effort required to provide such alternative capabilities, this control would typically be applied only to critical security capabilities provided by information systems, system components, or information system services. For example, an organization may issue to senior executives and system administrators one-time pads in case multifactor tokens, the organization's standard means for secure remote authentication, is compromised. Related control: CP-2.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: IDENTIFICATION AND AUTHENTICATION

IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

   1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and

b. Reviews and updates the current:

   1. Identification and authentication policy [*Assignment: organization-defined frequency*]; and

   2. Identification and authentication procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: FIPS Publication 201; NIST Special Publications 800-12, 800-63, 800-73, 800-76, 800-78, 800-100.

Priority and Baseline Allocation:

P1	**LOW** IA-1	**MOD** IA-1	**HIGH** IA-1

IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Control: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

Supplemental Guidance: Organizational users include employees or individuals that organizations deem to have equivalent status of employees (e.g., contractors, guest researchers). This control applies to all accesses other than: (i) accesses that are explicitly identified and documented in AC-14; and (ii) accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity. Organizations employ passwords, tokens, or biometrics to authenticate user identities, or in the case multifactor authentication, or some combination thereof. Access to organizational information systems is defined as either local access or network access. Local access is any access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to

organizational information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks (e.g., the Internet). Internal networks include local area networks and wide area networks. In addition, the use of encrypted virtual private networks (VPNs) for network connections between organization-controlled endpoints and non-organization controlled endpoints may be treated as internal networks from the perspective of protecting the confidentiality and integrity of information traversing the network.

Organizations can satisfy the identification and authentication requirements in this control by complying with the requirements in Homeland Security Presidential Directive 12 consistent with the specific organizational implementation plans. Multifactor authentication requires the use of two or more different factors to achieve authentication. The factors are defined as: (i) something you know (e.g., password, personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD common access card. In addition to identifying and authenticating users at the information system level (i.e., at logon), organizations also employ identification and authentication mechanisms at the application level, when necessary, to provide increased information security. Identification and authentication requirements for other than organizational users are described in IA-8. Related controls: AC-2, AC-3, AC-14, AC-17, AC-18, IA-4, IA-5, IA-8.

Control Enhancements:

(1) *IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS*

The information system implements multifactor authentication for network access to privileged accounts.

Supplemental Guidance: Related control: AC-6.

(2) *IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS*

The information system implements multifactor authentication for network access to non-privileged accounts.

(3) *IDENTIFICATION AND AUTHENTICATION | LOCAL ACCESS TO PRIVILEGED ACCOUNTS*

The information system implements multifactor authentication for local access to privileged accounts.

Supplemental Guidance: Related control: AC-6.

(4) *IDENTIFICATION AND AUTHENTICATION | LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS*

The information system implements multifactor authentication for local access to non-privileged accounts.

(5) *IDENTIFICATION AND AUTHENTICATION | GROUP AUTHENTICATION*

The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.

Supplemental Guidance: Requiring individuals to use individual authenticators as a second level of authentication helps organizations to mitigate the risk of using group authenticators.

(6) *IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - SEPARATE DEVICE*

The information system implements multifactor authentication for network access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [*Assignment: organization-defined strength of mechanism requirements*].

Supplemental Guidance: Related control: AC-6.

(7) *IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - SEPARATE DEVICE*

The information system implements multifactor authentication for network access to non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [*Assignment: organization-defined strength of mechanism requirements*].

(8) *IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT*

The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.

Supplemental Guidance: Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.

(9) *IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - REPLAY RESISTANT*

The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.

Supplemental Guidance: Authentication processes resist replay attacks if it is impractical to achieve successful authentications by recording/replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.

(10) *IDENTIFICATION AND AUTHENTICATION | SINGLE SIGN-ON*

The information system provides a single sign-on capability for [*Assignment: organization-defined list of information system accounts and services*].

Supplemental Guidance: Single sign-on enables users to log in once and gain access to multiple information system resources. Organizations consider the operational efficiencies provided by single sign-on capabilities with the increased risk from disclosures of single authenticators providing access to multiple system resources.

(11) *IDENTIFICATION AND AUTHENTICATION | REMOTE ACCESS - SEPARATE DEVICE*

The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [*Assignment: organization-defined strength of mechanism requirements*].

Supplemental Guidance: For remote access to privileged/non-privileged accounts, the purpose of requiring a device that is separate from the information system gaining access for one of the factors during multifactor authentication is to reduce the likelihood of compromising authentication credentials stored on the system. For example, adversaries deploying malicious code on organizational information systems can potentially compromise such credentials resident on the system and subsequently impersonate authorized users. Related control: AC-6.

(12) *IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV CREDENTIALS*

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.

Supplemental Guidance: This control enhancement applies to organizations implementing logical access control systems (LACS) and physical access control systems (PACS). Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials. Related controls: AU-2, PE-3, SA-4.

(13) *IDENTIFICATION AND AUTHENTICATION | OUT-OF-BAND AUTHENTICATION*

The information system implements [*Assignment: organization-defined out-of-band authentication*] under [*Assignment: organization-defined conditions*].

Supplemental Guidance: Out-of-band authentication (OOBA) refers to the use of two separate communication paths to identify and authenticate users or devices to an information system. The first path (i.e., the in-band path), is used to identify and authenticate users or devices, and generally is the path through which information flows. The second path (i.e., the out-of-band path) is used to independently verify the authentication and/or requested action. For example, a user authenticates via a notebook computer to a remote server to which the user desires access, and requests some action of the server via that communication path. Subsequently, the server contacts the user via the user's cell phone to verify that the requested action originated

from the user. The user may either confirm the intended action to an individual on the telephone or provide an authentication code via the telephone. This type of authentication can be employed by organizations to mitigate actual or suspected man-in the-middle attacks. The conditions for activation can include, for example, suspicious activities, new threat indicators or elevated threat levels, or the impact level or classification level of information in requested transactions. Related controls: IA-10, IA-11, SC-37.

References: HSPD-12; OMB Memoranda 04-04, 06-16, 11-11; FIPS Publication 201; NIST Special Publications 800-63, 800-73, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: http://idmanagement.gov.

Priority and Baseline Allocation:

P1	**LOW** IA-2 (1) (12)	**MOD** IA-2 (1) (2) (3) (8) (11) (12)	**HIGH** IA-2 (1) (2) (3) (4) (8) (9) (11) (12)

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

Control: The information system uniquely identifies and authenticates [*Assignment: organization-defined specific and/or types of devices*] before establishing a [*Selection (one or more): local; remote; network*] connection.

Supplemental Guidance: Organizational devices requiring unique device-to-device identification and authentication may be defined by type, by device, or by a combination of type/device. Information systems typically use either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify/authenticate devices on local and/or wide area networks. Organizations determine the required strength of authentication mechanisms by the security categories of information systems. Because of the challenges of applying this control on large scale, organizations are encouraged to only apply the control to those limited number (and type) of devices that truly need to support this capability. Related controls: AC-17, AC-18, AC-19, CA-3, IA-4, IA-5.

Control Enhancements:

(1) *DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION*

The information system authenticates [*Assignment: organization-defined specific devices and/or types of devices*] before establishing [*Selection (one or more): local; remote; network*] connection using bidirectional authentication that is cryptographically based.

Supplemental Guidance: A local connection is any connection with a device communicating without the use of a network. A network connection is any connection with a device that communicates through a network (e.g., local area or wide area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Bidirectional authentication provides stronger safeguards to validate the identity of other devices for connections that are of greater risk (e.g., remote connections). Related controls: SC-8, SC-12, SC-13.

(2) *DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL NETWORK AUTHENTICATION*

[Withdrawn: Incorporated into IA-3 (1)].

(3) *DEVICE IDENTIFICATION AND AUTHENTICATION | DYNAMIC ADDRESS ALLOCATION*

The organization:

(a) Standardizes dynamic address allocation lease information and the lease duration assigned to devices in accordance with [*Assignment: organization-defined lease information and lease duration*]; and

(b) Audits lease information when assigned to a device.

Supplemental Guidance: DHCP-enabled clients obtaining *leases* for IP addresses from DHCP servers, is a typical example of dynamic address allocation for devices. Related controls: AU-2, AU-3, AU-6, AU-12.

(4) *DEVICE IDENTIFICATION AND AUTHENTICATION | DEVICE ATTESTATION*

The organization ensures that device identification and authentication based on attestation is handled by [*Assignment: organization-defined configuration management process*].

Supplemental Guidance: Device attestation refers to the identification and authentication of a device based on its configuration and known operating state. This might be determined via some cryptographic hash of the device. If device attestation is the means of identification and authentication, then it is important that patches and updates to the device are handled via a configuration management process such that the those patches/updates are done securely and at the same time do not disrupt the identification and authentication to other devices.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** IA-3	**HIGH** IA-3

IA-4 IDENTIFIER MANAGEMENT

Control: The organization manages information system identifiers by:

a. Receiving authorization from [*Assignment: organization-defined personnel or roles*] to assign an individual, group, role, or device identifier;

b. Selecting an identifier that identifies an individual, group, role, or device;

c. Assigning the identifier to the intended individual, group, role, or device;

d. Preventing reuse of identifiers for [*Assignment: organization-defined time period*]; and

e. Disabling the identifier after [*Assignment: organization-defined time period of inactivity*].

Supplemental Guidance: Common device identifiers include, for example, media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). Typically, individual identifiers are the user names of the information system accounts assigned to those individuals. In such instances, the account management activities of AC-2 use account names provided by IA-4. This control also addresses individual identifiers not necessarily associated with information system accounts (e.g., identifiers used in physical security control databases accessed by badge reader systems for access to information systems). Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices. Related controls: AC-2, IA-2, IA-3, IA-5, IA-8, SC-37.

Control Enhancements:

(1) *IDENTIFIER MANAGEMENT | PROHIBIT ACCOUNT IDENTIFIERS AS PUBLIC IDENTIFIERS*

The organization prohibits the use of information system account identifiers that are the same as public identifiers for individual electronic mail accounts.

Supplemental Guidance: Prohibiting the use of information systems account identifiers that are the same as some public identifier such as the individual identifier section of an electronic mail address, makes it more difficult for adversaries to guess user identifiers on organizational information systems. Related control: AT-2.

(2) *IDENTIFIER MANAGEMENT | SUPERVISOR AUTHORIZATION*

The organization requires that the registration process to receive an individual identifier includes supervisor authorization.

(3) *IDENTIFIER MANAGEMENT | MULTIPLE FORMS OF CERTIFICATION*

The organization requires multiple forms of certification of individual identification such as documentary evidence or a combination of documents and biometrics be presented to the registration authority.

Supplemental Guidance: Requiring multiple forms of identification reduces the likelihood of individuals using fraudulent identification to establish an identity, or at least increases the work factor of potential adversaries.

(4) *IDENTIFIER MANAGEMENT | IDENTIFY USER STATUS*

The organization manages individual identifiers by uniquely identifying each individual as [*Assignment: organization-defined characteristic identifying individual status*].

Supplemental Guidance: Characteristics identifying the status of individuals include, for example, contractors and foreign nationals. Identifying the status of individuals by specific characteristics provides additional information about the people with whom organizational personnel are communicating. For example, it might be useful for a government employee to know that one of the individuals on an email message is a contractor. Related control: AT-2.

(5) *IDENTIFIER MANAGEMENT | DYNAMIC MANAGEMENT*

The information system dynamically manages identifiers.

Supplemental Guidance: In contrast to conventional approaches to identification which presume static accounts for preregistered users, many distributed information systems including, for example, service-oriented architectures, rely on establishing identifiers at run time for entities that were previously unknown. In these situations, organizations anticipate and provision for the dynamic establishment of identifiers. Preestablished trust relationships and mechanisms with appropriate authorities to validate identities and related credentials are essential. Related control: AC-16.

(6) *IDENTIFIER MANAGEMENT | CROSS-ORGANIZATION MANAGEMENT*

The organization coordinates with [*Assignment: organization-defined external organizations*] for cross-organization management of identifiers.

Supplemental Guidance: Cross-organization identifier management provides the capability for organizations to appropriately identify individuals, groups, roles, or devices when conducting cross-organization activities involving the processing, storage, or transmission of information.

(7) *IDENTIFIER MANAGEMENT | IN-PERSON REGISTRATION*

The organization requires that the registration process to receive an individual identifier be conducted in person before a designated registration authority.

Supplemental Guidance: In-person registration reduces the likelihood of fraudulent identifiers being issued because it requires the physical presence of individuals and actual face-to-face interactions with designated registration authorities.

References: FIPS Publication 201; NIST Special Publications 800-73, 800-76, 800-78.

Priority and Baseline Allocation:

P1	**LOW** IA-4	**MOD** IA-4	**HIGH** IA-4

IA-5 AUTHENTICATOR MANAGEMENT

Control: The organization manages information system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;

b. Establishing initial authenticator content for authenticators defined by the organization;

c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;

d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;

e. Changing default content of authenticators prior to information system installation;

f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;

g. Changing/refreshing authenticators [*Assignment: organization-defined time period by authenticator type*];

h. Protecting authenticator content from unauthorized disclosure and modification;

i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and

j. Changing authenticators for group/role accounts when membership to those accounts changes.

Supplemental Guidance: Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). In many cases, developers ship information system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored within organizational information systems (e.g., passwords stored in hashed or encrypted formats, files containing encrypted or hashed passwords accessible with administrator privileges). Information systems support individual authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Specific actions that can be taken to safeguard authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing individual authenticators with others, and reporting lost, stolen, or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords. Related controls: AC-2, AC-3, AC-6, CM-6, IA-2, IA-4, IA-8, PL-4, PS-5, PS-6, SC-12, SC-13, SC-17, SC-28.

Control Enhancements:

(1) *AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION*

The information system, for password-based authentication:

(a) Enforces minimum password complexity of [*Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type*];

(b) Enforces at least the following number of changed characters when new passwords are created: [*Assignment: organization-defined number*];

(c) Stores and transmits only cryptographically-protected passwords;

(d) Enforces password minimum and maximum lifetime restrictions of [*Assignment: organization-defined numbers for lifetime minimum, lifetime maximum*];

(e) Prohibits password reuse for [*Assignment: organization-defined number*] generations; and

(f) Allows the use of a temporary password for system logons with an immediate change to a permanent password.

Supplemental Guidance: This control enhancement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are part of multifactor authenticators. This control enhancement does *not* apply when passwords are used to unlock hardware authenticators (e.g., Personal Identity

Verification cards). The implementation of such password mechanisms may not meet all of the requirements in the enhancement. Cryptographically-protected passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords. The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. Password lifetime restrictions do not apply to temporary passwords. To mitigate certain brute force attacks against passwords, organizations may also consider salting passwords. Related control: IA-6.

(2) *AUTHENTICATOR MANAGEMENT | PKI-BASED AUTHENTICATION*

The information system, for PKI-based authentication:

(a) Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;

(b) Enforces authorized access to the corresponding private key;

(c) Maps the authenticated identity to the account of the individual or group; and

(d) Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

Supplemental Guidance: Status information for certification paths includes, for example, certificate revocation lists or certificate status protocol responses. For PIV cards, validation of certifications involves the construction and verification of a certification path to the Common Policy Root trust anchor including certificate policy processing. Related control: IA-6.

(3) *AUTHENTICATOR MANAGEMENT | IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION*

The organization requires that the registration process to receive [*Assignment: organization-defined types of and/or specific authenticators*] be conducted [*Selection: in person; by a trusted third party*] before [*Assignment: organization-defined registration authority*] with authorization by *[Assignment: organization-defined personnel or roles*].

(4) *AUTHENTICATOR MANAGEMENT | AUTOMATED SUPPORT FOR PASSWORD STRENGTH DETERMINATION*

The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy [*Assignment: organization-defined requirements*].

Supplemental Guidance: This control enhancement focuses on the creation of strong passwords and the characteristics of such passwords (e.g., complexity) prior to use, the enforcement of which is carried out by organizational information systems in IA-5 (1). Related controls: CA-2, CA-7, RA-5.

(5) *AUTHENTICATOR MANAGEMENT | CHANGE AUTHENTICATORS PRIOR TO DELIVERY*

The organization requires developers/installers of information system components to provide unique authenticators or change default authenticators prior to delivery/installation.

Supplemental Guidance: This control enhancement extends the requirement for organizations to change default authenticators upon information system installation, by requiring developers and/or installers to provide unique authenticators or change default authenticators for system components prior to delivery and/or installation. However, it typically does not apply to the developers of commercial off-the-shelve information technology products. Requirements for unique authenticators can be included in acquisition documents prepared by organizations when procuring information systems or system components.

(6) *AUTHENTICATOR MANAGEMENT | PROTECTION OF AUTHENTICATORS*

The organization protects authenticators commensurate with the security category of the information to which use of the authenticator permits access.

Supplemental Guidance: For information systems containing multiple security categories of information without reliable physical or logical separation between categories, authenticators used to grant access to the systems are protected commensurate with the highest security category of information on the systems.

(7) *AUTHENTICATOR MANAGEMENT | NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS*

The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.

Supplemental Guidance: Organizations exercise caution in determining whether embedded or stored authenticators are in encrypted or unencrypted form. If authenticators are used in the

manner stored, then those representations are considered unencrypted authenticators. This is irrespective of whether that representation is perhaps an encrypted version of something else (e.g., a password).

(8) *AUTHENTICATOR MANAGEMENT | MULTIPLE INFORMATION SYSTEM ACCOUNTS*

The organization implements [*Assignment: organization-defined security safeguards*] to manage the risk of compromise due to individuals having accounts on multiple information systems.

Supplemental Guidance: When individuals have accounts on multiple information systems, there is the risk that the compromise of one account may lead to the compromise of other accounts if individuals use the same authenticators. Possible alternatives include, for example: (i) having different authenticators on all systems; (ii) employing some form of single sign-on mechanism; or (iii) including some form of one-time passwords on all systems.

(9) *AUTHENTICATOR MANAGEMENT | CROSS-ORGANIZATION CREDENTIAL MANAGEMENT*

The organization coordinates with [*Assignment: organization-defined external organizations*] for cross-organization management of credentials.

Supplemental Guidance: Cross-organization management of credentials provides the capability for organizations to appropriately authenticate individuals, groups, roles, or devices when conducting cross-organization activities involving the processing, storage, or transmission of information.

(10) *AUTHENTICATOR MANAGEMENT | DYNAMIC CREDENTIAL ASSOCIATION*

The information system dynamically provisions identities.

Supplemental Guidance: Authentication requires some form of binding between an identity and the authenticator used to confirm the identity. In conventional approaches, this binding is established by pre-provisioning both the identity and the authenticator to the information system. For example, the binding between a username (i.e., identity) and a password (i.e., authenticator) is accomplished by provisioning the identity and authenticator as a pair in the information system. New authentication techniques allow the binding between the identity and the authenticator to be implemented outside an information system. For example, with smartcard credentials, the identity and the authenticator are bound together on the card. Using these credentials, information systems can authenticate identities that have not been pre-provisioned, dynamically provisioning the identity after authentication. In these situations, organizations can anticipate the dynamic provisioning of identities. Preestablished trust relationships and mechanisms with appropriate authorities to validate identities and related credentials are essential.

(11) *AUTHENTICATOR MANAGEMENT | HARDWARE TOKEN-BASED AUTHENTICATION*

The information system, for hardware token-based authentication, employs mechanisms that satisfy [*Assignment: organization-defined token quality requirements*].

Supplemental Guidance: Hardware token-based authentication typically refers to the use of PKI-based tokens, such as the U.S. Government Personal Identity Verification (PIV) card. Organizations define specific requirements for tokens, such as working with a particular PKI.

(12) *AUTHENTICATOR MANAGEMENT | BIOMETRIC AUTHENTICATION*

The information system, for biometric-based authentication, employs mechanisms that satisfy [*Assignment: organization-defined biometric quality requirements*].

Supplemental Guidance: Unlike password-based authentication which provides exact matches of user-input passwords to stored passwords, biometric authentication does not provide such exact matches. Depending upon the type of biometric and the type of collection mechanism, there is likely to be some divergence from the presented biometric and stored biometric which serves as the basis of comparison. There will likely be both false positives and false negatives when making such comparisons. The rate at which the false accept and false reject rates are equal is known as the crossover rate. Biometric quality requirements include, for example, acceptable crossover rates, as that essentially reflects the accuracy of the biometric.

(13) *AUTHENTICATOR MANAGEMENT | EXPIRATION OF CACHED AUTHENTICATORS*

The information system prohibits the use of cached authenticators after [*Assignment: organization-defined time period*].

(14) *AUTHENTICATOR MANAGEMENT | MANAGING CONTENT OF PKI TRUST STORES*

The organization, for PKI-based authentication, employs a deliberate organization-wide methodology for managing the content of PKI trust stores installed across all platforms including networks, operating systems, browsers, and applications.

(15) *AUTHENTICATOR MANAGEMENT | FICAM-APPROVED PRODUCTS AND SERVICES*

The organization uses only FICAM-approved path discovery and validation products and services.

Supplemental Guidance: Federal Identity, Credential, and Access Management (FICAM)-approved path discovery and validation products and services are those products and services that have been approved through the FICAM conformance program, where applicable.

References: OMB Memoranda 04-04, 11-11; FIPS Publication 201; NIST Special Publications 800-73, 800-63, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: http://idmanagement.gov.

Priority and Baseline Allocation:

P1	**LOW** IA-5 (1) (11)	**MOD** IA-5 (1) (2) (3) (11)	**HIGH** IA-5 (1) (2) (3) (11)

IA-6 AUTHENTICATOR FEEDBACK

Control: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Supplemental Guidance: The feedback from information systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of information systems or system components, for example, desktops/notebooks with relatively large monitors, the threat (often referred to as shoulder surfing) may be significant. For other types of systems or components, for example, mobile devices with 2-4 inch screens, this threat may be less significant, and may need to be balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring the authenticator feedback is selected accordingly. Obscuring the feedback of authentication information includes, for example, displaying asterisks when users type passwords into input devices, or displaying feedback for a very limited time before fully obscuring it. Related control: PE-18.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** IA-6	**MOD** IA-6	**HIGH** IA-6

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

Control: The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

Supplemental Guidance: Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role. Related controls: SC-12, SC-13.

Control Enhancements: None.

References: FIPS Publication 140; Web: http://csrc.nist.gov/groups/STM/cmvp/index.html.

Priority and Baseline Allocation:

P1	**LOW** IA-7	**MOD** IA-7	**HIGH** IA-7

IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

Control: The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

Supplemental Guidance: Non-organizational users include information system users other than organizational users explicitly covered by IA-2. These individuals are uniquely identified and authenticated for accesses other than those accesses explicitly identified and documented in AC-14. In accordance with the E-Authentication E-Government initiative, authentication of non-organizational users accessing federal information systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Organizations use risk assessments to determine authentication needs and consider scalability, practicality, and security in balancing the need to ensure ease of use for access to federal information and information systems with the need to protect and adequately mitigate risk. IA-2 addresses identification and authentication requirements for access to information systems by organizational users. Related controls: AC-2, AC-14, AC-17, AC-18, IA-2, IA-4, IA-5, MA-4, RA-3, SA-12, SC-8.

Control Enhancements:

(1) *IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES*

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.

Supplemental Guidance: This control enhancement applies to logical access control systems (LACS) and physical access control systems (PACS). Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials. Related controls: AU-2, PE-3, SA-4.

(2) *IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF THIRD-PARTY CREDENTIALS*

The information system accepts only FICAM-approved third-party credentials.

Supplemental Guidance: This control enhancement typically applies to organizational information systems that are accessible to the general public, for example, public-facing websites. Third-party credentials are those credentials issued by nonfederal government entities approved by the Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative. Approved third-party credentials meet or exceed the set of minimum federal government-wide technical, security, privacy, and organizational maturity requirements. This allows federal government relying parties to trust such credentials at their approved assurance levels. Related control: AU-2.

(3) *IDENTIFICATION AND AUTHENTICATION | USE OF FICAM-APPROVED PRODUCTS*

The organization employs only FICAM-approved information system components in [*Assignment: organization-defined information systems*] to accept third-party credentials.

Supplemental Guidance: This control enhancement typically applies to information systems that are accessible to the general public, for example, public-facing websites. FICAM-approved information system components include, for example, information technology products and software libraries that have been approved by the Federal Identity, Credential, and Access Management conformance program. Related control: SA-4.

(4) *IDENTIFICATION AND AUTHENTICATION | USE OF FICAM-ISSUED PROFILES*

The information system conforms to FICAM-issued profiles.

Supplemental Guidance: This control enhancement addresses open identity management standards. To ensure that these standards are viable, robust, reliable, sustainable (e.g., available in commercial information technology products), and interoperable as documented, the United States Government assesses and scopes identity management standards and technology implementations against applicable federal legislation, directives, policies, and requirements. The result is FICAM-issued implementation profiles of approved protocols (e.g., FICAM authentication protocols such as SAML 2.0 and OpenID 2.0, as well as other protocols such as the FICAM Backend Attribute Exchange). Related control: SA-4.

(5) *IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV-I CREDENTIALS*

The information system accepts and electronically verifies Personal Identity Verification-I (PIV-I) credentials.

Supplemental Guidance: This control enhancement: (i) applies to logical and physical access control systems; and (ii) addresses Non-Federal Issuers (NFIs) of identity cards that desire to interoperate with United States Government Personal Identity Verification (PIV) information systems and that can be trusted by federal government-relying parties. The X.509 certificate policy for the Federal Bridge Certification Authority (FBCA) addresses PIV-I requirements. The PIV-I card is suitable for Assurance Level 4 as defined in OMB Memorandum 04-04 and NIST Special Publication 800-63, and multifactor authentication as defined in NIST Special Publication 800-116. PIV-I credentials are those credentials issued by a PIV-I provider whose PIV-I certificate policy maps to the Federal Bridge PIV-I Certificate Policy. A PIV-I provider is cross-certified (directly or through another PKI bridge) with the FBCA with policies that have been mapped and approved as meeting the requirements of the PIV-I policies defined in the FBCA certificate policy. Related control: AU-2.

References: OMB Memoranda 04-04, 11-11, 10-06-2011; FICAM Roadmap and Implementation Guidance; FIPS Publication 201; NIST Special Publications 800-63, 800-116; National Strategy for Trusted Identities in Cyberspace; Web: http://idmanagement.gov.

Priority and Baseline Allocation:

P1	**LOW** IA-8 (1) (2) (3) (4)	**MOD** IA-8 (1) (2) (3) (4)	**HIGH** IA-8 (1) (2) (3) (4)

IA-9 SERVICE IDENTIFICATION AND AUTHENTICATION

Control: The organization identifies and authenticates [*Assignment: organization-defined information system services*] using [*Assignment: organization-defined security safeguards*].

Supplemental Guidance: This control supports service-oriented architectures and other distributed architectural approaches requiring the identification and authentication of information system services. In such architectures, external services often appear dynamically. Therefore, information systems should be able to determine in a dynamic manner, if external providers and associated services are authentic. Safeguards implemented by organizational information systems to validate provider and service authenticity include, for example, information or code signing, provenance graphs, and/or electronic signatures indicating or including the sources of services.

Control Enhancements:

(1) *SERVICE IDENTIFICATION AND AUTHENTICATION | INFORMATION EXCHANGE*

The organization ensures that service providers receive, validate, and transmit identification and authentication information.

(2) *SERVICE IDENTIFICATION AND AUTHENTICATION | TRANSMISSION OF DECISIONS*

The organization ensures that identification and authentication decisions are transmitted between [*Assignment: organization-defined services*] consistent with organizational policies.

Supplemental Guidance: For distributed architectures (e.g., service-oriented architectures), the decisions regarding the validation of identification and authentication claims may be made by services separate from the services acting on those decisions. In such situations, it is necessary

Supplemental Guidance: This control enhancement addresses open identity management standards. To ensure that these standards are viable, robust, reliable, sustainable (e.g., available in commercial information technology products), and interoperable as documented, the United States Government assesses and scopes identity management standards and technology implementations against applicable federal legislation, directives, policies, and requirements. The result is FICAM-issued implementation profiles of approved protocols (e.g., FICAM authentication protocols such as SAML 2.0 and OpenID 2.0, as well as other protocols such as the FICAM Backend Attribute Exchange). Related control: SA-4.

(5) *IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV-I CREDENTIALS*

The information system accepts and electronically verifies Personal Identity Verification-I (PIV-I) credentials.

Supplemental Guidance: This control enhancement: (i) applies to logical and physical access control systems; and (ii) addresses Non-Federal Issuers (NFIs) of identity cards that desire to interoperate with United States Government Personal Identity Verification (PIV) information systems and that can be trusted by federal government-relying parties. The X.509 certificate policy for the Federal Bridge Certification Authority (FBCA) addresses PIV-I requirements. The PIV-I card is suitable for Assurance Level 4 as defined in OMB Memorandum 04-04 and NIST Special Publication 800-63, and multifactor authentication as defined in NIST Special Publication 800-116. PIV-I credentials are those credentials issued by a PIV-I provider whose PIV-I certificate policy maps to the Federal Bridge PIV-I Certificate Policy. A PIV-I provider is cross-certified (directly or through another PKI bridge) with the FBCA with policies that have been mapped and approved as meeting the requirements of the PIV-I policies defined in the FBCA certificate policy. Related control: AU-2.

References: OMB Memoranda 04-04, 11-11, 10-06-2011; FICAM Roadmap and Implementation Guidance; FIPS Publication 201; NIST Special Publications 800-63, 800-116; National Strategy for Trusted Identities in Cyberspace; Web: http://idmanagement.gov.

Priority and Baseline Allocation:

P1	**LOW** IA-8 (1) (2) (3) (4)	**MOD** IA-8 (1) (2) (3) (4)	**HIGH** IA-8 (1) (2) (3) (4)

IA-9 SERVICE IDENTIFICATION AND AUTHENTICATION

Control: The organization identifies and authenticates [*Assignment: organization-defined information system services*] using [*Assignment: organization-defined security safeguards*].

Supplemental Guidance: This control supports service-oriented architectures and other distributed architectural approaches requiring the identification and authentication of information system services. In such architectures, external services often appear dynamically. Therefore, information systems should be able to determine in a dynamic manner, if external providers and associated services are authentic. Safeguards implemented by organizational information systems to validate provider and service authenticity include, for example, information or code signing, provenance graphs, and/or electronic signatures indicating or including the sources of services.

Control Enhancements:

(1) *SERVICE IDENTIFICATION AND AUTHENTICATION | INFORMATION EXCHANGE*

The organization ensures that service providers receive, validate, and transmit identification and authentication information.

(2) *SERVICE IDENTIFICATION AND AUTHENTICATION | TRANSMISSION OF DECISIONS*

The organization ensures that identification and authentication decisions are transmitted between [*Assignment: organization-defined services*] consistent with organizational policies.

Supplemental Guidance: For distributed architectures (e.g., service-oriented architectures), the decisions regarding the validation of identification and authentication claims may be made by services separate from the services acting on those decisions. In such situations, it is necessary

to provide the identification and authentication decisions (as opposed to the actual identifiers and authenticators) to the services that need to act on those decisions. Related control: SC-8.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

IA-10 ADAPTIVE IDENTIFICATION AND AUTHENTICATION

Control: The organization requires that individuals accessing the information system employ [*Assignment: organization-defined supplemental authentication techniques or mechanisms*] under specific [*Assignment: organization-defined circumstances or situations*].

Supplemental Guidance: Adversaries may compromise individual authentication mechanisms and subsequently attempt to impersonate legitimate users. This situation can potentially occur with any authentication mechanisms employed by organizations. To address this threat, organizations may employ specific techniques/mechanisms and establish protocols to assess suspicious behavior (e.g., individuals accessing information that they do not typically access as part of their normal duties, roles, or responsibilities, accessing greater quantities of information than the individuals would routinely access, or attempting to access information from suspicious network addresses). In these situations when certain preestablished conditions or triggers occur, organizations can require selected individuals to provide additional authentication information. Another potential use for adaptive identification and authentication is to increase the strength of mechanism based on the number and/or types of records being accessed. Related controls: AU-6, SI-4.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

IA-11 RE-AUTHENTICATION

Control: The organization requires users and devices to re-authenticate when [*Assignment: organization-defined circumstances or situations requiring re-authentication*].

Supplemental Guidance: In addition to the re-authentication requirements associated with session locks, organizations may require re-authentication of individuals and/or devices in other situations including, for example: (i) when authenticators change; (ii), when roles change; (iii) when security categories of information systems change; (iv), when the execution of privileged functions occurs; (v) after a fixed period of time; or (vi) periodically. Related control: AC-11.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: INCIDENT RESPONSE

IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

   1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and

b. Reviews and updates the current:

   1. Incident response policy [*Assignment: organization-defined frequency*]; and

   2. Incident response procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IR family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-61, 800-83, 800-100.

Priority and Baseline Allocation:

P1	**LOW** IR-1	**MOD** IR-1	**HIGH** IR-1

IR-2 INCIDENT RESPONSE TRAINING

Control: The organization provides incident response training to information system users consistent with assigned roles and responsibilities:

a. Within [*Assignment: organization-defined time period*] of assuming an incident response role or responsibility;

b. When required by information system changes; and

c. [*Assignment: organization-defined frequency*] thereafter.

Supplemental Guidance: Incident response training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the information system; system administrators may require additional training on how to handle/remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources. Related controls: AT-3, CP-3, IR-8.

Control Enhancements:

(1) *INCIDENT RESPONSE TRAINING | SIMULATED EVENTS*

The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

(2) *INCIDENT RESPONSE TRAINING | AUTOMATED TRAINING ENVIRONMENTS*

The organization employs automated mechanisms to provide a more thorough and realistic incident response training environment.

References: NIST Special Publications 800-16, 800-50.

Priority and Baseline Allocation:

P2	**LOW** IR-2	**MOD** IR-2	**HIGH** IR-2 (1) (2)

IR-3 INCIDENT RESPONSE TESTING

Control: The organization tests the incident response capability for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests*] to determine the incident response effectiveness and documents the results.

Supplemental Guidance: Organizations test incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations (parallel/full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response. Related controls: CP-4, IR-8.

Control Enhancements:

(1) *INCIDENT RESPONSE TESTING | AUTOMATED TESTING*

The organization employs automated mechanisms to more thoroughly and effectively test the incident response capability.

Supplemental Guidance: Organizations use automated mechanisms to more thoroughly and effectively test incident response capabilities, for example: (i) by providing more complete coverage of incident response issues; (ii) by selecting more realistic test scenarios and test environments; and (iii) by stressing the response capability. Related control: AT-2.

(2) *INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS*

The organization coordinates incident response testing with organizational elements responsible for related plans.

Supplemental Guidance: Organizational plans related to incident response testing include, for example, Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and Occupant Emergency Plans.

References: NIST Special Publications 800-84, 800-115.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** IR-3 (2)	**HIGH** IR-3 (2)

IR-4 INCIDENT HANDLING

Control: The organization:

a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;

b. Coordinates incident handling activities with contingency planning activities; and

c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

Supplemental Guidance: Organizations recognize that incident response capability is dependent on the capabilities of organizational information systems and the mission/business processes being supported by those systems. Therefore, organizations consider incident response as part of the definition, design, and development of mission/business processes and information systems. Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function). Related controls: AU-6, CM-6, CP-2, CP-4, IR-2, IR-3, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.

Control Enhancements:

(1) *INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES*

The organization employs automated mechanisms to support the incident handling process.

Supplemental Guidance: Automated mechanisms supporting incident handling processes include, for example, online incident management systems.

(2) *INCIDENT HANDLING | DYNAMIC RECONFIGURATION*

The organization includes dynamic reconfiguration of [*Assignment: organization-defined information system components*] as part of the incident response capability.

Supplemental Guidance: Dynamic reconfiguration includes, for example, changes to router rules, access control lists, intrusion detection/prevention system parameters, and filter rules for firewalls and gateways. Organizations perform dynamic reconfiguration of information systems, for example, to stop attacks, to misdirect attackers, and to isolate components of systems, thus limiting the extent of the damage from breaches or compromises. Organizations include time frames for achieving the reconfiguration of information systems in the definition of the reconfiguration capability, considering the potential need for rapid response in order to effectively address sophisticated cyber threats. Related controls: AC-2, AC-4, AC-16, CM-2, CM-3, CM-4.

(3) *INCIDENT HANDLING | CONTINUITY OF OPERATIONS*

The organization identifies [*Assignment: organization-defined classes of incidents*] and [*Assignment: organization-defined actions to take in response to classes of incidents*] to ensure continuation of organizational missions and business functions.

Supplemental Guidance: Classes of incidents include, for example, malfunctions due to design/implementation errors and omissions, targeted malicious attacks, and untargeted malicious attacks. Appropriate incident response actions include, for example, graceful degradation, information system shutdown, fall back to manual mode/alternative technology whereby the system operates differently, employing deceptive measures, alternate information flows, or operating in a mode that is reserved solely for when systems are under attack.

(4) *INCIDENT HANDLING | INFORMATION CORRELATION*

The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

Supplemental Guidance: Sometimes the nature of a threat event, for example, a hostile cyber attack, is such that it can only be observed by bringing together information from different sources including various reports and reporting procedures established by organizations.

(5) *INCIDENT HANDLING | AUTOMATIC DISABLING OF INFORMATION SYSTEM*

The organization implements a configurable capability to automatically disable the information system if [*Assignment: organization-defined security violations*] are detected.

(6) *INCIDENT HANDLING | INSIDER THREATS - SPECIFIC CAPABILITIES*

The organization implements incident handling capability for insider threats.

Supplemental Guidance: While many organizations address insider threat incidents as an inherent part of their organizational incident response capability, this control enhancement provides additional emphasis on this type of threat and the need for specific incident handling capabilities (as defined within organizations) to provide appropriate and timely responses.

(7) *INCIDENT HANDLING | INSIDER THREATS - INTRA-ORGANIZATION COORDINATION*

The organization coordinates incident handling capability for insider threats across [*Assignment: organization-defined components or elements of the organization*].

Supplemental Guidance: Incident handling for insider threat incidents (including preparation, detection and analysis, containment, eradication, and recovery) requires close coordination among a variety of organizational components or elements to be effective. These components or elements include, for example, mission/business owners, information system owners, human resources offices, procurement offices, personnel/physical security offices, operations personnel, and risk executive (function). In addition, organizations may require external support from federal, state, and local law enforcement agencies.

(8) *INCIDENT HANDLING | CORRELATION WITH EXTERNAL ORGANIZATIONS*

The organization coordinates with [*Assignment: organization-defined external organizations*] to correlate and share [*Assignment: organization-defined incident information*] to achieve a cross-organization perspective on incident awareness and more effective incident responses.

Supplemental Guidance: The coordination of incident information with external organizations including, for example, mission/business partners, military/coalition partners, customers, and multitiered developers, can provide significant benefits. Cross-organizational coordination with respect to incident handling can serve as an important risk management capability. This capability allows organizations to leverage critical information from a variety of sources to effectively respond to information security-related incidents potentially affecting the organization's operations, assets, and individuals.

(9) *INCIDENT HANDLING | DYNAMIC RESPONSE CAPABILITY*

The organization employs [*Assignment: organization-defined dynamic response capabilities*] to effectively respond to security incidents.

Supplemental Guidance: This control enhancement addresses the deployment of replacement or new capabilities in a timely manner in response to security incidents (e.g., adversary actions during hostile cyber attacks). This includes capabilities implemented at the mission/business process level (e.g., activating alternative mission/business processes) and at the information system level. Related control: CP-10.

(10) *INCIDENT HANDLING | SUPPLY CHAIN COORDINATION*

The organization coordinates incident handling activities involving supply chain events with other organizations involved in the supply chain.

Supplemental Guidance: Organizations involved in supply chain activities include, for example, system/product developers, integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Supply chain incidents include, for example, compromises/breaches involving information system components, information technology products, development processes or personnel, and distribution processes or warehousing facilities.

References: Executive Order 13587; NIST Special Publication 800-61.

Priority and Baseline Allocation:

P1	**LOW** IR-4	**MOD** IR-4 (1)	**HIGH** IR-4 (1) (4)

IR-5 INCIDENT MONITORING

Control: The organization tracks and documents information system security incidents.

Supplemental Guidance: Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. Related controls: AU-6, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.

Control Enhancements:

(1) *INCIDENT MONITORING | AUTOMATED TRACKING / DATA COLLECTION / ANALYSIS*

The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

Supplemental Guidance: Automated mechanisms for tracking security incidents and collecting/analyzing incident information include, for example, the Einstein network monitoring device and monitoring online Computer Incident Response Centers (CIRCs) or other electronic databases of incidents. Related controls: AU-7, IR-4.

References: NIST Special Publication 800-61.

Priority and Baseline Allocation:

P1	**LOW** IR-5	**MOD** IR-5	**HIGH** IR-5 (1)

IR-6 INCIDENT REPORTING

Control: The organization:

a. Requires personnel to report suspected security incidents to the organizational incident response capability within [*Assignment: organization-defined time period*]; and

b. Reports security incident information to [*Assignment: organization-defined authorities*].

Supplemental Guidance: The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. Suspected security incidents include, for example, the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling. Related controls: IR-4, IR-5, IR-8.

Control Enhancements:

(1) *INCIDENT REPORTING | AUTOMATED REPORTING*

The organization employs automated mechanisms to assist in the reporting of security incidents.

Supplemental Guidance: Related control: IR-7.

(2) *INCIDENT REPORTING | VULNERABILITIES RELATED TO INCIDENTS*

The organization reports information system vulnerabilities associated with reported security incidents to [*Assignment: organization-defined personnel or roles*].

(3) *INCIDENT REPORTING | COORDINATION WITH SUPPLY CHAIN*

The organization provides security incident information to other organizations involved in the supply chain for information systems or information system components related to the incident.

Supplemental Guidance: Organizations involved in supply chain activities include, for example, system/product developers, integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Supply chain incidents include, for example, compromises/breaches involving information system components, information technology products, development processes or personnel, and distribution processes or warehousing facilities. Organizations determine the appropriate information to share considering the value gained from support by external organizations with the potential for harm due to sensitive information being released to outside organizations of perhaps questionable trustworthiness.

References: NIST Special Publication 800-61; Web: http://www.us-cert.gov.

Priority and Baseline Allocation:

P1	**LOW** IR-6	**MOD** IR-6 (1)	**HIGH** IR-6 (1)

IR-7 INCIDENT RESPONSE ASSISTANCE

Control: The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

Supplemental Guidance: Incident response support resources provided by organizations include, for example, help desks, assistance groups, and access to forensics services, when required. Related controls: AT-2, IR-4, IR-6, IR-8, SA-9.

Control Enhancements:

(1) *INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT*

The organization employs automated mechanisms to increase the availability of incident response-related information and support.

Supplemental Guidance: Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or conversely, the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

(2) *INCIDENT RESPONSE ASSISTANCE | COORDINATION WITH EXTERNAL PROVIDERS*

The organization:

(a) Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and

(b) Identifies organizational incident response team members to the external providers.

Supplemental Guidance: External providers of information system protection capability include, for example, the Computer Network Defense program within the U.S. Department of Defense. External providers help to protect, monitor, analyze, detect, and respond to unauthorized activity within organizational information systems and networks.

References: None.

Priority and Baseline Allocation:

P2	**LOW** IR-7	**MOD** IR-7 (1)	**HIGH** IR-7 (1)

IR-8 INCIDENT RESPONSE PLAN

Control: The organization:

a. Develops an incident response plan that:

1. Provides the organization with a roadmap for implementing its incident response capability;
2. Describes the structure and organization of the incident response capability;
3. Provides a high-level approach for how the incident response capability fits into the overall organization;
4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
5. Defines reportable incidents;
6. Provides metrics for measuring the incident response capability within the organization;
7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
8. Is reviewed and approved by [*Assignment: organization-defined personnel or roles*];

b. Distributes copies of the incident response plan to [*Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements*];

c. Reviews the incident response plan [*Assignment: organization-defined frequency*];

d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;

e. Communicates incident response plan changes to [*Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements*]; and

f. Protects the incident response plan from unauthorized disclosure and modification.

Supplemental Guidance: It is important that organizations develop and implement a coordinated approach to incident response. Organizational missions, business functions, strategies, goals, and objectives for incident response help to determine the structure of incident response capabilities. As part of a comprehensive incident response capability, organizations consider the coordination and sharing of information with external organizations, including, for example, external service providers and organizations involved in the supply chain for organizational information systems. Related controls: MP-2, MP-4, MP-5.

Control Enhancements: None.

References: NIST Special Publication 800-61.

Priority and Baseline Allocation:

P1	**LOW** IR-8	**MOD** IR-8	**HIGH** IR-8

IR-9 INFORMATION SPILLAGE RESPONSE

Control: The organization responds to information spills by:

a. Identifying the specific information involved in the information system contamination;

b. Alerting [*Assignment: organization-defined personnel or roles*] of the information spill using a method of communication not associated with the spill;

c. Isolating the contaminated information system or system component;

d. Eradicating the information from the contaminated information system or component;

e. Identifying other information systems or system components that may have been subsequently contaminated; and

f. Performing other [*Assignment: organization-defined actions*].

Supplemental Guidance: Information spillage refers to instances where either classified or sensitive information is inadvertently placed on information systems that are not authorized to process such information. Such information spills often occur when information that is initially thought to be of lower sensitivity is transmitted to an information system and then is subsequently determined to be of higher sensitivity. At that point, corrective action is required. The nature of the organizational response is generally based upon the degree of sensitivity of the spilled information (e.g., security category or classification level), the security capabilities of the information system, the specific nature of contaminated storage media, and the access authorizations (e.g., security clearances) of individuals with authorized access to the contaminated system. The methods used to communicate information about the spill after the fact do not involve methods directly associated with the actual spill to minimize the risk of further spreading the contamination before such contamination is isolated and eradicated.

Control Enhancements:

(1) *INFORMATION SPILLAGE RESPONSE | RESPONSIBLE PERSONNEL*

The organization assigns [*Assignment: organization-defined personnel or roles*] with responsibility for responding to information spills.

(2) *INFORMATION SPILLAGE RESPONSE | TRAINING*

The organization provides information spillage response training [*Assignment: organization-defined frequency*].

(3) *INFORMATION SPILLAGE RESPONSE | POST-SPILL OPERATIONS*

The organization implements [*Assignment: organization-defined procedures*] to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.

Supplemental Guidance: Correction actions for information systems contaminated due to information spillages may be very time-consuming. During those periods, personnel may not have access to the contaminated systems, which may potentially affect their ability to conduct organizational business.

(4) *INFORMATION SPILLAGE RESPONSE | EXPOSURE TO UNAUTHORIZED PERSONNEL*

The organization employs [*Assignment: organization-defined security safeguards*] for personnel exposed to information not within assigned access authorizations.

Supplemental Guidance: Security safeguards include, for example, making personnel exposed to spilled information aware of the federal laws, directives, policies, and/or regulations regarding the information and the restrictions imposed based on exposure to such information.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

IR-10 INTEGRATED INFORMATION SECURITY ANALYSIS TEAM

Control: The organization establishes an integrated team of forensic/malicious code analysts, tool developers, and real-time operations personnel.

Supplemental Guidance: Having an integrated team for incident response facilitates information sharing. Such capability allows organizational personnel, including developers, implementers, and operators, to leverage the team knowledge of the threat in order to implement defensive measures that will enable organizations to deter intrusions more effectively. Moreover, it promotes the rapid detection of intrusions, development of appropriate mitigations, and the deployment of effective defensive measures. For example, when an intrusion is detected, the integrated security analysis team can rapidly develop an appropriate response for operators to implement, correlate the new incident with information on past intrusions, and augment ongoing intelligence development. This

enables the team to identify adversary TTPs that are linked to the operations tempo or to specific missions/business functions, and to define responsive actions in a way that does not disrupt the mission/business operations. Ideally, information security analysis teams are distributed within organizations to make the capability more resilient.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: MAINTENANCE

MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

   1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and

b. Reviews and updates the current:

   1. System maintenance policy [*Assignment: organization-defined frequency*]; and

   2. System maintenance procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** MA-1	**MOD** MA-1	**HIGH** MA-1

MA-2 CONTROLLED MAINTENANCE

Control: The organization:

a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;

b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;

c. Requires that [*Assignment: organization-defined personnel or roles*] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;

d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;

e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and

f. Includes [*Assignment: organization-defined maintenance-related information*] in organizational maintenance records.

Supplemental Guidance: This control addresses the information security aspects of the information system maintenance program and applies to all types of maintenance to any system component (including applications) conducted by any local or nonlocal entity (e.g., in-contract, warranty, in-house, software maintenance agreement). System maintenance also includes those components not directly associated with information processing and/or data/information retention such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes, for example: (i) date and time of maintenance; (ii) name of individuals or group performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) information system components/equipment removed or replaced (including identification numbers, if applicable). The level of detail included in maintenance records can be informed by the security categories of organizational information systems. Organizations consider supply chain issues associated with replacement components for information systems. Related controls: CM-3, CM-4, MA-4, MP-6, PE-16, SA-12, SI-2.

Control Enhancements:

(1) *CONTROLLED MAINTENANCE | RECORD CONTENT*

[Withdrawn: Incorporated into MA-2]**.**

(2) *CONTROLLED MAINTENANCE | AUTOMATED MAINTENANCE ACTIVITIES*

The organization:

(a) Employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and

(b) Produces up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed.

Supplemental Guidance: Related controls: CA-7, MA-3.

References: None.

Priority and Baseline Allocation:

P2	**LOW** MA-2	**MOD** MA-2	**HIGH** MA-2 (2)

MA-3 MAINTENANCE TOOLS

Control: The organization approves, controls, and monitors information system maintenance tools.

Supplemental Guidance: This control addresses security-related issues associated with maintenance tools used specifically for diagnostic and repair actions on organizational information systems. Maintenance tools can include hardware, software, and firmware items. Maintenance tools are potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into organizational information systems. Maintenance tools can include, for example, hardware/software diagnostic test equipment and hardware/software packet sniffers. This control does not cover hardware/software components that may support information system maintenance, yet are a part of the system, for example, the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch. Related controls: MA-2, MA-5, MP-6.

Control Enhancements:

(1) *MAINTENANCE TOOLS | INSPECT TOOLS*

The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

Supplemental Guidance: If, upon inspection of maintenance tools, organizations determine that the tools have been modified in an improper/unauthorized manner or contain malicious code,

the incident is handled consistent with organizational policies and procedures for incident handling. Related control: SI-7.

(2) *MAINTENANCE TOOLS | INSPECT MEDIA*

The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.

Supplemental Guidance: If, upon inspection of media containing maintenance diagnostic and test programs, organizations determine that the media contain malicious code, the incident is handled consistent with organizational incident handling policies and procedures. Related control: SI-3.

(3) *MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL*

The organization prevents the unauthorized removal of maintenance equipment containing organizational information by:

(a) Verifying that there is no organizational information contained on the equipment;

(b) Sanitizing or destroying the equipment;

(c) Retaining the equipment within the facility; or

(d) Obtaining an exemption from [*Assignment: organization-defined personnel or roles*] explicitly authorizing removal of the equipment from the facility.

Supplemental Guidance: Organizational information includes all information specifically owned by organizations and information provided to organizations in which organizations serve as information stewards.

(4) *MAINTENANCE TOOLS | RESTRICTED TOOL USE*

The information system restricts the use of maintenance tools to authorized personnel only.

Supplemental Guidance: This control enhancement applies to information systems that are used to carry out maintenance functions. Related controls: AC-2, AC-3, AC-5, AC-6.

References: NIST Special Publication 800-88.

Priority and Baseline Allocation:

P3	**LOW** Not Selected	**MOD** MA-3 (1) (2)	**HIGH** MA-3 (1) (2) (3)

MA-4 NONLOCAL MAINTENANCE

Control: The organization:

a. Approves and monitors nonlocal maintenance and diagnostic activities;

b. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;

c. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;

d. Maintains records for nonlocal maintenance and diagnostic activities; and

e. Terminates session and network connections when nonlocal maintenance is completed.

Supplemental Guidance: Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. Authentication techniques used in the establishment of nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA-2. Typically, strong authentication requires authenticators that are resistant to replay attacks and employ multifactor authentication. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric.

Enforcing requirements in MA-4 is accomplished in part by other controls. Related controls: AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5, MP-6, PL-2, SC-7, SC-10, SC-17.

Control Enhancements:

(1) *NONLOCAL MAINTENANCE | AUDITING AND REVIEW*

The organization:

(a) Audits nonlocal maintenance and diagnostic sessions [*Assignment: organization-defined audit events*]; and

(b) Reviews the records of the maintenance and diagnostic sessions.

Supplemental Guidance: Related controls: AU-2, AU-6, AU-12.

(2) *NONLOCAL MAINTENANCE | DOCUMENT NONLOCAL MAINTENANCE*

The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

(3) *NONLOCAL MAINTENANCE | COMPARABLE SECURITY / SANITIZATION*

The organization:

(a) Requires that nonlocal maintenance and diagnostic services be performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced; or

(b) Removes the component to be serviced from the information system and prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the information system.

Supplemental Guidance: Comparable security capability on information systems, diagnostic tools, and equipment providing maintenance services implies that the implemented security controls on those systems, tools, and equipment are at least as comprehensive as the controls on the information system being serviced. Related controls: MA-3, SA-12, SI-3, SI-7.

(4) *NONLOCAL MAINTENANCE | AUTHENTICATION / SEPARATION OF MAINTENANCE SESSIONS*

The organization protects nonlocal maintenance sessions by:

(a) Employing [*Assignment: organization-defined authenticators that are replay resistant*]; and

(b) Separating the maintenance sessions from other network sessions with the information system by either:

(1) Physically separated communications paths; or

(2) Logically separated communications paths based upon encryption.

Supplemental Guidance: Related control: SC-13.

(5) *NONLOCAL MAINTENANCE | APPROVALS AND NOTIFICATIONS*

The organization:

(a) Requires the approval of each nonlocal maintenance session by [*Assignment: organization-defined personnel or roles*]; and

(b) Notifies [*Assignment: organization-defined personnel or roles*] of the date and time of planned nonlocal maintenance.

Supplemental Guidance: Notification may be performed by maintenance personnel. Approval of nonlocal maintenance sessions is accomplished by organizational personnel with sufficient information security and information system knowledge to determine the appropriateness of the proposed maintenance.

(6) *NONLOCAL MAINTENANCE | CRYPTOGRAPHIC PROTECTION*

The information system implements cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications.

Supplemental Guidance: Related controls: SC-8, SC-13.

(7) *NONLOCAL MAINTENANCE | REMOTE DISCONNECT VERIFICATION*

The information system implements remote disconnect verification at the termination of nonlocal maintenance and diagnostic sessions.

Supplemental Guidance: Remote disconnect verification ensures that remote connections from nonlocal maintenance sessions have been terminated and are no longer available for use. Related control: SC-13.

References: FIPS Publications 140-2, 197, 201; NIST Special Publications 800-63, 800-88; CNSS Policy 15.

Priority and Baseline Allocation:

P2	**LOW** MA-4	**MOD** MA-4 (2)	**HIGH** MA-4 (2) (3)

MA-5 MAINTENANCE PERSONNEL

Control: The organization:

a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;

b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and

c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

Supplemental Guidance: This control applies to individuals performing hardware or software maintenance on organizational information systems, while PE-2 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems (e.g., custodial staff, physical plant maintenance personnel). Technical competence of supervising individuals relates to the maintenance performed on the information systems while having required access authorizations refers to maintenance on and near the systems. Individuals not previously identified as authorized maintenance personnel, such as information technology manufacturers, vendors, systems integrators, and consultants, may require privileged access to organizational information systems, for example, when required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, organizations may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time periods. Related controls: AC-2, IA-8, MP-2, PE-2, PE-3, PE-4, RA-3.

Control Enhancements:

(1) *MAINTENANCE PERSONNEL | INDIVIDUALS WITHOUT APPROPRIATE ACCESS*

The organization:

(a) Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:

(1) Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;

(2) Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and

(b) Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.

Supplemental Guidance: This control enhancement denies individuals who lack appropriate security clearances (i.e., individuals who do not possess security clearances or possess security clearances at a lower level than required) or who are not U.S. citizens, visual and electronic access to any classified information, Controlled Unclassified Information (CUI), or any other sensitive information contained on organizational information systems. Procedures for the use of maintenance personnel can be documented in security plans for the information systems. Related controls: MP-6, PL-2.

(2) *MAINTENANCE PERSONNEL | SECURITY CLEARANCES FOR CLASSIFIED SYSTEMS*

The organization ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting classified information possess security clearances and formal access approvals for at least the highest classification level and for all compartments of information on the system.

Supplemental Guidance: Related control: PS-3.

(3) *MAINTENANCE PERSONNEL | CITIZENSHIP REQUIREMENTS FOR CLASSIFIED SYSTEMS*

The organization ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting classified information are U.S. citizens.

Supplemental Guidance: Related control: PS-3.

(4) *MAINTENANCE PERSONNEL | FOREIGN NATIONALS*

The organization ensures that:

(a) Cleared foreign nationals (i.e., foreign nationals with appropriate security clearances), are used to conduct maintenance and diagnostic activities on classified information systems only when the systems are jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments; and

(b) Approvals, consents, and detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on classified information systems are fully documented within Memoranda of Agreements.

Supplemental Guidance: Related control: PS-3.

(5) *MAINTENANCE PERSONNEL | NONSYSTEM-RELATED MAINTENANCE*

The organization ensures that non-escorted personnel performing maintenance activities not directly associated with the information system but in the physical proximity of the system, have required access authorizations.

Supplemental Guidance: Personnel performing maintenance activities in other capacities not directly related to the information system include, for example, physical plant personnel and janitorial personnel.

References: None.

Priority and Baseline Allocation:

P2	**LOW** MA-5	**MOD** MA-5	**HIGH** MA-5 (1)

MA-6 TIMELY MAINTENANCE

Control: The organization obtains maintenance support and/or spare parts for [*Assignment: organization-defined information system components*] within [*Assignment: organization-defined time period*] of failure.

Supplemental Guidance: Organizations specify the information system components that result in increased risk to organizational operations and assets, individuals, other organizations, or the Nation when the functionality provided by those components is not operational. Organizational actions to obtain maintenance support typically include having appropriate contracts in place. Related controls: CM-8, CP-2, CP-7, SA-14, SA-15.

Control Enhancements:

(1) *TIMELY MAINTENANCE | PREVENTIVE MAINTENANCE*

The organization performs preventive maintenance on [*Assignment: organization-defined information system components*] at [*Assignment: organization-defined time intervals*].

Supplemental Guidance: Preventive maintenance includes proactive care and servicing of organizational information systems components for the purpose of maintaining equipment and facilities in satisfactory operating condition. Such maintenance provides for the systematic inspection, tests, measurements, adjustments, parts replacement, detection, and correction of incipient failures either before they occur or before they develop into major defects. The primary goal of preventive maintenance is to avoid/mitigate the consequences of equipment failures. Preventive maintenance is designed to preserve and restore equipment reliability by replacing worn components before they actually fail. Methods of determining what preventive (or other) failure management policies to apply include, for example, original equipment manufacturer (OEM) recommendations, statistical failure records, requirements of codes, legislation, or regulations within a jurisdiction, expert opinion, maintenance that has already been conducted on similar equipment, or measured values and performance indications.

(2) *TIMELY MAINTENANCE | PREDICTIVE MAINTENANCE*

The organization performs predictive maintenance on [*Assignment: organization-defined information system components*] at [*Assignment: organization-defined time intervals*].

Supplemental Guidance: Predictive maintenance, or condition-based maintenance, attempts to evaluate the condition of equipment by performing periodic or continuous (online) equipment condition monitoring. The goal of predictive maintenance is to perform maintenance at a scheduled point in time when the maintenance activity is most cost-effective and before the equipment loses performance within a threshold. The predictive component of predictive maintenance stems from the goal of predicting the future trend of the equipment's condition. This approach uses principles of statistical process control to determine at what point in the future maintenance activities will be appropriate. Most predictive maintenance inspections are performed while equipment is in service, thereby minimizing disruption of normal system operations. Predictive maintenance can result in substantial cost savings and higher system reliability. Predictive maintenance tends to include measurement of the item. To evaluate equipment condition, predictive maintenance utilizes nondestructive testing technologies such as infrared, acoustic (partial discharge and airborne ultrasonic), corona detection, vibration analysis, sound level measurements, oil analysis, and other specific online tests.

(3) *TIMELY MAINTENANCE | AUTOMATED SUPPORT FOR PREDICTIVE MAINTENANCE*

The organization employs automated mechanisms to transfer predictive maintenance data to a computerized maintenance management system.

Supplemental Guidance: A computerized maintenance management system maintains a computer database of information about the maintenance operations of organizations and automates processing equipment condition data in order to trigger maintenance planning, execution, and reporting.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** MA-6	**HIGH** MA-6

FAMILY: MEDIA PROTECTION

MP-1 MEDIA PROTECTION POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

   1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and

b. Reviews and updates the current:

   1. Media protection policy [*Assignment: organization-defined frequency*]; and

   2. Media protection procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MP family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** MP-1	**MOD** MP-1	**HIGH** MP-1

MP-2 MEDIA ACCESS

Control: The organization restricts access to [*Assignment: organization-defined types of digital and/or non-digital media*] to [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Restricting non-digital media access includes, for example, denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers. Restricting access to digital media includes, for example, limiting access to design specifications stored on compact disks in the media library to the project leader and the individuals on the development team. Related controls: AC-3, IA-2, MP-4, PE-2, PE-3, PL-2.

Control Enhancements:

(1) *MEDIA ACCESS | AUTOMATED RESTRICTED ACCESS*

[Withdrawn: Incorporated into MP-4 (2)].

(2) *MEDIA ACCESS | CRYPTOGRAPHIC PROTECTION*
[Withdrawn: Incorporated into SC-28 (1)].

References: FIPS Publication 199; NIST Special Publication 800-111.

Priority and Baseline Allocation:

P1	**LOW** MP-2	**MOD** MP-2	**HIGH** MP-2

MP-3 MEDIA MARKING

Control: The organization:

a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and

b. Exempts [*Assignment: organization-defined types of information system media*] from marking as long as the media remain within [*Assignment: organization-defined controlled areas*].

Supplemental Guidance: The term *security marking* refers to the application/use of human-readable security attributes. The term *security labeling* refers to the application/use of security attributes with regard to internal data structures within information systems (see AC-16). Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Security marking is generally not required for media containing information determined by organizations to be in the public domain or to be publicly releasable. However, some organizations may require markings for public information indicating that the information is publicly releasable. Marking of information system media reflects applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Related controls: AC-16, PL-2, RA-3.

Control Enhancements: None.

References: FIPS Publication 199.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** MP-3	**HIGH** MP-3

MP-4 MEDIA STORAGE

Control: The organization:

a. Physically controls and securely stores [*Assignment: organization-defined types of digital and/or non-digital media*] within [*Assignment: organization-defined controlled areas*]; and

b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Supplemental Guidance: Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Physically controlling information system media includes, for example, conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media. Secure storage includes, for example, a locked drawer, desk, or cabinet, or a controlled media library. The type of media storage is commensurate with the security category and/or classification of the information residing on the media. Controlled areas are areas for which organizations

provide sufficient physical and procedural safeguards to meet the requirements established for protecting information and/or information systems. For media containing information determined by organizations to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on organizations or individuals if accessed by other than authorized personnel, fewer safeguards may be needed. In these situations, physical access controls provide adequate protection. Related controls: CP-6, CP-9, MP-2, MP-7, PE-3.

Control Enhancements:

(1) *MEDIA STORAGE | CRYPTOGRAPHIC PROTECTION*

[Withdrawn: Incorporated into SC-28 (1)].

(2) *MEDIA STORAGE | AUTOMATED RESTRICTED ACCESS*

The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.

Supplemental Guidance: Automated mechanisms can include, for example, keypads on the external entries to media storage areas. Related controls: AU-2, AU-9, AU-6, AU-12.

References: FIPS Publication 199; NIST Special Publications 800-56, 800-57, 800-111.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** MP-4	**HIGH** MP-4

MP-5 MEDIA TRANSPORT

Control: The organization:

a. Protects and controls [*Assignment: organization-defined types of information system media*] during transport outside of controlled areas using [*Assignment: organization-defined security safeguards*];

b. Maintains accountability for information system media during transport outside of controlled areas;

c. Documents activities associated with the transport of information system media; and

d. Restricts the activities associated with the transport of information system media to authorized personnel.

Supplemental Guidance: Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers), that are transported outside of controlled areas. Controlled areas are areas or spaces for which organizations provide sufficient physical and/or procedural safeguards to meet the requirements established for protecting information and/or information systems.

Physical and technical safeguards for media are commensurate with the security category or classification of the information residing on the media. Safeguards to protect media during transport include, for example, locked containers and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service). Maintaining accountability of media during transport includes, for example, restricting transport activities to authorized personnel, and tracking and/or obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss,

destruction, or tampering. Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with organizational assessments of risk to include the flexibility to define different record-keeping methods for the different types of media transport as part of an overall system of transport-related records. Related controls: AC-19, CP-9, MP-3, MP-4, RA-3, SC-8, SC-13, SC-28.

Control Enhancements:

(1) *MEDIA TRANSPORT | PROTECTION OUTSIDE OF CONTROLLED AREAS*

[Withdrawn: Incorporated into MP-5].

(2) *MEDIA TRANSPORT | DOCUMENTATION OF ACTIVITIES*

[Withdrawn: Incorporated into MP-5].

(3) *MEDIA TRANSPORT | CUSTODIANS*

The organization employs an identified custodian during transport of information system media outside of controlled areas.

Supplemental Guidance: Identified custodians provide organizations with specific points of contact during the media transport process and facilitate individual accountability. Custodial responsibilities can be transferred from one individual to another as long as an unambiguous custodian is identified at all times.

(4) *MEDIA TRANSPORT | CRYPTOGRAPHIC PROTECTION*

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

Supplemental Guidance: This control enhancement applies to both portable storage devices (e.g., USB memory sticks, compact disks, digital video disks, external/removable hard disk drives) and mobile devices with storage capability (e.g., smart phones, tablets, E-readers). Related control: MP-2.

References: FIPS Publication 199; NIST Special Publication 800-60.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** MP-5 (4)	**HIGH** MP-5 (4)

MP-6 MEDIA SANITIZATION

Control: The organization:

a. Sanitizes [*Assignment: organization-defined information system media*] prior to disposal, release out of organizational control, or release for reuse using [*Assignment: organization-defined sanitization techniques and procedures*] in accordance with applicable federal and organizational standards and policies; and

b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Supplemental Guidance: This control applies to all information system media, both digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal.

Sanitization of non-digital media includes, for example, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections/words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media containing classified information. Related controls: MA-2, MA-4, RA-3, SC-4.

Control Enhancements:

(1) *MEDIA SANITIZATION | REVIEW / APPROVE / TRACK / DOCUMENT / VERIFY*

The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.

Supplemental Guidance: Organizations review and approve media to be sanitized to ensure compliance with records-retention policies. Tracking/documenting actions include, for example, listing personnel who reviewed and approved sanitization and disposal actions, types of media sanitized, specific files stored on the media, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitization, verification actions taken, personnel who performed the verification, and disposal action taken. Organizations verify that the sanitization of the media was effective prior to disposal. Related control: SI-12.

(2) *MEDIA SANITIZATION | EQUIPMENT TESTING*

The organization tests sanitization equipment and procedures [*Assignment: organization-defined frequency*] to verify that the intended sanitization is being achieved.

Supplemental Guidance: Testing of sanitization equipment and procedures may be conducted by qualified and authorized external entities (e.g., other federal agencies or external service providers).

(3) *MEDIA SANITIZATION | NONDESTRUCTIVE TECHNIQUES*

The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the following circumstances: [*Assignment: organization-defined circumstances requiring sanitization of portable storage devices*].

Supplemental Guidance: This control enhancement applies to digital media containing classified information and Controlled Unclassified Information (CUI). Portable storage devices can be the source of malicious code insertions into organizational information systems. Many of these devices are obtained from unknown and potentially untrustworthy sources and may contain malicious code that can be readily transferred to information systems through USB ports or other entry portals. While scanning such storage devices is always recommended, sanitization provides additional assurance that the devices are free of malicious code to include code capable of initiating zero-day attacks. Organizations consider nondestructive sanitization of portable storage devices when such devices are first purchased from the manufacturer or vendor prior to initial use or when organizations lose a positive chain of custody for the devices. Related control: SI-3.

(4) *MEDIA SANITIZATION | CONTROLLED UNCLASSIFIED INFORMATION*

[Withdrawn: Incorporated into MP-6].

(5) *MEDIA SANITIZATION | CLASSIFIED INFORMATION*

[Withdrawn: Incorporated into MP-6].

(6) *MEDIA SANITIZATION | MEDIA DESTRUCTION*

[Withdrawn: Incorporated into MP-6].

(7) *MEDIA SANITIZATION | DUAL AUTHORIZATION*

The organization enforces dual authorization for the sanitization of [*Assignment: organization-defined information system media*].

Supplemental Guidance: Organizations employ dual authorization to ensure that information system media sanitization cannot occur unless two technically qualified individuals conduct the task. Individuals sanitizing information system media possess sufficient skills/expertise to determine if the proposed sanitization reflects applicable federal/organizational standards, policies, and procedures. Dual authorization also helps to ensure that sanitization occurs as

intended, both protecting against errors and false claims of having performed the sanitization actions. Dual authorization may also be known as two-person control. Related controls: AC-3, MP-2.

(8) *MEDIA SANITIZATION | REMOTE PURGING / WIPING OF INFORMATION*

The organization provides the capability to purge/wipe information from [*Assignment: organization-defined information systems, system components, or devices*] either remotely or under the following conditions: [*Assignment: organization-defined conditions*].

Supplemental Guidance: This control enhancement protects data/information on organizational information systems, system components, or devices (e.g., mobile devices) if such systems, components, or devices are obtained by unauthorized individuals. Remote purge/wipe commands require strong authentication to mitigate the risk of unauthorized individuals purging/wiping the system/component/device. The purge/wipe function can be implemented in a variety of ways including, for example, by overwriting data/information multiple times or by destroying the key necessary to decrypt encrypted data.

References: FIPS Publication 199; NIST Special Publications 800-60, 800-88; Web: http://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml.

Priority and Baseline Allocation:

P1	**LOW** MP-6	**MOD** MP-6	**HIGH** MP-6 (1) (2) (3)

MP-7 MEDIA USE

Control: The organization [*Selection: restricts; prohibits*] the use of [*Assignment: organization-defined types of information system media*] on [*Assignment: organization-defined information systems or system components*] using [*Assignment: organization-defined security safeguards*].

Supplemental Guidance: Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers). In contrast to MP-2, which restricts user access to media, this control restricts the use of certain types of media on information systems, for example, restricting/prohibiting the use of flash drives or external hard disk drives. Organizations can employ technical and nontechnical safeguards (e.g., policies, procedures, rules of behavior) to restrict the use of information system media. Organizations may restrict the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling/removing the ability to insert, read or write to such devices. Organizations may also limit the use of portable storage devices to only approved devices including, for example, devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may restrict the use of portable storage devices based on the type of device, for example, prohibiting the use of writeable, portable storage devices, and implementing this restriction by disabling or removing the capability to write to such devices. Related controls: AC-19, PL-4.

Control Enhancements:

(1) *MEDIA USE | PROHIBIT USE WITHOUT OWNER*

The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

Supplemental Guidance: Requiring identifiable owners (e.g., individuals, organizations, or projects) for portable storage devices reduces the risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., malicious code insertion). Related control: PL-4.

(2) *MEDIA USE | PROHIBIT USE OF SANITIZATION-RESISTANT MEDIA*

The organization prohibits the use of sanitization-resistant media in organizational information systems.

Supplemental Guidance: Sanitation-resistance applies to the capability to purge information from media. Certain types of media do not support sanitize commands, or if supported, the interfaces are not supported in a standardized way across these devices. Sanitation-resistant media include, for example, compact flash, embedded flash on boards and devices, solid state drives, and USB removable media. Related control: MP-6.

References: FIPS Publication 199; NIST Special Publication 800-111.

Priority and Baseline Allocation:

P1	**LOW** MP-7	**MOD** MP-7 (1)	**HIGH** MP-7 (1)

MP-8 MEDIA DOWNGRADING

Control: The organization:

a. Establishes [*Assignment: organization-defined information system media downgrading process*] that includes employing downgrading mechanisms with [*Assignment: organization-defined strength and integrity*];

b. Ensures that the information system media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information;

c. Identifies [*Assignment: organization-defined information system media requiring downgrading*]; and

d. Downgrades the identified information system media using the established process.

Supplemental Guidance: This control applies to all information system media, digital and non-digital, subject to release outside of the organization, whether or not the media is considered removable. The downgrading process, when applied to system media, removes information from the media, typically by security category or classification level, such that the information cannot be retrieved or reconstructed. Downgrading of media includes redacting information to enable wider release and distribution. Downgrading of media also ensures that empty space on the media (e.g., slack space within files) is devoid of information.

Control Enhancements:

(1) *MEDIA DOWNGRADING | DOCUMENTATION OF PROCESS*

The organization documents information system media downgrading actions.

Supplemental Guidance: Organizations can document the media downgrading process by providing information such as the downgrading technique employed, the identification number of the downgraded media, and the identity of the individual that authorized and/or performed the downgrading action.

(2) *MEDIA DOWNGRADING | EQUIPMENT TESTING*

The organization employs [*Assignment: organization-defined tests*] of downgrading equipment and procedures to verify correct performance [*Assignment: organization-defined frequency*].

(3) *MEDIA DOWNGRADING | CONTROLLED UNCLASSIFIED INFORMATION*

The organization downgrades information system media containing [*Assignment: organization-defined Controlled Unclassified Information (CUI)*] prior to public release in accordance with applicable federal and organizational standards and policies.

(4) *MEDIA DOWNGRADING | CLASSIFIED INFORMATION*

The organization downgrades information system media containing classified information prior to release to individuals without required access authorizations in accordance with NSA standards and policies.

Supplemental Guidance: Downgrading of classified information uses approved sanitization tools, techniques, and procedures to transfer information confirmed to be unclassified from classified information systems to unclassified media.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

   1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and

b. Reviews and updates the current:

   1. Physical and environmental protection policy [*Assignment: organization-defined frequency*]; and

   2. Physical and environmental protection procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PE family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** PE-1	**MOD** PE-1	**HIGH** PE-1

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

Control: The organization:

a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;

b. Issues authorization credentials for facility access;

c. Reviews the access list detailing authorized facility access by individuals [*Assignment: organization-defined frequency*]; and

d. Removes individuals from the facility access list when access is no longer required.

Supplemental Guidance: This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Authorization credentials include, for example, badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed (including level of forge-proof badges, smart cards, or identification cards) consistent with federal

standards, policies, and procedures. This control only applies to areas within facilities that have not been designated as publicly accessible. Related controls: PE-3, PE-4, PS-3.

Control Enhancements:

(1) *PHYSICAL ACCESS AUTHORIZATIONS | ACCESS BY POSITION / ROLE*

The organization authorizes physical access to the facility where the information system resides based on position or role.

Supplemental Guidance: Related controls: AC-2, AC-3, AC-6.

(2) *PHYSICAL ACCESS AUTHORIZATIONS | TWO FORMS OF IDENTIFICATION*

The organization requires two forms of identification from [*Assignment: organization-defined list of acceptable forms of identification*] for visitor access to the facility where the information system resides.

Supplemental Guidance: Acceptable forms of government photo identification include, for example, passports, Personal Identity Verification (PIV) cards, and drivers' licenses. In the case of gaining access to facilities using automated mechanisms, organizations may use PIV cards, key cards, PINs, and biometrics. Related controls: IA-2, IA-4, IA-5.

(3) *PHYSICAL ACCESS AUTHORIZATIONS | RESTRICT UNESCORTED ACCESS*

The organization restricts unescorted access to the facility where the information system resides to personnel with [*Selection (one or more): security clearances for all information contained within the system; formal access authorizations for all information contained within the system; need for access to all information contained within the system;* [*Assignment: organization-defined credentials*]].

Supplemental Guidance: Due to the highly sensitive nature of classified information stored within certain facilities, it is important that individuals lacking sufficient security clearances, access approvals, or need to know, be escorted by individuals with appropriate credentials to ensure that such information is not exposed or otherwise compromised. Related controls: PS-2, PS-6.

References: None.

Priority and Baseline Allocation:

P1	**LOW** PE-2	**MOD** PE-2	**HIGH** PE-2

PE-3 PHYSICAL ACCESS CONTROL

Control: The organization:

a. Enforces physical access authorizations at [*Assignment: organization-defined entry/exit points to the facility where the information system resides*] by;

   1. Verifying individual access authorizations before granting access to the facility; and

   2. Controlling ingress/egress to the facility using [*Selection (one or more):* [*Assignment: organization-defined physical access control systems/devices*]; *guards*];

b. Maintains physical access audit logs for [*Assignment: organization-defined entry/exit points*];

c. Provides [*Assignment: organization-defined security safeguards*] to control access to areas within the facility officially designated as publicly accessible;

d. Escorts visitors and monitors visitor activity [*Assignment: organization-defined circumstances requiring visitor escorts and monitoring*];

e. Secures keys, combinations, and other physical access devices;

f. Inventories [*Assignment: organization-defined physical access devices*] every [*Assignment: organization-defined frequency*]; and

g. Changes combinations and keys [*Assignment: organization-defined frequency*] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Supplemental Guidance: This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Organizations determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or information system users. Physical access devices include, for example, keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, and isolating selected information systems and/or system components in secured areas. Physical access control systems comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The Federal Identity, Credential, and Access Management Program provides implementation guidance for identity, credential, and access management capabilities for physical access control systems. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to information systems and/or components requiring supplemental access controls, or both. Components of organizational information systems (e.g., workstations, terminals) may be located in areas designated as publicly accessible with organizations safeguarding access to such devices. Related controls: AU-2, AU-6, MP-2, MP-4, PE-2, PE-4, PE-5, PS-3, RA-3.

Control Enhancements:

(1) *PHYSICAL ACCESS CONTROL | INFORMATION SYSTEM ACCESS*

The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at [*Assignment: organization-defined physical spaces containing one or more components of the information system*].

Supplemental Guidance: This control enhancement provides additional physical security for those areas within facilities where there is a concentration of information system components (e.g., server rooms, media storage areas, data and communications centers). Related control: PS-2.

(2) *PHYSICAL ACCESS CONTROL | FACILITY / INFORMATION SYSTEM BOUNDARIES*

The organization performs security checks [*Assignment: organization-defined frequency*] at the physical boundary of the facility or information system for unauthorized exfiltration of information or removal of information system components.

Supplemental Guidance: Organizations determine the extent, frequency, and/or randomness of security checks to adequately mitigate risk associated with exfiltration. Related controls: AC-4, SC-7.

(3) *PHYSICAL ACCESS CONTROL | CONTINUOUS GUARDS / ALARMS / MONITORING*

The organization employs guards and/or alarms to monitor every physical access point to the facility where the information system resides 24 hours per day, 7 days per week.

Supplemental Guidance: Related controls: CP-6, CP-7.

(4) *PHYSICAL ACCESS CONTROL | LOCKABLE CASINGS*

The organization uses lockable physical casings to protect [*Assignment: organization-defined information system components*] from unauthorized physical access.

(5) *PHYSICAL ACCESS CONTROL | TAMPER PROTECTION*

The organization employs [*Assignment: organization-defined security safeguards*] to [*Selection (one or more): detect; prevent*] physical tampering or alteration of [*Assignment: organization-defined hardware components*] within the information system.

Supplemental Guidance: Organizations may implement tamper detection/prevention at selected hardware components or tamper detection at some components and tamper prevention at other components. Tamper detection/prevention activities can employ many types of anti-tamper technologies including, for example, tamper-detection seals and anti-tamper coatings. Anti-tamper programs help to detect hardware alterations through counterfeiting and other supply chain-related risks. Related control: SA-12.

(6) *PHYSICAL ACCESS CONTROL | FACILITY PENETRATION TESTING*

The organization employs a penetration testing process that includes [*Assignment: organization-defined frequency*], unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility.

Supplemental Guidance: Related controls: CA-2, CA-7.

References: FIPS Publication 201; NIST Special Publications 800-73, 800-76, 800-78, 800-116; ICD 704, 705; DoD Instruction 5200.39; Personal Identity Verification (PIV) in Enterprise Physical Access Control System (E-PACS); Web: http://idmanagement.gov, http://fips201ep.cio.gov.

Priority and Baseline Allocation:

P1	**LOW** PE-3	**MOD** PE-3	**HIGH** PE-3 (1)

PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM

Control: The organization controls physical access to [*Assignment: organization-defined information system distribution and transmission lines*] within organizational facilities using [*Assignment: organization-defined security safeguards*].

Supplemental Guidance: Physical security safeguards applied to information system distribution and transmission lines help to prevent accidental damage, disruption, and physical tampering. In addition, physical safeguards may be necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Security safeguards to control physical access to system distribution and transmission lines include, for example: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays. Related controls: MP-2, MP-4, PE-2, PE-3, PE-5, SC-7, SC-8.

Control Enhancements: None.

References: NSTISSI No. 7003.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** PE-4	**HIGH** PE-4

PE-5 ACCESS CONTROL FOR OUTPUT DEVICES

Control: The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

Supplemental Guidance: Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only, and placing output devices in locations that can be monitored by organizational personnel. Monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of information system output devices. Related controls: PE-2, PE-3, PE-4, PE-18.

Control Enhancements:

(1) *ACCESS CONTROL FOR OUTPUT DEVICES | ACCESS TO OUTPUT BY AUTHORIZED INDIVIDUALS*

The organization:

(a) Controls physical access to output from [*Assignment: organization-defined output devices*]; and

(b) Ensures that only authorized individuals receive output from the device.

Supplemental Guidance: Controlling physical access to selected output devices includes, for example, placing printers, copiers, and facsimile machines in controlled areas with keypad access controls or limiting access to individuals with certain types of badges.

(2) *ACCESS CONTROL FOR OUTPUT DEVICES | ACCESS TO OUTPUT BY INDIVIDUAL IDENTITY*

The information system:

(a) Controls physical access to output from [*Assignment: organization-defined output devices*]; and

(b) Links individual identity to receipt of the output from the device.

Supplemental Guidance: Controlling physical access to selected output devices includes, for example, installing security functionality on printers, copiers, and facsimile machines that allows organizations to implement authentication (e.g., using a PIN or hardware token) on output devices prior to the release of output to individuals.

(3) *ACCESS CONTROL FOR OUTPUT DEVICES | MARKING OUTPUT DEVICES*

The organization marks [*Assignment: organization-defined information system output devices*] indicating the appropriate security marking of the information permitted to be output from the device.

Supplemental Guidance: Outputs devices include, for example, printers, monitors, facsimile machines, scanners, copiers, and audio devices. This control enhancement is generally applicable to information system output devices other than mobiles devices.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** PE-5	**HIGH** PE-5

PE-6 MONITORING PHYSICAL ACCESS

Control: The organization:

a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;

b. Reviews physical access logs [*Assignment: organization-defined frequency*] and upon occurrence of [*Assignment: organization-defined events or potential indications of events*]; and

c. Coordinates results of reviews and investigations with the organizational incident response capability.

Supplemental Guidance: Organizational incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities. Suspicious physical access activities include, for example: (i) accesses outside of normal work hours; (ii) repeated accesses to areas not normally accessed; (iii) accesses for unusual lengths of time; and (iv) out-of-sequence accesses. Related controls: CA-7, IR-4, IR-8.

Control Enhancements:

(1) *MONITORING PHYSICAL ACCESS | INTRUSION ALARMS / SURVEILLANCE EQUIPMENT*

The organization monitors physical intrusion alarms and surveillance equipment.

(2) *MONITORING PHYSICAL ACCESS | AUTOMATED INTRUSION RECOGNITION / RESPONSES*

The organization employs automated mechanisms to recognize [*Assignment: organization-defined classes/types of intrusions*] and initiate [*Assignment: organization-defined response actions*].

Supplemental Guidance: Related control: SI-4.

(3) *MONITORING PHYSICAL ACCESS | VIDEO SURVEILLANCE*

The organization employs video surveillance of [*Assignment: organization-defined operational areas*] and retains video recordings for [*Assignment: organization-defined time period*].

Supplemental Guidance: This control enhancement focuses on recording surveillance video for purposes of subsequent review, if circumstances so warrant (e.g., a break-in detected by other means). It does not require monitoring surveillance video although organizations may choose to do so. Note that there may be legal considerations when performing and retaining video surveillance, especially if such surveillance is in a public location.

(4) *MONITORING PHYSICAL ACCESS | MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS*

The organization monitors physical access to the information system in addition to the physical access monitoring of the facility as [*Assignment: organization-defined physical spaces containing one or more components of the information system*].

Supplemental Guidance: This control enhancement provides additional monitoring for those areas within facilities where there is a concentration of information system components (e.g., server rooms, media storage areas, communications centers). Related controls: PS-2, PS-3.

References: None.

Priority and Baseline Allocation:

P1	**LOW** PE-6	**MOD** PE-6 (1)	**HIGH** PE-6 (1) (4)

PE-7 VISITOR CONTROL

[Withdrawn: Incorporated into PE-2 and PE-3].

PE-8 VISITOR ACCESS RECORDS

Control: The organization:

a. Maintains visitor access records to the facility where the information system resides for [*Assignment: organization-defined time period*]; and

b. Reviews visitor access records [*Assignment: organization-defined frequency*].

Supplemental Guidance: Visitor access records include, for example, names and organizations of persons visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purposes of visits, and names and organizations of persons visited. Visitor access records are not required for publicly accessible areas.

Control Enhancements:

(1) *VISITOR ACCESS RECORDS | AUTOMATED RECORDS MAINTENANCE / REVIEW*

The organization employs automated mechanisms to facilitate the maintenance and review of visitor access records.

(2) *VISITOR ACCESS RECORDS | PHYSICAL ACCESS RECORDS*

[Withdrawn: Incorporated into PE-2].

References: None.

Priority and Baseline Allocation:

P3	**LOW** PE-8	**MOD** PE-8	**HIGH** PE-8 (1)

PE-9 POWER EQUIPMENT AND CABLING

Control: The organization protects power equipment and power cabling for the information system from damage and destruction.

Supplemental Guidance: Organizations determine the types of protection necessary for power equipment and cabling employed at different locations both internal and external to organizational facilities and environments of operation. This includes, for example, generators and power cabling outside of buildings, internal cabling and uninterruptable power sources within an office or data center, and power sources for self-contained entities such as vehicles and satellites. Related control: PE-4.

Control Enhancements:

(1) *POWER EQUIPMENT AND CABLING | REDUNDANT CABLING*

The organization employs redundant power cabling paths that are physically separated by [*Assignment: organization-defined distance*].

Supplemental Guidance: Physically separate, redundant power cables help to ensure that power continues to flow in the event one of the cables is cut or otherwise damaged.

(2) *POWER EQUIPMENT AND CABLING | AUTOMATIC VOLTAGE CONTROLS*

The organization employs automatic voltage controls for [*Assignment: organization-defined critical information system components*].

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** PE-9	**HIGH** PE-9

PE-10 EMERGENCY SHUTOFF

Control: The organization:

a. Provides the capability of shutting off power to the information system or individual system components in emergency situations;

b. Places emergency shutoff switches or devices in [*Assignment: organization-defined location by information system or system component*] to facilitate safe and easy access for personnel; and

c. Protects emergency power shutoff capability from unauthorized activation.

Supplemental Guidance: This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Related control: PE-15.

Control Enhancements:

(1) *EMERGENCY SHUTOFF | ACCIDENTAL / UNAUTHORIZED ACTIVATION*

[Withdrawn: Incorporated into PE-10].

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** PE-10	**HIGH** PE-10

PE-11 EMERGENCY POWER

Control: The organization provides a short-term uninterruptible power supply to facilitate [*Selection (one or more): an orderly shutdown of the information system; transition of the information system to long-term alternate power*] in the event of a primary power source loss.

Supplemental Guidance: Related controls: AT-3, CP-2, CP-7.

Control Enhancements:

(1) *EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY - MINIMAL OPERATIONAL CAPABILITY*

The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

Supplemental Guidance: This control enhancement can be satisfied, for example, by the use of a secondary commercial power supply or other external power supply. Long-term alternate power supplies for the information system can be either manually or automatically activated.

(2) *EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY - SELF-CONTAINED*

The organization provides a long-term alternate power supply for the information system that is:

(a) Self-contained;

(b) Not reliant on external power generation; and

(c) Capable of maintaining [*Selection: minimally required operational capability; full operational capability*] in the event of an extended loss of the primary power source.

Supplemental Guidance: This control enhancement can be satisfied, for example, by the use of one or more generators with sufficient capacity to meet the needs of the organization. Long-term alternate power supplies for organizational information systems are either manually or automatically activated.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** PE-11	**HIGH** PE-11 (1)

PE-12 EMERGENCY LIGHTING

Control: The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Supplemental Guidance: This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Related controls: CP-2, CP-7.

Control Enhancements:

(1) *EMERGENCY LIGHTING | ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*

The organization provides emergency lighting for all areas within the facility supporting essential missions and business functions.

References: None.

Priority and Baseline Allocation:

P1	**LOW** PE-12	**MOD** PE-12	**HIGH** PE-12

PE-13 FIRE PROTECTION

Control: The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

Supplemental Guidance: This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

Control Enhancements:

(1) *FIRE PROTECTION | DETECTION DEVICES / SYSTEMS*

The organization employs fire detection devices/systems for the information system that activate automatically and notify [*Assignment: organization-defined personnel or roles*] and [*Assignment: organization-defined emergency responders*] in the event of a fire.

Supplemental Guidance: Organizations can identify specific personnel, roles, and emergency responders in the event that individuals on the notification list must have appropriate access authorizations and/or clearances, for example, to obtain access to facilities where classified operations are taking place or where there are information systems containing classified information.

(2) *FIRE PROTECTION | SUPPRESSION DEVICES / SYSTEMS*

The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to *Assignment: organization-defined personnel or roles*] and [*Assignment: organization-defined* emergency responders].

Supplemental Guidance: Organizations can identify specific personnel, roles, and emergency responders in the event that individuals on the notification list must have appropriate access authorizations and/or clearances, for example, to obtain access to facilities where classified operations are taking place or where there are information systems containing classified information.

(3) *FIRE PROTECTION | AUTOMATIC FIRE SUPPRESSION*

The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

(4) *FIRE PROTECTION | INSPECTIONS*

The organization ensures that the facility undergoes [*Assignment: organization-defined frequency*] inspections by authorized and qualified inspectors and resolves identified deficiencies within [*Assignment: organization-defined time period*].

References: None.

Priority and Baseline Allocation:

P1	**LOW** PE-13	**MOD** PE-13 (3)	**HIGH** PE-13 (1) (2) (3)

PE-14 TEMPERATURE AND HUMIDITY CONTROLS

Control: The organization:

a. Maintains temperature and humidity levels within the facility where the information system resides at [*Assignment: organization-defined acceptable levels*]; and

b. Monitors temperature and humidity levels [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control applies primarily to facilities containing concentrations of information system resources, for example, data centers, server rooms, and mainframe computer rooms. Related control: AT-3.

Control Enhancements:

(1) *TEMPERATURE AND HUMIDITY CONTROLS | AUTOMATIC CONTROLS*

The organization employs automatic temperature and humidity controls in the facility to prevent fluctuations potentially harmful to the information system.

(2) *TEMPERATURE AND HUMIDITY CONTROLS | MONITORING WITH ALARMS / NOTIFICATIONS*

The organization employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.

References: None.

Priority and Baseline Allocation:

P1	**LOW** PE-14	**MOD** PE-14	**HIGH** PE-14

PE-15 WATER DAMAGE PROTECTION

Control: The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Supplemental Guidance: This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern, without affecting entire organizations. Related control: AT-3.

Control Enhancements:

(1) *WATER DAMAGE PROTECTION | AUTOMATION SUPPORT*

The organization employs automated mechanisms to detect the presence of water in the vicinity of the information system and alerts [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: Automated mechanisms can include, for example, water detection sensors, alarms, and notification systems.

References: None.

Priority and Baseline Allocation:

P1	**LOW** PE-15	**MOD** PE-15	**HIGH** PE-15 (1)

PE-16 DELIVERY AND REMOVAL

Control: The organization authorizes, monitors, and controls [*Assignment: organization-defined types of information system components*] entering and exiting the facility and maintains records of those items.

Supplemental Guidance: Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries. Related controls: CM-3, MA-2, MA-3, MP-5, SA-12.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** PE-16	**MOD** PE-16	**HIGH** PE-16

PE-17 ALTERNATE WORK SITE

Control: The organization:

a. Employs [*Assignment: organization-defined security controls*] at alternate work sites;

b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and

c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

Supplemental Guidance: Alternate work sites may include, for example, government facilities or private residences of employees. While commonly distinct from alternative processing sites, alternate work sites may provide readily available alternate locations as part of contingency operations. Organizations may define different sets of security controls for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites. This control supports the contingency planning activities of organizations and the federal telework initiative. Related controls: AC-17, CP-7.

Control Enhancements: None.

References: NIST Special Publication 800-46.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** PE-17	**HIGH** PE-17

PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS

Control: The organization positions information system components within the facility to minimize potential damage from [*Assignment: organization-defined physical and environmental hazards*] and to minimize the opportunity for unauthorized access.

Supplemental Guidance: Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. In addition, organizations consider the location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to information systems and therefore increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones). Related controls: CP-2, PE-19, RA-3.

Control Enhancements:

(1) *LOCATION OF INFORMATION SYSTEM COMPONENTS | FACILITY SITE*

The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.

Supplemental Guidance: Related control: PM-8.

References: None.

Priority and Baseline Allocation:

P3	**LOW** Not Selected	**MOD** Not Selected	**HIGH** PE-18

PE-19 INFORMATION LEAKAGE

Control: The organization protects the information system from information leakage due to electromagnetic signals emanations.

Supplemental Guidance: Information leakage is the intentional or unintentional release of information to an untrusted environment from electromagnetic signals emanations. Security categories or classifications of information systems (with respect to confidentiality) and organizational security policies guide the selection of security controls employed to protect systems against information leakage due to electromagnetic signals emanations.

Control Enhancements:

(1) *INFORMATION LEAKAGE | NATIONAL EMISSIONS / TEMPEST POLICIES AND PROCEDURES*

The organization ensures that information system components, associated data communications, and networks are protected in accordance with national emissions and TEMPEST policies and procedures based on the security category or classification of the information.

References: FIPS Publication 199.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

PE-20 ASSET MONITORING AND TRACKING

Control: The organization:

a. Employs [*Assignment: organization-defined asset location technologies*] to track and monitor the location and movement of [*Assignment: organization-defined assets*] within [*Assignment: organization-defined controlled areas*]; and

b. Ensures that asset location technologies are employed in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

Supplemental Guidance: Asset location technologies can help organizations ensure that critical assets such as vehicles or essential information system components remain in authorized locations. Organizations consult with the Office of the General Counsel and the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) regarding the deployment and use of asset location technologies to address potential privacy concerns. Related control: CM-8.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: PLANNING

PL-1 SECURITY PLANNING POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

   1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and

b. Reviews and updates the current:

   1. Security planning policy [*Assignment: organization-defined frequency*]; and

   2. Security planning procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PL family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-18, 800-100.

Priority and Baseline Allocation:

P1	**LOW** PL-1	**MOD** PL-1	**HIGH** PL-1

PL-2 SYSTEM SECURITY PLAN

Control: The organization:

a. Develops a security plan for the information system that:

   1. Is consistent with the organization's enterprise architecture;

   2. Explicitly defines the authorization boundary for the system;

   3. Describes the operational context of the information system in terms of missions and business processes;

   4. Provides the security categorization of the information system including supporting rationale;

   5. Describes the operational environment for the information system and relationships with or connections to other information systems;

   6. Provides an overview of the security requirements for the system;

   7. Identifies any relevant overlays, if applicable;

8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;

b. Distributes copies of the security plan and communicates subsequent changes to the plan to [*Assignment: organization-defined personnel or roles*];

c. Reviews the security plan for the information system [*Assignment: organization-defined frequency*];

d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and

e. Protects the security plan from unauthorized disclosure and modification.

Supplemental Guidance: Security plans relate security requirements to a set of security controls and control enhancements. Security plans also describe, at a high level, how the security controls and control enhancements meet those security requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls/enhancements. Security plans contain sufficient information (including the specification of parameter values for assignment and selection statements either explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented as intended. Organizations can also apply tailoring guidance to the security control baselines in Appendix D and CNSS Instruction 1253 to develop *overlays* for community-wide use or to address specialized requirements, technologies, or missions/environments of operation (e.g., DoD-tactical, Federal Public Key Infrastructure, or Federal Identity, Credential, and Access Management, space operations). Appendix I provides guidance on developing overlays.

Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition. For example, security plans do not contain detailed contingency plan or incident response plan information but instead provide explicitly or by reference, sufficient information to define what needs to be accomplished by those plans. Related controls: AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CP-2, IR-8, MA-4, MA-5, MP-2, MP-4, MP-5, PL-7, PM-1, PM-7, PM-8, PM-9, PM-11, SA-5, SA-17.

Control Enhancements:

(1) *SYSTEM SECURITY PLAN | CONCEPT OF OPERATIONS*

[Withdrawn: Incorporated into PL-7].

(2) *SYSTEM SECURITY PLAN | FUNCTIONAL ARCHITECTURE*

[Withdrawn: Incorporated into PL-8].

(3) *SYSTEM SECURITY PLAN | PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES*

The organization plans and coordinates security-related activities affecting the information system with [*Assignment: organization-defined individuals or groups*] before conducting such activities in order to reduce the impact on other organizational entities.

Supplemental Guidance: Security-related activities include, for example, security assessments, audits, hardware and software maintenance, patch management, and contingency plan testing. Advance planning and coordination includes emergency and nonemergency (i.e., planned or nonurgent unplanned) situations. The process defined by organizations to plan and coordinate security-related activities can be included in security plans for information systems or other documents, as appropriate. Related controls: CP-4, IR-4.

References: NIST Special Publication 800-18.

Priority and Baseline Allocation:

P1	**LOW** PL-2	**MOD** PL-2 (3)	**HIGH** PL-2 (3)

PL-3 SYSTEM SECURITY PLAN UPDATE

[Withdrawn: Incorporated into PL-2].

PL-4 RULES OF BEHAVIOR

Control: The organization:

a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;

b. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;

c. Reviews and updates the rules of behavior [*Assignment: organization-defined frequency*]; and

d. Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.

Supplemental Guidance: This control enhancement applies to organizational users. Organizations consider rules of behavior based on individual user roles and responsibilities, differentiating, for example, between rules that apply to privileged users and rules that apply to general users. Establishing rules of behavior for some types of non-organizational users including, for example, individuals who simply receive data/information from federal information systems, is often not feasible given the large number of such users and the limited nature of their interactions with the systems. Rules of behavior for both organizational and non-organizational users can also be established in AC-8, System Use Notification. PL-4 b. (the signed acknowledgment portion of this control) may be satisfied by the security awareness training and role-based security training programs conducted by organizations if such training includes rules of behavior. Organizations can use electronic signatures for acknowledging rules of behavior. Related controls: AC-2, AC-6, AC-8, AC-9, AC-17, AC-18, AC-19, AC-20, AT-2, AT-3, CM-11, IA-2, IA-4, IA-5, MP-7, PS-6, PS-8, SA-5.

Control Enhancements:

(1) *RULES OF BEHAVIOR | SOCIAL MEDIA AND NETWORKING RESTRICTIONS*

The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.

Supplemental Guidance: This control enhancement addresses rules of behavior related to the use of social media/networking sites: (i) when organizational personnel are using such sites for official duties or in the conduct of official business; (ii) when organizational information is involved in social media/networking transactions; and (iii) when personnel are accessing social media/networking sites from organizational information systems. Organizations also address specific rules that prevent unauthorized entities from obtaining and/or inferring non-public organizational information (e.g., system account information, personally identifiable information) from social media/networking sites.

References: NIST Special Publication 800-18.

Priority and Baseline Allocation:

P2	**LOW** PL-4	**MOD** PL-4 (1)	**HIGH** PL-4 (1)

PL-5 PRIVACY IMPACT ASSESSMENT

[Withdrawn: Incorporated into Appendix J, AR-2].

PL-6 SECURITY-RELATED ACTIVITY PLANNING

[Withdrawn: Incorporated into PL-2].

PL-7 SECURITY CONCEPT OF OPERATIONS

Control: The organization:

a. Develops a security Concept of Operations (CONOPS) for the information system containing at a minimum, how the organization intends to operate the system from the perspective of information security; and

b. Reviews and updates the CONOPS [*Assignment: organization-defined frequency*].

Supplemental Guidance: The security CONOPS may be included in the security plan for the information system or in other system development life cycle-related documents, as appropriate. Changes to the CONOPS are reflected in ongoing updates to the security plan, the information security architecture, and other appropriate organizational documents (e.g., security specifications for procurements/acquisitions, system development life cycle documents, and systems/security engineering documents). Related control: PL-2.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

PL-8 INFORMATION SECURITY ARCHITECTURE

Control: The organization:

a. Develops an information security architecture for the information system that:

   1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;

   2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and

   3. Describes any information security assumptions about, and dependencies on, external services;

b. Reviews and updates the information security architecture [*Assignment: organization-defined frequency*] to reflect updates in the enterprise architecture; and

c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

Supplemental Guidance: This control addresses actions taken by organizations in the design and development of information systems. The information security architecture at the individual information system level is consistent with and complements the more global, organization-wide information security architecture described in PM-7 that is integral to and developed as part of the enterprise architecture. The information security architecture includes an architectural description, the placement/allocation of security functionality (including security controls), security-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. In addition, the security architecture can include other important security-related information, for example, user roles and access privileges assigned to each role, unique security requirements, the types of information processed, stored, and transmitted by the information system, restoration priorities of information and information system services, and any other specific protection needs.

In today's modern architecture, it is becoming less common for organizations to control all information resources. There are going to be key dependencies on external information services and service providers. Describing such dependencies in the information security architecture is important to developing a comprehensive mission/business protection strategy. Establishing, developing, documenting, and maintaining under configuration control, a baseline configuration for organizational information systems is critical to implementing and maintaining an effective information security architecture. The development of the information security architecture is coordinated with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) to ensure that security controls needed to support privacy requirements are identified and effectively implemented. PL-8 is primarily directed at organizations (i.e., internally focused) to help ensure that organizations develop an information security architecture for the information system, and that the security architecture is integrated with or tightly coupled to the enterprise architecture through the organization-wide information security architecture. In contrast, SA-17 is primarily directed at external information technology product/system developers and integrators (although SA-17 could be used internally within organizations for in-house system development). SA-17, which is complementary to PL-8, is selected when organizations outsource the development of information systems or information system components to external entities, and there is a need to demonstrate/show consistency with the organization's enterprise architecture and information security architecture. Related controls: CM-2, CM-6, PL-2, PM-7, SA-5, SA-17, Appendix J.

Control Enhancements:

(1) *INFORMATION SECURITY ARCHITECTURE | DEFENSE-IN-DEPTH*

The organization designs its security architecture using a defense-in-depth approach that:

(a) Allocates [*Assignment: organization-defined security safeguards*] to [*Assignment: organization-defined locations and architectural layers*]; and

(b) Ensures that the allocated security safeguards operate in a coordinated and mutually reinforcing manner.

Supplemental Guidance: Organizations strategically allocate security safeguards (procedural, technical, or both) in the security architecture so that adversaries have to overcome multiple safeguards to achieve their objective. Requiring adversaries to defeat multiple mechanisms makes it more difficult to successfully attack critical information resources (i.e., increases adversary work factor) and also increases the likelihood of detection. The coordination of allocated safeguards is essential to ensure that an attack that involves one safeguard does not create adverse unintended consequences (e.g., lockout, cascading alarms) by interfering with another safeguard. Placement of security safeguards is a key activity. Greater asset criticality or information value merits additional layering. Thus, an organization may choose to place anti-virus software at organizational boundary layers, email/web servers, notebook computers, and workstations to maximize the number of related safeguards adversaries must penetrate before compromising the information and information systems. Related controls: SC-29, SC-36.

(2) *INFORMATION SECURITY ARCHITECTURE | SUPPLIER DIVERSITY*

The organization requires that [*Assignment: organization-defined security safeguards*] allocated to [*Assignment: organization-defined locations and architectural layers*] are obtained from different suppliers.

Supplemental Guidance: Different information technology products have different strengths and weaknesses. Providing a broad spectrum of products complements the individual offerings. For example, vendors offering malicious code protection typically update their products at different times, often developing solutions for known viruses, Trojans, or worms according to their priorities and development schedules. By having different products at different locations (e.g., server, boundary, desktop) there is an increased likelihood that at least one will detect the malicious code. Related control: SA-12.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** PL-8	**HIGH** PL-8

PL-9 CENTRAL MANAGEMENT

Control: The organization centrally manages [*Assignment: organization-defined security controls and related processes*].

Supplemental Guidance: Central management refers to the organization-wide management and implementation of selected security controls and related processes. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed security controls and processes. As central management of security controls is generally associated with common controls, such management promotes and facilitates standardization of security control implementations and management and judicious use of organizational resources. Centrally-managed security controls and processes may also meet independence requirements for assessments in support of initial and ongoing authorizations to operate as part of organizational continuous monitoring. As part of the security control selection process, organizations determine which controls may be suitable for central management based on organizational resources and capabilities. Organizations consider that it may not always be possible to centrally manage every aspect of a security control. In such cases, the security control is treated as a hybrid control with the control managed and implemented either centrally or at the information system level. Controls and control enhancements that are candidates for full or partial central management include, but are not limited to: AC-2 (1) (2) (3) (4); AC-17 (1) (2) (3) (9); AC-18 (1) (3) (4) (5); AC-19 (4); AC-22; AC-23; AT-2 (1) (2); AT-3 (1) (2) (3); AT-4; AU-6 (1) (3) (5) (6) (9); AU-7 (1) (2); AU-11, AU-13, AU-16, CA-2 (1) (2) (3); CA-3 (1) (2) (3); CA-7 (1); CA-9; CM-2 (1) (2); CM-3 (1) (4); CM-4; CM-6 (1); CM-7 (4) (5); CM-8 (all); CM-9 (1); CM-10; CM-11; CP-7 (all); CP-8 (all); SC-43; SI-2; SI-3; SI-7; and SI-8.

Control Enhancements: None.

References: NIST Special Publication 800-37.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: PERSONNEL SECURITY

PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

   1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and

b. Reviews and updates the current:

   1. Personnel security policy [*Assignment: organization-defined frequency*]; and

   2. Personnel security procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PS family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** PS-1	**MOD** PS-1	**HIGH** PS-1

PS-2 POSITION RISK DESIGNATION

Control: The organization:

a. Assigns a risk designation to all organizational positions;

b. Establishes screening criteria for individuals filling those positions; and

c. Reviews and updates position risk designations [*Assignment: organization-defined frequency*].

Supplemental Guidance: Position risk designations reflect Office of Personnel Management policy and guidance. Risk designations can guide and inform the types of authorizations individuals receive when accessing organizational information and information systems. Position screening criteria include explicit information security role appointment requirements (e.g., training, security clearances). Related controls: AT-3, PL-2, PS-3.

Control Enhancements: None.

References: 5 C.F.R. 731.106.

Priority and Baseline Allocation:

P1	**LOW** PS-2	**MOD** PS-2	**HIGH** PS-2

PS-3 PERSONNEL SCREENING

Control: The organization:

a. Screens individuals prior to authorizing access to the information system; and

b. Rescreens individuals according to [*Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening*].

Supplemental Guidance: Personnel screening and rescreening activities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions. Organizations may define different rescreening conditions and frequencies for personnel accessing information systems based on types of information processed, stored, or transmitted by the systems. Related controls: AC-2, IA-4, PE-2, PS-2.

Control Enhancements:

(1) *PERSONNEL SCREENING | CLASSIFIED INFORMATION*

The organization ensures that individuals accessing an information system processing, storing, or transmitting classified information are cleared and indoctrinated to the highest classification level of the information to which they have access on the system.

Supplemental Guidance: Related controls: AC-3, AC-4.

(2) *PERSONNEL SCREENING | FORMAL INDOCTRINATION*

The organization ensures that individuals accessing an information system processing, storing, or transmitting types of classified information which require formal indoctrination, are formally indoctrinated for all of the relevant types of information to which they have access on the system.

Supplemental Guidance: Types of classified information requiring formal indoctrination include, for example, Special Access Program (SAP), Restricted Data (RD), and Sensitive Compartment Information (SCI). Related controls: AC-3, AC-4.

(3) *PERSONNEL SCREENING | INFORMATION WITH SPECIAL PROTECTION MEASURES*

The organization ensures that individuals accessing an information system processing, storing, or transmitting information requiring special protection:

(a) Have valid access authorizations that are demonstrated by assigned official government duties; and

(b) Satisfy [*Assignment: organization-defined additional personnel screening criteria*].

Supplemental Guidance: Organizational information requiring special protection includes, for example, Controlled Unclassified Information (CUI) and Sources and Methods Information (SAMI). Personnel security criteria include, for example, position sensitivity background screening requirements.

References: 5 C.F.R. 731.106; FIPS Publications 199, 201; NIST Special Publications 800-60, 800-73, 800-76, 800-78; ICD 704.

Priority and Baseline Allocation:

P1	**LOW** PS-3	**MOD** PS-3	**HIGH** PS-3

PS-4 PERSONNEL TERMINATION

Control: The organization, upon termination of individual employment:

a. Disables information system access within [*Assignment: organization-defined time period*];

b. Terminates/revokes any authenticators/credentials associated with the individual;

c. Conducts exit interviews that include a discussion of [*Assignment: organization-defined information security topics*];

d. Retrieves all security-related organizational information system-related property;

e. Retains access to organizational information and information systems formerly controlled by terminated individual; and

f. Notifies [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*].

Supplemental Guidance: Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and nonavailability of supervisors. Exit interviews are important for individuals with security clearances. Timely execution of termination actions is essential for individuals terminated for cause. In certain situations, organizations consider disabling the information system accounts of individuals that are being terminated prior to the individuals being notified. Related controls: AC-2, IA-4, PE-2, PS-5, PS-6.

Control Enhancements:

(1) *PERSONNEL TERMINATION | POST-EMPLOYMENT REQUIREMENTS*

The organization:

(a) Notifies terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information; and

(b) Requires terminated individuals to sign an acknowledgment of post-employment requirements as part of the organizational termination process.

Supplemental Guidance: Organizations consult with the Office of the General Counsel regarding matters of post-employment requirements on terminated individuals.

(2) *PERSONNEL TERMINATION | AUTOMATED NOTIFICATION*

The organization employs automated mechanisms to notify [*Assignment: organization-defined personnel or roles*] upon termination of an individual.

Supplemental Guidance: In organizations with a large number of employees, not all personnel who need to know about termination actions receive the appropriate notifications—or, if such notifications are received, they may not occur in a timely manner. Automated mechanisms can be used to send automatic alerts or notifications to specific organizational personnel or roles (e.g., management personnel, supervisors, personnel security officers, information security officers, systems administrators, or information technology administrators) when individuals are terminated. Such automatic alerts or notifications can be conveyed in a variety of ways, including, for example, telephonically, via electronic mail, via text message, or via websites.

References: None.

Priority and Baseline Allocation:

P1	**LOW** PS-4	**MOD** PS-4	**HIGH** PS-4 (2)

PS-5 PERSONNEL TRANSFER

Control: The organization:

a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;

b. Initiates [*Assignment: organization-defined transfer or reassignment actions*] within [*Assignment: organization-defined time period following the formal transfer action*];

c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and

d. Notifies [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*].

Supplemental Guidance: This control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted. Organizations define actions appropriate for the types of reassignments or transfers, whether permanent or extended. Actions that may be required for personnel transfers or reassignments to other positions within organizations include, for example: (i) returning old and issuing new keys, identification cards, and building passes; (ii) closing information system accounts and establishing new accounts; (iii) changing information system access authorizations (i.e., privileges); and (iv) providing for access to official records to which individuals had access at previous work locations and in previous information system accounts. Related controls: AC-2, IA-4, PE-2, PS-4.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** PS-5	**MOD** PS-5	**HIGH** PS-5

PS-6 ACCESS AGREEMENTS

Control: The organization:

a. Develops and documents access agreements for organizational information systems;

b. Reviews and updates the access agreements [*Assignment: organization-defined frequency*]; and

c. Ensures that individuals requiring access to organizational information and information systems:

   1. Sign appropriate access agreements prior to being granted access; and

   2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [*Assignment: organization-defined frequency*].

Supplemental Guidance: Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to

abide by the constraints associated with organizational information systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy. Related control: PL-4, PS-2, PS-3, PS-4, PS-8.

Control Enhancements:

(1) *ACCESS AGREEMENTS | INFORMATION REQUIRING SPECIAL PROTECTION*

[Withdrawn: Incorporated into PS-3].

(2) *ACCESS AGREEMENTS | CLASSIFIED INFORMATION REQUIRING SPECIAL PROTECTION*

The organization ensures that access to classified information requiring special protection is granted only to individuals who:

(a) Have a valid access authorization that is demonstrated by assigned official government duties;

(b) Satisfy associated personnel security criteria; and

(c) Have read, understood, and signed a nondisclosure agreement.

Supplemental Guidance: Classified information requiring special protection includes, for example, collateral information, Special Access Program (SAP) information, and Sensitive Compartmented Information (SCI). Personnel security criteria reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

(3) *ACCESS AGREEMENTS | POST-EMPLOYMENT REQUIREMENTS*

The organization:

(a) Notifies individuals of applicable, legally binding post-employment requirements for protection of organizational information; and

(b) Requires individuals to sign an acknowledgment of these requirements, if applicable, as part of granting initial access to covered information.

Supplemental Guidance: Organizations consult with the Office of the General Counsel regarding matters of post-employment requirements on terminated individuals.

References: None.

Priority and Baseline Allocation:

P3	**LOW** PS-6	**MOD** PS-6	**HIGH** PS-6

PS-7 THIRD-PARTY PERSONNEL SECURITY

Control: The organization:

a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;

b. Requires third-party providers to comply with personnel security policies and procedures established by the organization;

c. Documents personnel security requirements;

d. Requires third-party providers to notify [*Assignment: organization-defined personnel or roles*] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [*Assignment: organization-defined time period*]; and

e. Monitors provider compliance.

Supplemental Guidance: Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. Organizations explicitly include personnel security requirements in acquisition-related documents. Third-party providers

may have personnel working at organizational facilities with credentials, badges, or information system privileges issued by organizations. Notifications of third-party personnel changes ensure appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include, for example, functions, roles, and nature of credentials/privileges associated with individuals transferred or terminated. Related controls: PS-2, PS-3, PS-4, PS-5, PS-6, SA-9, SA-21.

Control Enhancements: None.

References: NIST Special Publication 800-35.

Priority and Baseline Allocation:

P1	**LOW** PS-7	**MOD** PS-7	**HIGH** PS-7

PS-8 PERSONNEL SANCTIONS

Control: The organization:

a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and

b. Notifies [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Supplemental Guidance: Organizational sanctions processes reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Sanctions processes are described in access agreements and can be included as part of general personnel policies and procedures for organizations. Organizations consult with the Office of the General Counsel regarding matters of employee sanctions. Related controls: PL-4, PS-6.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P3	**LOW** PS-8	**MOD** PS-8	**HIGH** PS-8

FAMILY: RISK ASSESSMENT

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

   1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and

b. Reviews and updates the current:

   1. Risk assessment policy [*Assignment: organization-defined frequency*]; and

   2. Risk assessment procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the RA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-30, 800-100.

Priority and Baseline Allocation:

P1	**LOW** RA-1	**MOD** RA-1	**HIGH** RA-1

RA-2 SECURITY CATEGORIZATION

Control: The organization:

a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and

c. Ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

Supplemental Guidance: Clearly defined authorization boundaries are a prerequisite for effective security categorization decisions. Security categories describe the potential adverse impacts to organizational operations, organizational assets, and individuals if organizational information and information systems are comprised through a loss of confidentiality, integrity, or availability. Organizations conduct the security categorization process as an organization-wide activity with the involvement of chief information officers, senior information security officers, information system owners, mission/business owners, and information owners/stewards. Organizations also

consider the potential adverse impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level adverse impacts. Security categorization processes carried out by organizations facilitate the development of inventories of information assets, and along with CM-8, mappings to specific information system components where information is processed, stored, or transmitted. Related controls: CM-8, MP-4, RA-3, SC-7.

Control Enhancements: None.

References: FIPS Publication 199; NIST Special Publications 800-30, 800-39, 800-60.

Priority and Baseline Allocation:

P1	**LOW** RA-2	**MOD** RA-2	**HIGH** RA-2

RA-3 RISK ASSESSMENT

Control: The organization:

a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;

b. Documents risk assessment results in [*Selection: security plan; risk assessment report;* [*Assignment: organization-defined document*]];

c. Reviews risk assessment results [*Assignment: organization-defined frequency*];

d. Disseminates risk assessment results to [*Assignment: organization-defined personnel or roles*]; and

e. Updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Supplemental Guidance: Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation based on the operation and use of information systems. Risk assessments also take into account risk from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems.

Risk assessments (either formal or informal) can be conducted at all three tiers in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any phase in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. RA-3 is noteworthy in that the control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework. Risk assessments can play an important role in security control selection processes, particularly during the application of tailoring guidance, which includes security control supplementation. Related controls: RA-2, PM-9.

Control Enhancements: None.

References: OMB Memorandum 04-04; NIST Special Publications 800-30, 800-39; Web: http://idmanagement.gov.

Priority and Baseline Allocation:

P1	**LOW** RA-3	**MOD** RA-3	**HIGH** RA-3

RA-4 RISK ASSESSMENT UPDATE

[Withdrawn: Incorporated into RA-3].

RA-5 VULNERABILITY SCANNING

Control: The organization:

a. Scans for vulnerabilities in the information system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system/applications are identified and reported;

b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

   1. Enumerating platforms, software flaws, and improper configurations;

   2. Formatting checklists and test procedures; and

   3. Measuring vulnerability impact;

c. Analyzes vulnerability scan reports and results from security control assessments;

d. Remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk; and

e. Shares information obtained from the vulnerability scanning process and security control assessments with [*Assignment: organization-defined personnel or roles*] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Supplemental Guidance: Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans. Organizations determine the required vulnerability scanning for all information system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Vulnerability scanning includes, for example: (i) scanning for patch levels; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms. Organizations consider using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to determine/test for the presence of vulnerabilities. Suggested sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). In addition, security control assessments such as red team exercises provide other sources of potential vulnerabilities for which to scan. Organizations also consider using tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS). Related controls: CA-2, CA-7, CM-4, CM-6, RA-2, RA-3, SA-11, SI-2.

Control Enhancements:

(1) *VULNERABILITY SCANNING | UPDATE TOOL CAPABILITY*

The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.

Supplemental Guidance: The vulnerabilities to be scanned need to be readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This updating process helps to ensure that potential vulnerabilities in the information system are identified and addressed as quickly as possible. Related controls: SI-3, SI-7.

(2) *VULNERABILITY SCANNING | UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED*

The organization updates the information system vulnerabilities scanned [*Selection (one or more):* [*Assignment: organization-defined frequency*]*; prior to a new scan; when new vulnerabilities are identified and reported*].

Supplemental Guidance: Related controls: SI-3, SI-5.

(3) *VULNERABILITY SCANNING | BREADTH / DEPTH OF COVERAGE*

The organization employs vulnerability scanning procedures that can identify the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).

(4) *VULNERABILITY SCANNING | DISCOVERABLE INFORMATION*

The organization determines what information about the information system is discoverable by adversaries and subsequently takes [*Assignment: organization-defined corrective actions*].

Supplemental Guidance: Discoverable information includes information that adversaries could obtain without directly compromising or breaching the information system, for example, by collecting information the system is exposing or by conducting extensive searches of the web. Corrective actions can include, for example, notifying appropriate organizational personnel, removing designated information, or changing the information system to make designated information less relevant or attractive to adversaries. Related control: AU-13.

(5) *VULNERABILITY SCANNING | PRIVILEGED ACCESS*

The information system implements privileged access authorization to [*Assignment: organization-identified information system components*] for selected [*Assignment: organization-defined vulnerability scanning activities*].

Supplemental Guidance: In certain situations, the nature of the vulnerability scanning may be more intrusive or the information system component that is the subject of the scanning may contain highly sensitive information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and also protects the sensitive nature of such scanning.

(6) *VULNERABILITY SCANNING | AUTOMATED TREND ANALYSES*

The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.

Supplemental Guidance: Related controls: IR-4, IR-5, SI-4.

(7) *VULNERABILITY SCANNING | AUTOMATED DETECTION AND NOTIFICATION OF UNAUTHORIZED COMPONENTS*

[Withdrawn: Incorporated into CM-8].

(8) *VULNERABILITY SCANNING | REVIEW HISTORIC AUDIT LOGS*

The organization reviews historic audit logs to determine if a vulnerability identified in the information system has been previously exploited.

Supplemental Guidance: Related control: AU-6.

(9) *VULNERABILITY SCANNING | PENETRATION TESTING AND ANALYSES*

[Withdrawn: Incorporated into CA-8].

(10) *VULNERABILITY SCANNING | CORRELATE SCANNING INFORMATION*

The organization correlates the output from vulnerability scanning tools to determine the presence of multi-vulnerability/multi-hop attack vectors.

References: NIST Special Publications 800-40, 800-70, 800-115; Web: http://cwe.mitre.org, http://nvd.nist.gov.

Priority and Baseline Allocation:

P1	**LOW** RA-5	**MOD** RA-5 (1) (2) (5)	**HIGH** RA-5 (1) (2) (4) (5)

RA-6 TECHNICAL SURVEILLANCE COUNTERMEASURES SURVEY

Control: The organization employs a technical surveillance countermeasures survey at [*Assignment: organization-defined locations*] [*Selection (one or more):* [*Assignment: organization-defined frequency*]; [*Assignment: organization-defined events or indicators occur*]].

Supplemental Guidance: Technical surveillance countermeasures surveys are performed by qualified personnel to detect the presence of technical surveillance devices/hazards and to identify technical security weaknesses that could aid in the conduct of technical penetrations of surveyed facilities. Such surveys provide evaluations of the technical security postures of organizations and facilities and typically include thorough visual, electronic, and physical examinations in and about surveyed facilities. The surveys also provide useful input into risk assessments and organizational exposure to potential adversaries.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: SYSTEM AND SERVICES ACQUISITION

SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

   1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and

b. Reviews and updates the current:

   1. System and services acquisition policy [*Assignment: organization-defined frequency*]; and

   2. System and services acquisition procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** SA-1	**MOD** SA-1	**HIGH** SA-1

SA-2 ALLOCATION OF RESOURCES

Control: The organization:

a. Determines information security requirements for the information system or information system service in mission/business process planning;

b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and

c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

Supplemental Guidance: Resource allocation for information security includes funding for the initial information system or information system service acquisition and funding for the sustainment of the system/service. Related controls: PM-3, PM-11.

Control Enhancements: None.

References: NIST Special Publication 800-65.

Priority and Baseline Allocation:

P1	**LOW** SA-2	**MOD** SA-2	**HIGH** SA-2

SA-3 SYSTEM DEVELOPMENT LIFE CYCLE

Control: The organization:

a. Manages the information system using [*Assignment: organization-defined system development life cycle*] that incorporates information security considerations;

b. Defines and documents information security roles and responsibilities throughout the system development life cycle;

c. Identifies individuals having information security roles and responsibilities; and

d. Integrates the organizational information security risk management process into system development life cycle activities.

Supplemental Guidance: A well-defined system development life cycle provides the foundation for the successful development, implementation, and operation of organizational information systems. To apply the required security controls within the system development life cycle requires a basic understanding of information security, threats, vulnerabilities, adverse impacts, and risk to critical missions/business functions. The security engineering principles in SA-8 cannot be properly applied if individuals that design, code, and test information systems and system components (including information technology products) do not understand security. Therefore, organizations include qualified personnel, for example, chief information security officers, security architects, security engineers, and information system security officers in system development life cycle activities to ensure that security requirements are incorporated into organizational information systems. It is equally important that developers include individuals on the development team that possess the requisite security expertise and skills to ensure that needed security capabilities are effectively integrated into the information system. Security awareness and training programs can help ensure that individuals having key security roles and responsibilities have the appropriate experience, skills, and expertise to conduct assigned system development life cycle activities. The effective integration of security requirements into enterprise architecture also helps to ensure that important security considerations are addressed early in the system development life cycle and that those considerations are directly related to the organizational mission/business processes. This process also facilitates the integration of the information security architecture into the enterprise architecture, consistent with organizational risk management and information security strategies. Related controls: AT-3, PM-7, SA-8.

Control Enhancements: None.

References: NIST Special Publications 800-37, 800-64.

Priority and Baseline Allocation:

P1	**LOW** SA-3	**MOD** SA-3	**HIGH** SA-3

SA-4 ACQUISITION PROCESS

Control: The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

a. Security functional requirements;

b. Security strength requirements;

c. Security assurance requirements;

d. Security-related documentation requirements;

e. Requirements for protecting security-related documentation;

f. Description of the information system development environment and environment in which the system is intended to operate; and

g. Acceptance criteria.

Supplemental Guidance: Information system components are discrete, identifiable information technology assets (e.g., hardware, software, or firmware) that represent the building blocks of an information system. Information system components include commercial information technology products. Security functional requirements include security capabilities, security functions, and security mechanisms. Security strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to direct attack, and resistance to tampering or bypass. Security assurance requirements include: (i) development processes, procedures, practices, and methodologies; and (ii) evidence from development and assessment activities providing grounds for confidence that the required security functionality has been implemented and the required security strength has been achieved. Security documentation requirements address all phases of the system development life cycle.

Security functionality, assurance, and documentation requirements are expressed in terms of security controls and control enhancements that have been selected through the tailoring process. The security control tailoring process includes, for example, the specification of parameter values through the use of assignment and selection statements and the specification of platform dependencies and implementation information. Security documentation provides user and administrator guidance regarding the implementation and operation of security controls. The level of detail required in security documentation is based on the security category or classification level of the information system and the degree to which organizations depend on the stated security capability, functions, or mechanisms to meet overall risk response expectations (as defined in the organizational risk management strategy). Security requirements can also include organizationally mandated configuration settings specifying allowed functions, ports, protocols, and services. Acceptance criteria for information systems, information system components, and information system services are defined in the same manner as such criteria for any organizational acquisition or procurement. The Federal Acquisition Regulation (FAR) Section 7.103 contains information security requirements from FISMA. Related controls: CM-6, PL-2, PS-7, SA-3, SA-5, SA-8, SA-11, SA-12.

Control Enhancements:

(1) *ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS*

The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.

Supplemental Guidance: Functional properties of security controls describe the functionality (i.e., security capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls. Related control: SA-5.

(2) *ACQUISITION PROCESS | DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS*

The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [*Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics;* [*Assignment: organization-defined design/implementation information*]] at [*Assignment: organization-defined level of detail*].

Supplemental Guidance: Organizations may require different levels of detail in design and implementation documentation for security controls employed in organizational information systems, system components, or information system services based on mission/business requirements, requirements for trustworthiness/resiliency, and requirements for analysis and testing. Information systems can be partitioned into multiple subsystems. Each subsystem within the system can contain one or more modules. The high-level design for the system is expressed in terms of multiple subsystems and the interfaces between subsystems providing security-relevant functionality. The low-level design for the system is expressed in terms of modules with particular emphasis on software and firmware (but not excluding hardware) and the interfaces between modules providing security-relevant functionality. Source code and hardware schematics are typically referred to as the implementation representation of the information system. Related control: SA-5.

(3) *ACQUISITION PROCESS | DEVELOPMENT METHODS / TECHNIQUES / PRACTICES*

The organization requires the developer of the information system, system component, or information system service to demonstrate the use of a system development life cycle that includes [*Assignment: organization-defined state-of-the-practice system/security engineering methods, software development methods, testing/evaluation/validation techniques, and quality control processes*].

Supplemental Guidance: Following a well-defined system development life cycle that includes state-of-the-practice software development methods, systems/security engineering methods, quality control processes, and testing, evaluation, and validation techniques helps to reduce the number and severity of latent errors within information systems, system components, and information system services. Reducing the number/severity of such errors reduces the number of vulnerabilities in those systems, components, and services. Related control: SA-12.

(4) *ACQUISITION PROCESS | ASSIGNMENT OF COMPONENTS TO SYSTEMS*

[Withdrawn: Incorporated into CM-8 (9)].

(5) *ACQUISITION PROCESS | SYSTEM / COMPONENT / SERVICE CONFIGURATIONS*

The organization requires the developer of the information system, system component, or information system service to:

(a) Deliver the system, component, or service with [*Assignment: organization-defined security configurations*] implemented; and

(b) Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.

Supplemental Guidance: Security configurations include, for example, the U.S. Government Configuration Baseline (USGCB) and any limitations on functions, ports, protocols, and services. Security characteristics include, for example, requiring that all default passwords have been changed. Related control: CM-8.

(6) *ACQUISITION PROCESS | USE OF INFORMATION ASSURANCE PRODUCTS*

The organization:

(a) Employs only government off-the-shelf (GOTS) or commercial off-the-shelf (COTS) information assurance (IA) and IA-enabled information technology products that compose an NSA-approved solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being transmitted; and

(b) Ensures that these products have been evaluated and/or validated by NSA or in accordance with NSA-approved procedures.

Supplemental Guidance: COTS IA or IA-enabled information technology products used to protect classified information by cryptographic means may be required to use NSA-approved key management. Related controls: SC-8, SC-12, SC-13.

(7) *ACQUISITION PROCESS | NIAP-APPROVED PROTECTION PROFILES*

The organization:

(a) Limits the use of commercially provided information assurance (IA) and IA-enabled information technology products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile for a specific technology type, if such a profile exists; and

(b) Requires, if no NIAP-approved Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, that the cryptographic module is FIPS-validated.

Supplemental Guidance: Related controls: SC-12, SC-13.

(8) *ACQUISITION PROCESS | CONTINUOUS MONITORING PLAN*

The organization requires the developer of the information system, system component, or information system service to produce a plan for the continuous monitoring of security control effectiveness that contains [*Assignment: organization-defined level of detail*].

Supplemental Guidance: The objective of continuous monitoring plans is to determine if the complete set of planned, required, and deployed security controls within the information system, system component, or information system service continue to be effective over time based on the inevitable changes that occur. Developer continuous monitoring plans include a sufficient level of detail such that the information can be incorporated into the continuous monitoring strategies and programs implemented by organizations. Related control: CA-7.

(9) *ACQUISITION PROCESS | FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE*

The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.

Supplemental Guidance: The identification of functions, ports, protocols, and services early in the system development life cycle (e.g., during the initial requirements definition and design phases) allows organizations to influence the design of the information system, information system component, or information system service. This early involvement in the life cycle helps organizations to avoid or minimize the use of functions, ports, protocols, or services that pose unnecessarily high risks and understand the trade-offs involved in blocking specific ports, protocols, or services (or when requiring information system service providers to do so). Early identification of functions, ports, protocols, and services avoids costly retrofitting of security controls after the information system, system component, or information system service has been implemented. SA-9 describes requirements for external information system services with organizations identifying which functions, ports, protocols, and services are provided from external sources. Related controls: CM-7, SA-9.

(10) *ACQUISITION PROCESS | USE OF APPROVED PIV PRODUCTS*

The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

Supplemental Guidance: Related controls: IA-2; IA-8.

References: HSPD-12; ISO/IEC 15408; FIPS Publications 140-2, 201; NIST Special Publications 800-23, 800-35, 800-36, 800-37, 800-64, 800-70, 800-137; Federal Acquisition Regulation; Web: http://www.niap-ccevs.org, http://fips201ep.cio.gov, http://www.acquisition.gov/far.

Priority and Baseline Allocation:

P1	**LOW** SA-4 (10)	**MOD** SA-4 (1) (2) (9) (10)	**HIGH** SA-4 (1) (2) (9) (10)

SA-5 INFORMATION SYSTEM DOCUMENTATION

Control: The organization:

a. Obtains administrator documentation for the information system, system component, or information system service that describes:

   1. Secure configuration, installation, and operation of the system, component, or service;

   2. Effective use and maintenance of security functions/mechanisms; and

   3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;

b. Obtains user documentation for the information system, system component, or information system service that describes:

1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;

2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and

3. User responsibilities in maintaining the security of the system, component, or service;

c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [*Assignment: organization-defined actions*] in response;

d. Protects documentation as required, in accordance with the risk management strategy; and

e. Distributes documentation to [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: This control helps organizational personnel understand the implementation and operation of security controls associated with information systems, system components, and information system services. Organizations consider establishing specific measures to determine the quality/completeness of the content provided. The inability to obtain needed documentation may occur, for example, due to the age of the information system/component or lack of support from developers and contractors. In those situations, organizations may need to recreate selected documentation if such documentation is essential to the effective implementation or operation of security controls. The level of protection provided for selected information system, component, or service documentation is commensurate with the security category or classification of the system. For example, documentation associated with a key DoD weapons system or command and control system would typically require a higher level of protection than a routine administrative system. Documentation that addresses information system vulnerabilities may also require an increased level of protection. Secure operation of the information system, includes, for example, initially starting the system and resuming secure system operation after any lapse in system operation. Related controls: CM-6, CM-8, PL-2, PL-4, PS-2, SA-3, SA-4.

Control Enhancements:

(1) *INFORMATION SYSTEM DOCUMENTATION | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS*
[Withdrawn: Incorporated into SA-4 (1)].

(2) *INFORMATION SYSTEM DOCUMENTATION | SECURITY-RELEVANT EXTERNAL SYSTEM INTERFACES*
[Withdrawn: Incorporated into SA-4 (2)].

(3) *INFORMATION SYSTEM DOCUMENTATION | HIGH-LEVEL DESIGN*
[Withdrawn: Incorporated into SA-4 (2)].

(4) *INFORMATION SYSTEM DOCUMENTATION | LOW-LEVEL DESIGN*
[Withdrawn: Incorporated into SA-4 (2)].

(5) *INFORMATION SYSTEM DOCUMENTATION | SOURCE CODE*
[Withdrawn: Incorporated into SA-4 (2)].

References: None.

Priority and Baseline Allocation:

P2	**LOW** SA-5	**MOD** SA-5	**HIGH** SA-5

SA-6 SOFTWARE USAGE RESTRICTIONS

[Withdrawn: Incorporated into CM-10 and SI-7].

SA-7 USER-INSTALLED SOFTWARE

[Withdrawn: Incorporated into CM-11 and SI-7].

SA-8 SECURITY ENGINEERING PRINCIPLES

Control: The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

Supplemental Guidance: Organizations apply security engineering principles primarily to new development information systems or systems undergoing major upgrades. For legacy systems, organizations apply security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware within those systems. Security engineering principles include, for example: (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are trained on how to build secure software; (vi) tailoring security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions. Related controls: PM-7, SA-3, SA-4, SA-17, SC-2, SC-3.

Control Enhancements: None.

References: NIST Special Publication 800-27.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SA-8	**HIGH** SA-8

SA-9 EXTERNAL INFORMATION SYSTEM SERVICES

Control: The organization:

a. Requires that providers of external information system services comply with organizational information security requirements and employ [*Assignment: organization-defined security controls*] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and

c. Employs [*Assignment: organization-defined processes, methods, and techniques*] to monitor security control compliance by external service providers on an ongoing basis.

Supplemental Guidance: External information system services are services that are implemented outside of the authorization boundaries of organizational information systems. This includes services that are used by, but not a part of, organizational information systems. FISMA and OMB policy require that organizations using external service providers that are processing, storing, or transmitting federal information or operating information systems on behalf of the federal government ensure that such providers meet the same security requirements that federal agencies are required to meet. Organizations establish relationships with external service providers in a variety of ways including, for example, through joint ventures, business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, and supply chain exchanges. The responsibility for managing risks from the use of external information system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a level of confidence that each participating

provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust varies based on the relationships between organizations and the external providers. Organizations document the basis for trust relationships so the relationships can be monitored over time. External information system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define expectations of performance for security controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance. Related controls: CA-3, IR-7, PS-7.

Control Enhancements:

(1) *EXTERNAL INFORMATION SYSTEMS | RISK ASSESSMENTS / ORGANIZATIONAL APPROVALS*

The organization:

(a) Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and

(b) Ensures that the acquisition or outsourcing of dedicated information security services is approved by [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: Dedicated information security services include, for example, incident monitoring, analysis and response, operation of information security-related devices such as firewalls, or key management services. Related controls: CA-6, RA-3.

(2) *EXTERNAL INFORMATION SYSTEMS | IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES*

The organization requires providers of [*Assignment: organization-defined external information system services*] to identify the functions, ports, protocols, and other services required for the use of such services.

Supplemental Guidance: Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be particularly useful when the need arises to understand the trade-offs involved in restricting certain functions/services or blocking certain ports/protocols. Related control: CM-7.

(3) *EXTERNAL INFORMATION SYSTEMS | ESTABLISH / MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS*

The organization establishes, documents, and maintains trust relationships with external service providers based on [*Assignment: organization-defined security requirements, properties, factors, or conditions defining acceptable trust relationships*].

Supplemental Guidance: The degree of confidence that the risk from using external services is at an acceptable level depends on the trust that organizations place in the external providers, individually or in combination. Trust relationships can help organization to gain increased levels of confidence that participating service providers are providing adequate protection for the services rendered. Such relationships can be complicated due to the number of potential entities participating in the consumer-provider interactions, subordinate relationships and levels of trust, and the types of interactions between the parties. In some cases, the degree of trust is based on the amount of direct control organizations are able to exert on external service providers with regard to employment of security controls necessary for the protection of the service/information and the evidence brought forth as to the effectiveness of those controls. The level of control is typically established by the terms and conditions of the contracts or service-level agreements and can range from extensive control (e.g., negotiating contracts or agreements that specify security requirements for the providers) to very limited control (e.g., using contracts or service-level agreements to obtain commodity services such as commercial telecommunications services). In other cases, levels of trust are based on factors that convince organizations that required security controls have been employed and that determinations of control effectiveness exist. For example, separately authorized external information system services provided to organizations through well-established business relationships may provide degrees of trust in such services within the tolerable risk range of the organizations using the services. External service providers may also outsource selected services to other external entities, making the trust relationship more difficult and complicated to manage. Depending on the nature of the services, organizations may find it very difficult to

place significant trust in external providers. This is not due to any inherent untrustworthiness on the part of providers, but to the intrinsic level of risk in the services.

(4) *EXTERNAL INFORMATION SYSTEMS | CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS*

The organization employs [*Assignment: organization-defined security safeguards*] to ensure that the interests of [*Assignment: organization-defined external service providers*] are consistent with and reflect organizational interests.

Supplemental Guidance: As organizations increasingly use external service providers, the possibility exists that the interests of the service providers may diverge from organizational interests. In such situations, simply having the correct technical, procedural, or operational safeguards in place may not be sufficient if the service providers that implement and control those safeguards are not operating in a manner consistent with the interests of the consuming organizations. Possible actions that organizations might take to address such concerns include, for example, requiring background checks for selected service provider personnel, examining ownership records, employing only trustworthy service providers (i.e., providers with which organizations have had positive experiences), and conducting periodic/unscheduled visits to service provider facilities.

(5) *EXTERNAL INFORMATION SYSTEMS | PROCESSING, STORAGE, AND SERVICE LOCATION*

The organization restricts the location of [*Selection (one or more): information processing; information/data; information system services*] to [*Assignment: organization-defined locations*] based on [*Assignment: organization-defined requirements or conditions*].

Supplemental Guidance: The location of information processing, information/data storage, or information system services that are critical to organizations can have a direct impact on the ability of those organizations to successfully execute their missions/business functions. This situation exists when external providers control the location of processing, storage or services. The criteria external providers use for the selection of processing, storage, or service locations may be different from organizational criteria. For example, organizations may want to ensure that data/information storage locations are restricted to certain locations to facilitate incident response activities (e.g., forensic analyses, after-the-fact investigations) in case of information security breaches/compromises. Such incident response activities may be adversely affected by the governing laws or protocols in the locations where processing and storage occur and/or the locations from which information system services emanate.

References: NIST Special Publication 800-35.

Priority and Baseline Allocation:

P1	**LOW** SA-9	**MOD** SA-9 (2)	**HIGH** SA-9 (2)

SA-10 DEVELOPER CONFIGURATION MANAGEMENT

Control: The organization requires the developer of the information system, system component, or information system service to:

a. Perform configuration management during system, component, or service [*Selection (one or more): design; development; implementation; operation*];

b. Document, manage, and control the integrity of changes to [*Assignment: organization-defined configuration items under configuration management*];

c. Implement only organization-approved changes to the system, component, or service;

d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and

e. Track security flaws and flaw resolution within the system, component, or service and report findings to [*Assignment: organization-defined personnel*].

Supplemental Guidance: This control also applies to organizations conducting internal information systems development and integration. Organizations consider the quality and completeness of the configuration management activities conducted by developers as evidence of applying effective security safeguards. Safeguards include, for example, protecting from unauthorized modification or destruction, the master copies of all material used to generate security-relevant portions of the system hardware, software, and firmware. Maintaining the integrity of changes to the information system, information system component, or information system service requires configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes. Configuration items that are placed under configuration management (if existence/use is required by other security controls) include: the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and software/firmware source code with previous versions; and test fixtures and documentation. Depending on the mission/business needs of organizations and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance phases of the life cycle. Related controls: CM-3, CM-4, CM-9, SA-12, SI-2.

Control Enhancements:

(1) *DEVELOPER CONFIGURATION MANAGEMENT | SOFTWARE / FIRMWARE INTEGRITY VERIFICATION*

The organization requires the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components.

Supplemental Guidance: This control enhancement allows organizations to detect unauthorized changes to software and firmware components through the use of tools, techniques, and/or mechanisms provided by developers. Integrity checking mechanisms can also address counterfeiting of software and firmware components. Organizations verify the integrity of software and firmware components, for example, through secure one-way hashes provided by developers. Delivered software and firmware components also include any updates to such components. Related control: SI-7.

(2) *DEVELOPER CONFIGURATION MANAGEMENT | ALTERNATIVE CONFIGURATION MANAGEMENT PROCESSES*

The organization provides an alternate configuration management process using organizational personnel in the absence of a dedicated developer configuration management team.

Supplemental Guidance: Alternate configuration management processes may be required, for example, when organizations use commercial off-the-shelf (COTS) information technology products. Alternate configuration management processes include organizational personnel that: (i) are responsible for reviewing/approving proposed changes to information systems, system components, and information system services; and (ii) conduct security impact analyses prior to the implementation of any changes to systems, components, or services (e.g., a configuration control board that considers security impacts of changes during development and includes representatives of both the organization and the developer, when applicable).

(3) *DEVELOPER CONFIGURATION MANAGEMENT | HARDWARE INTEGRITY VERIFICATION*

The organization requires the developer of the information system, system component, or information system service to enable integrity verification of hardware components.

Supplemental Guidance: This control enhancement allows organizations to detect unauthorized changes to hardware components through the use of tools, techniques, and/or mechanisms provided by developers. Organizations verify the integrity of hardware components, for example, with hard-to-copy labels and verifiable serial numbers provided by developers, and by requiring the implementation of anti-tamper technologies. Delivered hardware components also include updates to such components. Related control: SI-7.

(4) *DEVELOPER CONFIGURATION MANAGEMENT | TRUSTED GENERATION*

The organization requires the developer of the information system, system component, or information system service to employ tools for comparing newly generated versions of security-relevant hardware descriptions and software/firmware source and object code with previous versions.

Supplemental Guidance: This control enhancement addresses changes to hardware, software, and firmware components between versions during development. In contrast, SA-10 (1) and SA-10 (3) allow organizations to detect unauthorized changes to hardware, software, and firmware components through the use of tools, techniques, and/or mechanisms provided by developers.

(5) *DEVELOPER CONFIGURATION MANAGEMENT | MAPPING INTEGRITY FOR VERSION CONTROL*

The organization requires the developer of the information system, system component, or information system service to maintain the integrity of the mapping between the master build data (hardware drawings and software/firmware code) describing the current version of security-relevant hardware, software, and firmware and the on-site master copy of the data for the current version.

Supplemental Guidance: This control enhancement addresses changes to hardware, software, and firmware components during initial development and during system life cycle updates. Maintaining the integrity between the master copies of security-relevant hardware, software, and firmware (including designs and source code) and the equivalent data in master copies on-site in operational environments is essential to ensure the availability of organizational information systems supporting critical missions and/or business functions.

(6) *DEVELOPER CONFIGURATION MANAGEMENT | TRUSTED DISTRIBUTION*

The organization requires the developer of the information system, system component, or information system service to execute procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization are exactly as specified by the master copies.

Supplemental Guidance: The trusted distribution of security-relevant hardware, software, and firmware updates helps to ensure that such updates are faithful representations of the master copies maintained by the developer and have not been tampered with during distribution.

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SA-10	**HIGH** SA-10

SA-11 DEVELOPER SECURITY TESTING AND EVALUATION

Control: The organization requires the developer of the information system, system component, or information system service to:

a. Create and implement a security assessment plan;

b. Perform [*Selection (one or more): unit; integration; system; regression*] testing/evaluation at [*Assignment: organization-defined depth and coverage*];

c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;

d. Implement a verifiable flaw remediation process; and

e. Correct flaws identified during security testing/evaluation.

Supplemental Guidance: Developmental security testing/evaluation occurs at all post-design phases of the system development life cycle. Such testing/evaluation confirms that the required security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements. Security properties of information systems may be affected by the interconnection of system components or changes to those components. These interconnections or changes (e.g., upgrading or replacing applications and operating systems) may adversely affect previously implemented security controls. This control provides additional types of security testing/evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as static analysis, dynamic

analysis, binary analysis, or a hybrid of the three approaches. Developers can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Security assessment plans provide the specific activities that developers plan to carry out including the types of analyses, testing, evaluation, and reviews of software and firmware components, the degree of rigor to be applied, and the types of artifacts produced during those processes. The *depth* of security testing/evaluation refers to the rigor and level of detail associated with the assessment process (e.g., black box, gray box, or white box testing). The *coverage* of security testing/evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security assessment plans, flaw remediation processes, and the evidence that the plans/processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements. Related controls: CA-2, CM-4, SA-3, SA-4, SA-5, SI-2.

Control Enhancements:

(1) *DEVELOPER SECURITY TESTING AND EVALUATION | STATIC CODE ANALYSIS*

The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

Supplemental Guidance: Static code analysis provides a technology and methodology for security reviews. Such analysis can be used to identify security vulnerabilities and enforce security coding practices. Static code analysis is most effective when used early in the development process, when each code change can be automatically scanned for potential weaknesses. Static analysis can provide clear remediation guidance along with defects to enable developers to fix such defects. Evidence of correct implementation of static analysis can include, for example, aggregate defect density for critical defect types, evidence that defects were inspected by developers or security professionals, and evidence that defects were fixed. An excessively high density of ignored findings (commonly referred to as ignored or false positives) indicates a potential problem with the analysis process or tool. In such cases, organizations weigh the validity of the evidence against evidence from other sources.

(2) *DEVELOPER SECURITY TESTING AND EVALUATION | THREAT AND VULNERABILITY ANALYSES*

The organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service.

Supplemental Guidance: Applications may deviate significantly from the functional and design specifications created during the requirements and design phases of the system development life cycle. Therefore, threat and vulnerability analyses of information systems, system components, and information system services prior to delivery are critical to the effective operation of those systems, components, and services. Threat and vulnerability analyses at this phase of the life cycle help to ensure that design or implementation changes have been accounted for, and that any new vulnerabilities created as a result of those changes have been reviewed and mitigated. Related controls: PM-15, RA-5.

(3) *DEVELOPER SECURITY TESTING AND EVALUATION | INDEPENDENT VERIFICATION OF ASSESSMENT PLANS / EVIDENCE*

The organization:

(a) Requires an independent agent satisfying [*Assignment: organization-defined independence criteria*] to verify the correct implementation of the developer security assessment plan and the evidence produced during security testing/evaluation; and

(b) Ensures that the independent agent either is provided with sufficient information to complete the verification process or has been granted the authority to obtain such information.

Supplemental Guidance: Independent agents have the necessary qualifications (i.e., expertise, skills, training, and experience) to verify the correct implementation of developer security assessment plans. Related controls: AT-3, CA-7, RA-5, SA-12.

(4) *DEVELOPER SECURITY TESTING AND EVALUATION | MANUAL CODE REVIEWS*

The organization requires the developer of the information system, system component, or information system service to perform a manual code review of [Assignment*: organization-defined specific code*] using [*Assignment: organization-defined processes, procedures, and/or techniques*].

Supplemental Guidance: Manual code reviews are usually reserved for the critical software and firmware components of information systems. Such code reviews are uniquely effective at identifying weaknesses that require knowledge of the application's requirements or context which are generally unavailable to more automated analytic tools and techniques such as static or dynamic analysis. Components benefiting from manual review include for example, verifying access control matrices against application controls and reviewing more detailed aspects of cryptographic implementations and controls.

(5) *DEVELOPER SECURITY TESTING AND EVALUATION | PENETRATION TESTING / ANALYSIS*

The organization requires the developer of the information system, system component, or information system service to perform penetration testing at [*Assignment: organization-defined breadth/depth*] and with [*Assignment: organization-defined constraints*].

Supplemental Guidance: Penetration testing is an assessment methodology in which assessors, using all available information technology product and/or information system documentation (e.g., product/system design specifications, source code, and administrator/operator manuals) and working under specific constraints, attempt to circumvent implemented security features of information technology products and information systems. Penetration testing can include, for example, white, gray, or black box testing with analyses performed by skilled security professionals simulating adversary actions. The objective of penetration testing is to uncover potential vulnerabilities in information technology products and information systems resulting from implementation errors, configuration faults, or other operational deployment weaknesses or deficiencies. Penetration tests can be performed in conjunction with automated and manual code reviews to provide greater levels of analysis than would ordinarily be possible.

(6) *DEVELOPER SECURITY TESTING AND EVALUATION | ATTACK SURFACE REVIEWS*

The organization requires the developer of the information system, system component, or information system service to perform attack surface reviews.

Supplemental Guidance: Attack surfaces of information systems are exposed areas that make those systems more vulnerable to cyber attacks. This includes any accessible areas where weaknesses or deficiencies in information systems (including the hardware, software, and firmware components) provide opportunities for adversaries to exploit vulnerabilities. Attack surface reviews ensure that developers: (i) analyze both design and implementation changes to information systems; and (ii) mitigate attack vectors generated as a result of the changes. Correction of identified flaws includes, for example, deprecation of unsafe functions.

(7) *DEVELOPER SECURITY TESTING AND EVALUATION | VERIFY SCOPE OF TESTING / EVALUATION*

The organization requires the developer of the information system, system component, or information system service to verify that the scope of security testing/evaluation provides complete coverage of required security controls at [*Assignment: organization-defined depth of testing/evaluation*].

Supplemental Guidance: Verifying that security testing/evaluation provides complete coverage of required security controls can be accomplished by a variety of analytic techniques ranging from informal to formal. Each of these techniques provides an increasing level of assurance corresponding to the degree of formality of the analysis. Rigorously demonstrating security control coverage at the highest levels of assurance can be provided by the use of formal modeling and analysis techniques including correlation between control implementation and corresponding test cases.

(8) *DEVELOPER SECURITY TESTING AND EVALUATION | DYNAMIC CODE ANALYSIS*

The organization requires the developer of the information system, system component, or information system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

Supplemental Guidance: Dynamic code analysis provides run-time verification of software programs, using tools capable of monitoring programs for memory corruption, user privilege

issues, and other potential security problems. Dynamic code analysis employs run-time tools to help to ensure that security functionality performs in the manner in which it was designed. A specialized type of dynamic analysis, known as fuzz testing, induces program failures by deliberately introducing malformed or random data into software programs. Fuzz testing strategies derive from the intended use of applications and the functional and design specifications for the applications. To understand the scope of dynamic code analysis and hence the assurance provided, organizations may also consider conducting code coverage analysis (checking the degree to which the code has been tested using metrics such as percent of subroutines tested or percent of program statements called during execution of the test suite) and/or concordance analysis (checking for words that are out of place in software code such as non-English language words or derogatory terms).

References: ISO/IEC 15408; NIST Special Publication 800-53A; Web: http://nvd.nist.gov, http://cwe.mitre.org, http://cve.mitre.org, http://capec.mitre.org.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SA-11	**HIGH** SA-11

SA-12 SUPPLY CHAIN PROTECTION

Control: The organization protects against supply chain threats to the information system, system component, or information system service by employing [*Assignment: organization-defined security safeguards*] as part of a comprehensive, defense-in-breadth information security strategy.

Supplemental Guidance: Information systems (including system components that compose those systems) need to be protected throughout the system development life cycle (i.e., during design, development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). Protection of organizational information systems is accomplished through threat awareness, by the identification, management, and reduction of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to respond to risk. Organizations consider implementing a standardized process to address supply chain risk with respect to information systems and system components, and to educate the acquisition workforce on threats, risk, and required security controls. Organizations use the acquisition/procurement processes to require supply chain entities to implement necessary security safeguards to: (i) reduce the likelihood of unauthorized modifications at each stage in the supply chain; and (ii) protect information systems and information system components, prior to taking delivery of such systems/components. This control enhancement also applies to information system services. Security safeguards include, for example: (i) security controls for development systems, development facilities, and external connections to development systems; (ii) vetting development personnel; and (iii) use of tamper-evident packaging during shipping/warehousing. Methods for reviewing and protecting development plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements. Related controls: AT-3, CM-8, IR-4, PE-16, PL-8, SA-3, SA-4, SA-8, SA-10, SA-14, SA-15, SA-18, SA-19, SC-29, SC-30, SC-38, SI-7.

Control Enhancements:

(1) *SUPPLY CHAIN PROTECTION | ACQUISITION STRATEGIES / TOOLS / METHODS*

The organization employs [*Assignment: organization-defined tailored acquisition strategies, contract tools, and procurement methods*] for the purchase of the information system, system component, or information system service from suppliers.

Supplemental Guidance: The use of acquisition and procurement processes by organizations early in the system development life cycle provides an important vehicle to protect the supply chain. Organizations use available all-source intelligence analysis to inform the tailoring of acquisition strategies, tools, and methods. There are a number of different tools and

techniques available (e.g., obscuring the end use of an information system or system component, using blind or filtered buys). Organizations also consider creating incentives for suppliers who: (i) implement required security safeguards; (ii) promote transparency into their organizational processes and security practices; (iii) provide additional vetting of the processes and security practices of subordinate suppliers, critical information system components, and services; (iv) restrict purchases from specific suppliers or countries; and (v) provide contract language regarding the prohibition of tainted or counterfeit components. In addition, organizations consider minimizing the time between purchase decisions and required delivery to limit opportunities for adversaries to corrupt information system components or products. Finally, organizations can use trusted/controlled distribution, delivery, and warehousing options to reduce supply chain risk (e.g., requiring tamper-evident packaging of information system components during shipping and warehousing). Related control: SA-19.

(2) *SUPPLY CHAIN PROTECTION | SUPPLIER REVIEWS*

The organization conducts a supplier review prior to entering into a contractual agreement to acquire the information system, system component, or information system service.

Supplemental Guidance: Supplier reviews include, for example: (i) analysis of supplier processes used to design, develop, test, implement, verify, deliver, and support information systems, system components, and information system services; and (ii) assessment of supplier training and experience in developing systems, components, or services with the required security capability. These reviews provide organizations with increased levels of visibility into supplier activities during the system development life cycle to promote more effective supply chain risk management. Supplier reviews can also help to determine whether primary suppliers have security safeguards in place and a practice for vetting subordinate suppliers, for example, second- and third-tier suppliers, and any subcontractors.

(3) *SUPPLY CHAIN PROTECTION | TRUSTED SHIPPING AND WAREHOUSING*

[Withdrawn: Incorporated into SA-12 (1)].

(4) *SUPPLY CHAIN PROTECTION | DIVERSITY OF SUPPLIERS*

[Withdrawn: Incorporated into SA-12 (13)].

(5) *SUPPLY CHAIN PROTECTION | LIMITATION OF HARM*

The organization employs [*Assignment: organization-defined security safeguards*] to limit harm from potential adversaries identifying and targeting the organizational supply chain.

Supplemental Guidance: Supply chain risk is part of the advanced persistent threat (APT). Security safeguards and countermeasures to reduce the probability of adversaries successfully identifying and targeting the supply chain include, for example: (i) avoiding the purchase of custom configurations to reduce the risk of acquiring information systems, components, or products that have been corrupted via supply chain actions targeted at specific organizations; (ii) employing a diverse set of suppliers to limit the potential harm from any given supplier in the supply chain; (iii) employing approved vendor lists with standing reputations in industry, and (iv) using procurement carve outs (i.e., exclusions to commitments or obligations).

(6) *SUPPLY CHAIN PROTECTION | MINIMIZING PROCUREMENT TIME*

[Withdrawn: Incorporated into SA-12 (1)].

(7) *SUPPLY CHAIN PROTECTION | ASSESSMENTS PRIOR TO SELECTION / ACCEPTANCE / UPDATE*

The organization conducts an assessment of the information system, system component, or information system service prior to selection, acceptance, or update.

Supplemental Guidance: Assessments include, for example, testing, evaluations, reviews, and analyses. Independent, third-party entities or organizational personnel conduct assessments of systems, components, products, tools, and services. Organizations conduct assessments to uncover unintentional vulnerabilities and intentional vulnerabilities including, for example, malicious code, malicious processes, defective software, and counterfeits. Assessments can include, for example, static analyses, dynamic analyses, simulations, white, gray, and black box testing, fuzz testing, penetration testing, and ensuring that components or services are genuine (e.g., using tags, cryptographic hash verifications, or digital signatures). Evidence

generated during security assessments is documented for follow-on actions carried out by organizations. Related controls: CA-2, SA-11.

(8) *SUPPLY CHAIN PROTECTION | USE OF ALL-SOURCE INTELLIGENCE*

The organization uses all-source intelligence analysis of suppliers and potential suppliers of the information system, system component, or information system service.

Supplemental Guidance: All-source intelligence analysis is employed by organizations to inform engineering, acquisition, and risk management decisions. All-source intelligence consists of intelligence products and/or organizations and activities that incorporate all sources of information, most frequently including human intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open source data in the production of finished intelligence. Where available, such information is used to analyze the risk of both intentional and unintentional vulnerabilities from development, manufacturing, and delivery processes, people, and the environment. This review is performed on suppliers at multiple tiers in the supply chain sufficient to manage risks. Related control: SA-15.

(9) *SUPPLY CHAIN PROTECTION | OPERATIONS SECURITY*

The organization employs [*Assignment: organization-defined Operations Security (OPSEC) safeguards*] in accordance with classification guides to protect supply chain-related information for the information system, system component, or information system service.

Supplemental Guidance: Supply chain information includes, for example: user identities; uses for information systems, information system components, and information system services; supplier identities; supplier processes; security requirements; design specifications; testing and evaluation results; and system/component configurations. This control enhancement expands the scope of OPSEC to include suppliers and potential suppliers. OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to operations and other activities to: (i) identify those actions that can be observed by potential adversaries; (ii) determine indicators that adversaries might obtain that could be interpreted or pieced together to derive critical information in sufficient time to cause harm to organizations; (iii) implement safeguards or countermeasures to eliminate or reduce to an acceptable level, exploitable vulnerabilities; and (iv) consider how aggregated information may compromise the confidentiality of users or uses of the supply chain. OPSEC may require organizations to withhold critical mission/business information from suppliers and may include the use of intermediaries to hide the end use, or users, of information systems, system components, or information system services. Related control: PE-21.

(10) *SUPPLY CHAIN PROTECTION | VALIDATE AS GENUINE AND NOT ALTERED*

The organization employs [*Assignment: organization-defined security safeguards*] to validate that the information system or system component received is genuine and has not been altered.

Supplemental Guidance: For some information system components, especially hardware, there are technical means to help determine if the components are genuine or have been altered. Security safeguards used to validate the authenticity of information systems and information system components include, for example, optical/nanotechnology tagging and side-channel analysis. For hardware, detailed bill of material information can highlight the elements with embedded logic complete with component and production location.

(11) *SUPPLY CHAIN PROTECTION | PENETRATION TESTING / ANALYSIS OF ELEMENTS, PROCESSES, AND ACTORS*

The organization employs [*Selection (one or more): organizational analysis, independent third-party analysis, organizational penetration testing, independent third-party penetration testing*] of [*Assignment: organization-defined supply chain elements, processes, and actors*] associated with the *information system, system component, or information system service*.

Supplemental Guidance: This control enhancement addresses analysis and/or testing of the supply chain, not just delivered items. Supply chain elements are information technology products or product components that contain programmable logic and that are critically important to information system functions. Supply chain processes include, for example: (i) hardware, software, and firmware development processes; (ii) shipping/handling procedures; (iii) personnel and physical security programs; (iv) configuration management tools/measures to maintain provenance; or (v) any other programs, processes, or procedures associated with the production/distribution of supply chain elements. Supply chain actors are individuals with

specific roles and responsibilities in the supply chain. The evidence generated during analyses and testing of supply chain elements, processes, and actors is documented and used to inform organizational risk management activities and decisions. Related control: RA-5.

(12) *SUPPLY CHAIN PROTECTION | INTER-ORGANIZATIONAL AGREEMENTS*

The organization establishes inter-organizational agreements and procedures with entities involved in the supply chain for the information system, system component, or information system service.

Supplemental Guidance: The establishment of inter-organizational agreements and procedures provides for notification of supply chain compromises. Early notification of supply chain compromises that can potentially adversely affect or have adversely affected organizational information systems, including critical system components, is essential for organizations to provide appropriate responses to such incidents.

(13) *SUPPLY CHAIN PROTECTION | CRITICAL INFORMATION SYSTEM COMPONENTS*

The organization employs [*Assignment: organization-defined security safeguards*] to ensure an adequate supply of [*Assignment: organization-defined critical information system components*].

Supplemental Guidance: Adversaries can attempt to impede organizational operations by disrupting the supply of critical information system components or corrupting supplier operations. Safeguards to ensure adequate supplies of critical information system components include, for example: (i) the use of multiple suppliers throughout the supply chain for the identified critical components; and (ii) stockpiling of spare components to ensure operation during mission-critical times.

(14) *SUPPLY CHAIN PROTECTION | IDENTITY AND TRACEABILITY*

The organization establishes and retains unique identification of [*Assignment: organization-defined supply chain elements, processes, and actors*] for the information system, system component, or information system service.

Supplemental Guidance: Knowing who and what is in the supply chains of organizations is critical to gaining visibility into what is happening within such supply chains, as well as monitoring and identifying high-risk events and activities. Without reasonable visibility and traceability into supply chains (i.e., elements, processes, and actors), it is very difficult for organizations to understand and therefore manage risk, and to reduce the likelihood of adverse events. Uniquely identifying acquirer and integrator roles, organizations, personnel, mission and element processes, testing and evaluation procedures, delivery mechanisms, support mechanisms, communications/delivery paths, and disposal/final disposition activities as well as the components and tools used, establishes a foundational identity structure for assessment of supply chain activities. For example, labeling (using serial numbers) and tagging (using radio-frequency identification [RFID] tags) individual supply chain elements including software packages, modules, and hardware devices, and processes associated with those elements can be used for this purpose. Identification methods are sufficient to support the provenance in the event of a supply chain issue or adverse supply chain event.

(15) *SUPPLY CHAIN PROTECTION | PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES*

The organization establishes a process to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.

Supplemental Guidance: Evidence generated during independent or organizational assessments of supply chain elements (e.g., penetration testing, audits, verification/validation activities) is documented and used in follow-on processes implemented by organizations to respond to the risks related to the identified weaknesses and deficiencies. Supply chain elements include, for example, supplier development processes and supplier distribution systems.

References: NIST Special Publication 800-161; NIST Interagency Report 7622.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SA-12

SA-13 TRUSTWORTHINESS

Control: The organization:

a. Describes the trustworthiness required in the [*Assignment: organization-defined information system, information system component, or information system service*] supporting its critical missions/business functions; and

b. Implements [*Assignment: organization-defined assurance overlay*] to achieve such trustworthiness.

Supplemental Guidance: This control helps organizations to make explicit trustworthiness decisions when designing, developing, and implementing information systems that are needed to conduct critical organizational missions/business functions. Trustworthiness is a characteristic/property of an information system that expresses the degree to which the system can be expected to preserve the confidentiality, integrity, and availability of the information it processes, stores, or transmits. Trustworthy information systems are systems that are capable of being trusted to operate within defined levels of *risk* despite the environmental disruptions, human errors, and purposeful attacks that are expected to occur in the specified environments of operation. Trustworthy systems are important to mission/business success. Two factors affecting the trustworthiness of information systems include: (i) security functionality (i.e., the security features, functions, and/or mechanisms employed within the system and its environment of operation); and (ii) security assurance (i.e., the grounds for confidence that the security functionality is effective in its application). Developers, implementers, operators, and maintainers of organizational information systems can increase the level of assurance (and trustworthiness), for example, by employing well-defined security policy models, structured and rigorous hardware, software, and firmware development techniques, sound system/security engineering principles, and secure configuration settings (defined by a set of assurance-related security controls in Appendix E).

Assurance is also based on the assessment of evidence produced during the system development life cycle. Critical missions/business functions are supported by high-impact systems and the associated assurance requirements for such systems. The additional assurance controls in Table E-4 in Appendix E (designated as optional) can be used to develop and implement high-assurance solutions for specific information systems and system components using the concept of overlays described in Appendix I. Organizations select assurance overlays that have been developed, validated, and approved for community adoption (e.g., cross-organization, governmentwide), limiting the development of such overlays on an organization-by-organization basis. Organizations can conduct criticality analyses as described in SA-14, to determine the information systems, system components, or information system services that require high-assurance solutions. Trustworthiness requirements and assurance overlays can be described in the security plans for organizational information systems. Related controls: RA-2, SA-4, SA-8, SA-14, SC-3.

Control Enhancements: None.

References: FIPS Publications 199, 200; NIST Special Publications 800-53, 800-53A, 800-60, 800-64.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SA-14 CRITICALITY ANALYSIS

Control: The organization identifies critical information system components and functions by performing a criticality analysis for [*Assignment: organization-defined information systems, information system components, or information system services*] at [*Assignment: organization-defined decision points in the system development life cycle*].

Supplemental Guidance: Criticality analysis is a key tenet of supply chain risk management and informs the prioritization of supply chain protection activities such as attack surface reduction, use of all-source intelligence, and tailored acquisition strategies. Information system engineers can conduct an end-to-end functional decomposition of an information system to identify mission-critical functions and components. The functional decomposition includes the identification of core organizational missions supported by the system, decomposition into the specific functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions, including when the functions are shared by many components within and beyond the information system boundary. Information system components that allow for unmediated access to critical components or functions are considered critical due to the inherent vulnerabilities such components create. Criticality is assessed in terms of the impact of the function or component failure on the ability of the component to complete the organizational missions supported by the information system. A criticality analysis is performed whenever an architecture or design is being developed or modified, including upgrades. Related controls: CP-2, PL-2, PL-8, PM-1, SA-8, SA-12, SA-13, SA-15, SA-20.

Control Enhancements: None.

(1) *CRITICALITY ANALYSIS | CRITICAL COMPONENTS WITH NO VIABLE ALTERNATIVE SOURCING*
[Withdrawn: Incorporated into SA-20].

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SA-15 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS

Control: The organization:

a. Requires the developer of the information system, system component, or information system service to follow a documented development process that:

   1. Explicitly addresses security requirements;

   2. Identifies the standards and tools used in the development process;

   3. Documents the specific tool options and tool configurations used in the development process; and

   4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and

b. Reviews the development process, standards, tools, and tool options/configurations [*Assignment: organization-defined frequency*] to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy [*Assignment: organization-defined security requirements*].

Supplemental Guidance: Development tools include, for example, programming languages and computer-aided design (CAD) systems. Reviews of development processes can include, for example, the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes enables accurate supply chain risk assessment and mitigation, and requires robust configuration control throughout the life cycle (including design, development, transport, delivery, integration, and maintenance) to track authorized changes and prevent unauthorized changes. Related controls: SA-3, SA-8.

Control Enhancements:

(1) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | QUALITY METRICS*

The organization requires the developer of the information system, system component, or information system service to:

(a) Define quality metrics at the beginning of the development process; and

(b) Provide evidence of meeting the quality metrics [*Selection (one or more):* [*Assignment: organization-defined frequency*]; [*Assignment: organization-defined program review milestones*]; *upon delivery*].

Supplemental Guidance: Organizations use quality metrics to establish minimum acceptable levels of information system quality. Metrics may include quality gates which are collections of completion criteria or sufficiency standards representing the satisfactory execution of particular phases of the system development project. A quality gate, for example, may require the elimination of all compiler warnings or an explicit determination that the warnings have no impact on the effectiveness of required security capabilities. During the execution phases of development projects, quality gates provide clear, unambiguous indications of progress. Other metrics apply to the entire development project. These metrics can include defining the severity thresholds of vulnerabilities, for example, requiring no known vulnerabilities in the delivered information system with a Common Vulnerability Scoring System (CVSS) severity of Medium or High.

(2) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | SECURITY TRACKING TOOLS*

The organization requires the developer of the information system, system component, or information system service to select and employ a security tracking tool for use during the development process.

Supplemental Guidance: Information system development teams select and deploy security tracking tools, including, for example, vulnerability/work item tracking systems that facilitate assignment, sorting, filtering, and tracking of completed work items or tasks associated with system development processes.

(3) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CRITICALITY ANALYSIS*

The organization requires the developer of the information system, system component, or information system service to perform a criticality analysis at [*Assignment: organization-defined breadth/depth*] and at [*Assignment: organization-defined decision points in the system development life cycle*].

Supplemental Guidance: This control enhancement provides developer input to the criticality analysis performed by organizations in SA-14. Developer input is essential to such analysis because organizations may not have access to detailed design documentation for information system components that are developed as commercial off-the-shelf (COTS) information technology products (e.g., functional specifications, high-level designs, low-level designs, and source code/hardware schematics). Related controls: SA-4, SA-14.

(4) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | THREAT MODELING / VULNERABILITY ANALYSIS*

The organization requires that developers perform threat modeling and a vulnerability analysis for the information system at [*Assignment: organization-defined breadth/depth*] that:

(a) Uses [*Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels*];

(b) Employs [*Assignment: organization-defined tools and methods*]; and

(c) Produces evidence that meets [*Assignment: organization-defined acceptance criteria*].

Supplemental Guidance: Related control: SA-4.

(5) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ATTACK SURFACE REDUCTION*

The organization requires the developer of the information system, system component, or information system service to reduce attack surfaces to [*Assignment: organization-defined thresholds*].

Supplemental Guidance: Attack surface reduction is closely aligned with developer threat and vulnerability analyses and information system architecture and design. Attack surface reduction is a means of reducing risk to organizations by giving attackers less opportunity to exploit weaknesses or deficiencies (i.e., potential vulnerabilities) within information systems,

information system components, and information system services. Attack surface reduction includes, for example, applying the principle of least privilege, employing layered defenses, applying the principle of least functionality (i.e., restricting ports, protocols, functions, and services), deprecating unsafe functions, and eliminating application programming interfaces (APIs) that are vulnerable to cyber attacks. Related control: CM-7.

(6) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CONTINUOUS IMPROVEMENT*

The organization requires the developer of the information system, system component, or information system service to implement an explicit process to continuously improve the development process.

Supplemental Guidance: Developers of information systems, information system components, and information system services consider the effectiveness/efficiency of current development processes for meeting quality objectives and addressing security capabilities in current threat environments.

(7) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | AUTOMATED VULNERABILITY ANALYSIS*

The organization requires the developer of the information system, system component, or information system service to:

(a) Perform an automated vulnerability analysis using [*Assignment: organization-defined tools*];

(b) Determine the exploitation potential for discovered vulnerabilities;

(c) Determine potential risk mitigations for delivered vulnerabilities; and

(d) Deliver the outputs of the tools and results of the analysis to [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: Related control: RA-5.

(8) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | REUSE OF THREAT / VULNERABILITY INFORMATION*

The organization requires the developer of the information system, system component, or information system service to use threat modeling and vulnerability analyses from similar systems, components, or services to inform the current development process.

Supplemental Guidance: Analysis of vulnerabilities found in similar software applications can inform potential design or implementation issues for information systems under development. Similar information systems or system components may exist within developer organizations. Authoritative vulnerability information is available from a variety of public and private sector sources including, for example, the National Vulnerability Database.

(9) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | USE OF LIVE DATA*

The organization approves, documents, and controls the use of live data in development and test environments for the information system, system component, or information system service.

Supplemental Guidance: The use of live data in preproduction environments can result in significant risk to organizations. Organizations can minimize such risk by using test or dummy data during the development and testing of information systems, information system components, and information system services.

(10) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | INCIDENT RESPONSE PLAN*

The organization requires the developer of the information system, system component, or information system service to provide an incident response plan.

Supplemental Guidance: The incident response plan for developers of information systems, system components, and information system services is incorporated into organizational incident response plans to provide the type of incident response information not readily available to organizations. Such information may be extremely helpful, for example, when organizations respond to vulnerabilities in commercial off-the-shelf (COTS) information technology products. Related control: IR-8.

(11) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ARCHIVE INFORMATION SYSTEM / COMPONENT*

The organization requires the developer of the information system or system component to archive the system or component to be released or delivered together with the corresponding evidence supporting the final security review.

Supplemental Guidance: Archiving relevant documentation from the development process can provide a readily available baseline of information that can be helpful during information system/component upgrades or modifications.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SA-15

SA-16 DEVELOPER-PROVIDED TRAINING

Control: The organization requires the developer of the information system, system component, or information system service to provide [*Assignment: organization-defined training*] on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

Supplemental Guidance: This control applies to external and internal (in-house) developers. Training of personnel is an essential element to ensure the effectiveness of security controls implemented within organizational information systems. Training options include, for example, classroom-style training, web-based/computer-based training, and hands-on training. Organizations can also request sufficient training materials from developers to conduct in-house training or offer self-training to organizational personnel. Organizations determine the type of training necessary and may require different types of training for different security functions, controls, or mechanisms. Related controls: AT-2, AT-3, SA-5.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SA-16

SA-17 DEVELOPER SECURITY ARCHITECTURE AND DESIGN

Control: The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that:

a. Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture;

b. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and

c. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

Supplemental Guidance: This control is primarily directed at external developers, although it could also be used for internal (in-house) development. In contrast, PL-8 is primarily directed at internal developers to help ensure that organizations develop an information security architecture and such security architecture is integrated or tightly coupled to the enterprise architecture. This distinction is important if/when organizations outsource the development of information systems, information system components, or information system services to external entities, and there is a requirement to demonstrate consistency with the organization's enterprise architecture and information security architecture. Related controls: PL-8, PM-7, SA-3, SA-8.

Control Enhancements:

(1) *DEVELOPER SECURITY ARCHITECTURE AND DESIGN | FORMAL POLICY MODEL*

The organization requires the developer of the information system, system component, or information system service to:

(a) Produce, as an integral part of the development process, a formal policy model describing the [*Assignment: organization-defined elements of organizational security policy*] to be enforced; and

(b) Prove that the formal policy model is internally consistent and sufficient to enforce the defined elements of the organizational security policy when implemented.

Supplemental Guidance: Formal models describe specific behaviors or security policies using formal languages, thus enabling the correctness of those behaviors/policies to be formally proven. Not all components of information systems can be modeled, and generally, formal specifications are scoped to specific behaviors or policies of interest (e.g., nondiscretionary access control policies). Organizations choose the particular formal modeling language and approach based on the nature of the behaviors/policies to be described and the available tools. Formal modeling tools include, for example, Gypsy and Zed.

(2) *DEVELOPER SECURITY ARCHITECTURE AND DESIGN | SECURITY-RELEVANT COMPONENTS*

The organization requires the developer of the information system, system component, or information system service to:

(a) Define security-relevant hardware, software, and firmware; and

(b) Provide a rationale that the definition for security-relevant hardware, software, and firmware is complete.

Supplemental Guidance: Security-relevant hardware, software, and firmware represent the portion of the information system, component, or service that must be trusted to perform correctly in order to maintain required security properties. Related control: SA-5.

(3) *DEVELOPER SECURITY ARCHITECTURE AND DESIGN | FORMAL CORRESPONDENCE*

The organization requires the developer of the information system, system component, or information system service to:

(a) Produce, as an integral part of the development process, a formal top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects;

(b) Show via proof to the extent feasible with additional informal demonstration as necessary, that the formal top-level specification is consistent with the formal policy model;

(c) Show via informal demonstration, that the formal top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware;

(d) Show that the formal top-level specification is an accurate description of the implemented security-relevant hardware, software, and firmware; and

(e) Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the formal top-level specification but strictly internal to the security-relevant hardware, software, and firmware.

Supplemental Guidance: Correspondence is an important part of the assurance gained through modeling. It demonstrates that the implementation is an accurate transformation of the model, and that any additional code or implementation details present have no impact on the behaviors or policies being modeled. Formal methods can be used to show that the high-level security properties are satisfied by the formal information system description, and that the formal system description is correctly implemented by a description of some lower level, for example a hardware description. Consistency between the formal top-level specification and the formal policy models is generally not amenable to being fully proven. Therefore, a combination of formal/informal methods may be needed to show such consistency. Consistency between the formal top-level specification and the implementation may require the use of an informal demonstration due to limitations in the applicability of formal methods to prove that the specification accurately reflects the implementation. Hardware, software, and firmware mechanisms strictly internal to security-relevant hardware, software, and firmware

include, for example, mapping registers and direct memory input/output. Related control: SA-5.

(4) *DEVELOPER SECURITY ARCHITECTURE AND DESIGN | INFORMAL CORRESPONDENCE*

The organization requires the developer of the information system, system component, or information system service to:

(a) Produce, as an integral part of the development process, an informal descriptive top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects;

(b) Show via [*Selection: informal demonstration, convincing argument with formal methods as feasible*] that the descriptive top-level specification is consistent with the formal policy model;

(c) Show via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware;

(d) Show that the descriptive top-level specification is an accurate description of the interfaces to security-relevant hardware, software, and firmware; and

(e) Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the descriptive top-level specification but strictly internal to the security-relevant hardware, software, and firmware.

Supplemental Guidance: Correspondence is an important part of the assurance gained through modeling. It demonstrates that the implementation is an accurate transformation of the model, and that any additional code or implementation details present has no impact on the behaviors or policies being modeled. Consistency between the descriptive top-level specification (i.e., high-level/low-level design) and the formal policy model is generally not amenable to being fully proven. Therefore, a combination of formal/informal methods may be needed to show such consistency. Hardware, software, and firmware mechanisms strictly internal to security-relevant hardware, software, and firmware include, for example, mapping registers and direct memory input/output. Related control: SA-5.

(5) *DEVELOPER SECURITY ARCHITECTURE AND DESIGN | CONCEPTUALLY SIMPLE DESIGN*

The organization requires the developer of the information system, system component, or information system service to:

(a) Design and structure the security-relevant hardware, software, and firmware to use a complete, conceptually simple protection mechanism with precisely defined semantics; and

(b) Internally structure the security-relevant hardware, software, and firmware with specific regard for this mechanism.

Supplemental Guidance: Related control: SC-3.

(6) *DEVELOPER SECURITY ARCHITECTURE AND DESIGN | STRUCTURE FOR TESTING*

The organization requires the developer of the information system, system component, or information system service to structure security-relevant hardware, software, and firmware to facilitate testing.

Supplemental Guidance: Related control: SA-11.

(7) *DEVELOPER SECURITY ARCHITECTURE AND DESIGN | STRUCTURE FOR LEAST PRIVILEGE*

The organization requires the developer of the information system, system component, or information system service to structure security-relevant hardware, software, and firmware to facilitate controlling access with least privilege.

Supplemental Guidance: Related controls: AC-5, AC-6.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SA-17

SA-18 TAMPER RESISTANCE AND DETECTION

Control: The organization implements a tamper protection program for the information system, system component, or information system service.

Supplemental Guidance: Anti-tamper technologies and techniques provide a level of protection for critical information systems, system components, and information technology products against a number of related threats including modification, reverse engineering, and substitution. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting information systems, components, and products during distribution and when in use. Related controls: PE-3, SA-12, SI-7.

Control Enhancements:

(1) *TAMPER RESISTANCE AND DETECTION | MULTIPLE PHASES OF SDLC*

The organization employs anti-tamper technologies and techniques during multiple phases in the system development life cycle including design, development, integration, operations, and maintenance.

Supplemental Guidance: Organizations use a combination of hardware and software techniques for tamper resistance and detection. Organizations employ obfuscation and self-checking, for example, to make reverse engineering and modifications more difficult, time-consuming, and expensive for adversaries. Customization of information systems and system components can make substitutions easier to detect and therefore limit damage. Related control: SA-3.

(2) *TAMPER RESISTANCE AND DETECTION | INSPECTION OF INFORMATION SYSTEMS, COMPONENTS, OR DEVICES*

The organization inspects [*Assignment: organization-defined information systems, system components, or devices*] [*Selection (one or more): at random;* at [*Assignment: organization-defined frequency*], *upon* [*Assignment: organization-defined indications of need for inspection*]] to detect tampering.

Supplemental Guidance: This control enhancement addresses both physical and logical tampering and is typically applied to mobile devices, notebook computers, or other system components taken out of organization-controlled areas. Indications of need for inspection include, for example, when individuals return from travel to high-risk locations. Related control: SI-4.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SA-19 COMPONENT AUTHENTICITY

Control: The organization:

a. Develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the information system; and

b. Reports counterfeit information system components to [*Selection (one or more): source of counterfeit component;* [*Assignment: organization-defined external reporting organizations*]*;* [*Assignment: organization-defined personnel or roles*]].

Supplemental Guidance: Sources of counterfeit components include, for example, manufacturers, developers, vendors, and contractors. Anti-counterfeiting policy and procedures support tamper resistance and provide a level of protection against the introduction of malicious code. External reporting organizations include, for example, US-CERT. Related controls: PE-3, SA-12, SI-7.

Control Enhancements:

(1) *COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT TRAINING*

The organization trains [*Assignment: organization-defined personnel or roles*] to detect counterfeit information system components (including hardware, software, and firmware).

(2) *COMPONENT AUTHENTICITY | CONFIGURATION CONTROL FOR COMPONENT SERVICE / REPAIR*

The organization maintains configuration control over [*Assignment: organization-defined information system components*] awaiting service/repair and serviced/repaired components awaiting return to service.

(3) *COMPONENT AUTHENTICITY | COMPONENT DISPOSAL*

The organization disposes of information system components using [*Assignment: organization-defined techniques and methods*].

Supplemental Guidance: Proper disposal of information system components helps to prevent such components from entering the gray market.

(4) *COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT SCANNING*

The organization scans for counterfeit information system components [*Assignment: organization-defined frequency*].

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SA-20 CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS

Control: The organization re-implements or custom develops [*Assignment: organization-defined critical information system components*].

Supplemental Guidance: Organizations determine that certain information system components likely cannot be trusted due to specific threats to and vulnerabilities in those components, and for which there are no viable security controls to adequately mitigate the resulting risk. Re-implementation or custom development of such components helps to satisfy requirements for higher assurance. This is accomplished by initiating changes to system components (including hardware, software, and firmware) such that the standard attacks by adversaries are less likely to succeed. In situations where no alternative sourcing is available and organizations choose not to re-implement or custom develop critical information system components, additional safeguards can be employed (e.g., enhanced auditing, restrictions on source code and system utility access, and protection from deletion of system and application files. Related controls: CP-2, SA-8, SA-14.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SA-21 DEVELOPER SCREENING

Control: The organization requires that the developer of [*Assignment: organization-defined information system, system component, or information system service*]:

a. Have appropriate access authorizations as determined by assigned [*Assignment: organization-defined official government duties*]; and

b. Satisfy [*Assignment: organization-defined additional personnel screening criteria*].

Supplemental Guidance: Because the information system, system component, or information system service may be employed in critical activities essential to the national and/or economic security interests of the United States, organizations have a strong interest in ensuring that the developer is trustworthy. The degree of trust required of the developer may need to be consistent with that of

the individuals accessing the information system/component/service once deployed. Examples of authorization and personnel screening criteria include clearance, satisfactory background checks, citizenship, and nationality. Trustworthiness of developers may also include a review and analysis of company ownership and any relationships the company has with entities potentially affecting the quality/reliability of the systems, components, or services being developed. Related controls: PS-3, PS-7.

Control Enhancements:

(1) *DEVELOPER SCREENING | VALIDATION OF SCREENING*

The organization requires the developer of the information system, system component, or information system service take [*Assignment: organization-defined actions*] to ensure that the required access authorizations and screening criteria are satisfied.

Supplemental Guidance: Satisfying required access authorizations and personnel screening criteria includes, for example, providing a listing of all the individuals authorized to perform development activities on the selected information system, system component, or information system service so that organizations can validate that the developer has satisfied the necessary authorization and screening requirements.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SA-22 UNSUPPORTED SYSTEM COMPONENTS

Control: The organization:

a. Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and

b. Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.

Supplemental Guidance: Support for information system components includes, for example, software patches, firmware updates, replacement parts, and maintenance contracts. Unsupported components (e.g., when vendors are no longer providing critical software patches), provide a substantial opportunity for adversaries to exploit new weaknesses discovered in the currently installed components. Exceptions to replacing unsupported system components may include, for example, systems that provide critical mission/business capability where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option. Related controls: PL-2, SA-3.

Control Enhancements:

(1) *UNSUPPORTED SYSTEM COMPONENTS | ALTERNATIVE SOURCES FOR CONTINUED SUPPORT*

The organization provides [*Selection (one or more): in-house support;* [*Assignment: organization-defined support from external providers*]] for unsupported information system components.

Supplemental Guidance: This control enhancement addresses the need to provide continued support for selected information system components that are no longer supported by the original developers, vendors, or manufacturers when such components remain essential to mission/business operations. Organizations can establish in-house support, for example, by developing customized patches for critical software components or secure the services of external providers who through contractual relationships, provide ongoing support for the designated unsupported components. Such contractual relationships can include, for example, Open Source Software value-added vendors.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SYSTEM AND SERVICES ACQUISITION CONTROLS

DEVELOPMENT OF SYSTEMS, COMPONENTS, AND SERVICES

With the renewed emphasis on trustworthy information systems and supply chain security, it is essential that organizations have the capability to express their information security requirements with clarity and specificity in order to engage the information technology industry and obtain the systems, components, and services necessary for mission and business success. To ensure that organizations have such capability, this publication provides a set of security controls in the System and Services Acquisition family (i.e., SA family) addressing requirements for the development of information systems, information technology products, and information system services. Therefore, many of the controls in the SA family are directed at developers of those systems, components, and services. It is important for organizations to recognize that the scope of the security controls in the SA family includes all system/component/service development and the developers associated with such development whether the development is conducted by internal organizational personnel or by external developers through the contracting/acquisition process. Affected controls include SA-8, SA-10, SA-11, SA-15, SA-16, SA-17, SA-20, and SA-21.

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

   1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and

b. Reviews and updates the current:

   1. System and communications protection policy [*Assignment: organization-defined frequency*]; and

   2. System and communications protection procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** SC-1	**MOD** SC-1	**HIGH** SC-1

SC-2 APPLICATION PARTITIONING

Control: The information system separates user functionality (including user interface services) from information system management functionality.

Supplemental Guidance: Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical. Organizations implement separation of system management-related functionality from user functionality by using different computers, different central processing units, different instances of operating systems, different network addresses, virtualization techniques, or combinations of these or other methods, as appropriate. This type of separation includes, for example, web administrative interfaces that use separate authentication methods for users of any other information system resources. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls. Related controls: SA-4, SA-8, SC-3.

Control Enhancements:

(1) *APPLICATION PARTITIONING | INTERFACES FOR NON-PRIVILEGED USERS*

The information system prevents the presentation of information system management-related functionality at an interface for non-privileged users.

Supplemental Guidance: This control enhancement ensures that administration options (e.g., administrator privileges) are not available to general users (including prohibiting the use of the grey-out option commonly used to eliminate accessibility to such information). Such restrictions include, for example, not presenting administration options until users establish sessions with administrator privileges. Related control: AC-3.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-2	**HIGH** SC-2

SC-3 SECURITY FUNCTION ISOLATION

Control: The information system isolates security functions from nonsecurity functions.

Supplemental Guidance: The information system isolates security functions from nonsecurity functions by means of an isolation boundary (implemented via partitions and domains). Such isolation controls access to and protects the integrity of the hardware, software, and firmware that perform those security functions. Information systems implement code separation (i.e., separation of security functions from nonsecurity functions) in a number of ways, including, for example, through the provision of security kernels via processor rings or processor modes. For non-kernel code, security function isolation is often achieved through file system protections that serve to protect the code on disk, and address space protections that protect executing code. Information systems restrict access to security functions through the use of access control mechanisms and by implementing least privilege capabilities. While the ideal is for all of the code within the security function isolation boundary to only contain security-relevant code, it is sometimes necessary to include nonsecurity functions within the isolation boundary as an exception. Related controls: AC-3, AC-6, SA-4, SA-5, SA-8, SA-13, SC-2, SC-7, SC-39.

Control Enhancements:

(1) *SECURITY FUNCTION ISOLATION | HARDWARE SEPARATION*

The information system utilizes underlying hardware separation mechanisms to implement security function isolation.

Supplemental Guidance: Underlying hardware separation mechanisms include, for example, hardware ring architectures, commonly implemented within microprocessors, and hardware-enforced address segmentation used to support logically distinct storage objects with separate attributes (i.e., readable, writeable).

(2) *SECURITY FUNCTION ISOLATION | ACCESS / FLOW CONTROL FUNCTIONS*

The information system isolates security functions enforcing access and information flow control from nonsecurity functions and from other security functions.

Supplemental Guidance: Security function isolation occurs as a result of implementation; the functions can still be scanned and monitored. Security functions that are potentially isolated from access and flow control enforcement functions include, for example, auditing, intrusion detection, and anti-virus functions.

(3) *SECURITY FUNCTION ISOLATION | MINIMIZE NONSECURITY FUNCTIONALITY*

The organization minimizes the number of nonsecurity functions included within the isolation boundary containing security functions.

Supplemental Guidance: In those instances where it is not feasible to achieve strict isolation of nonsecurity functions from security functions, it is necessary to take actions to minimize the nonsecurity-relevant functions within the security function boundary. Nonsecurity functions

contained within the isolation boundary are considered security-relevant because errors or maliciousness in such software, by virtue of being within the boundary, can impact the security functions of organizational information systems. The design objective is that the specific portions of information systems providing information security are of minimal size/complexity. Minimizing the number of nonsecurity functions in the security-relevant components of information systems allows designers and implementers to focus only on those functions which are necessary to provide the desired security capability (typically access enforcement). By minimizing nonsecurity functions within the isolation boundaries, the amount of code that must be trusted to enforce security policies is reduced, thus contributing to understandability.

(4) *SECURITY FUNCTION ISOLATION | MODULE COUPLING AND COHESIVENESS*

The organization implements security functions as largely independent modules that maximize internal cohesiveness within modules and minimize coupling between modules.

Supplemental Guidance: The reduction in inter-module interactions helps to constrain security functions and to manage complexity. The concepts of coupling and cohesion are important with respect to modularity in software design. Coupling refers to the dependencies that one module has on other modules. Cohesion refers to the relationship between the different functions within a particular module. Good software engineering practices rely on modular decomposition, layering, and minimization to reduce and manage complexity, thus producing software modules that are highly cohesive and loosely coupled.

(5) *SECURITY FUNCTION ISOLATION | LAYERED STRUCTURES*

The organization implements security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

Supplemental Guidance: The implementation of layered structures with minimized interactions among security functions and non-looping layers (i.e., lower-layer functions do not depend on higher-layer functions) further enables the isolation of security functions and management of complexity.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SC-3

SC-4 INFORMATION IN SHARED RESOURCES

Control: The information system prevents unauthorized and unintended information transfer via shared system resources.

Supplemental Guidance: This control prevents information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection. This control does not address: (i) information remanence which refers to residual representation of data that has been nominally erased or removed; (ii) covert channels (including storage and/or timing channels) where shared resources are manipulated to violate information flow restrictions; or (iii) components within information systems for which there are only single users/roles. Related controls: AC-3, AC-4, MP-6.

Control Enhancements:

(1) *INFORMATION IN SHARED RESOURCES | SECURITY LEVELS*

[Withdrawn: Incorporated into SC-4].

(2) *INFORMATION IN SHARED RESOURCES | PERIODS PROCESSING*

The information system prevents unauthorized information transfer via shared resources in accordance with [*Assignment: organization-defined procedures*] when system processing explicitly switches between different information classification levels or security categories.

Supplemental Guidance: This control enhancement applies when there are explicit changes in information processing levels during information system operations, for example, during multilevel processing and periods processing with information at different classification levels or security categories. Organization-defined procedures may include, for example, approved sanitization processes for electronically stored information.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-4	**HIGH** SC-4

SC-5 DENIAL OF SERVICE PROTECTION

Control: The information system protects against or limits the effects of the following types of denial of service attacks: [*Assignment: organization-defined types of denial of service attacks or reference to source for such information*] by employing [*Assignment: organization-defined security safeguards*].

Supplemental Guidance: A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect information system components on internal organizational networks from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may also reduce the susceptibility to denial of service attacks. Related controls: SC-6, SC-7.

Control Enhancements:

(1) *DENIAL OF SERVICE PROTECTION | RESTRICT INTERNAL USERS*

The information system restricts the ability of individuals to launch [*Assignment: organization-defined denial of service attacks*] against other information systems.

Supplemental Guidance: Restricting the ability of individuals to launch denial of service attacks requires that the mechanisms used for such attacks are unavailable. Individuals of concern can include, for example, hostile insiders or external adversaries that have successfully breached the information system and are using the system as a platform to launch cyber attacks on third parties. Organizations can restrict the ability of individuals to connect and transmit arbitrary information on the transport medium (i.e., network, wireless spectrum). Organizations can also limit the ability of individuals to use excessive information system resources. Protection against individuals having the ability to launch denial of service attacks may be implemented on specific information systems or on boundary devices prohibiting egress to potential target systems.

(2) *DENIAL OF SERVICE PROTECTION | EXCESS CAPACITY / BANDWIDTH / REDUNDANCY*

The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding denial of service attacks.

Supplemental Guidance: Managing excess capacity ensures that sufficient capacity is available to counter flooding attacks. Managing excess capacity may include, for example, establishing selected usage priorities, quotas, or partitioning.

(3) *DENIAL OF SERVICE PROTECTION | DETECTION / MONITORING*

The organization:

(a) Employs [*Assignment: organization-defined monitoring tools*] to detect indicators of denial of service attacks against the information system; and

(b) Monitors [*Assignment: organization-defined information system resources*] to determine if sufficient resources exist to prevent effective denial of service attacks.

Supplemental Guidance: Organizations consider utilization and capacity of information system resources when managing risk from denial of service due to malicious attacks. Denial of service attacks can originate from external or internal sources. Information system resources sensitive to denial of service include, for example, physical disk storage, memory, and CPU cycles. Common safeguards to prevent denial of service attacks related to storage utilization and capacity include, for example, instituting disk quotas, configuring information systems to automatically alert administrators when specific storage capacity thresholds are reached, using file compression technologies to maximize available storage space, and imposing separate partitions for system and user data. Related controls: CA-7, SI-4.

References: None.

Priority and Baseline Allocation:

P1	**LOW** SC-5	**MOD** SC-5	**HIGH** SC-5

SC-6 RESOURCE AVAILABILITY

Control: The information system protects the availability of resources by allocating [*Assignment: organization-defined resources*] by [*Selection (one or more); priority; quota;* [*Assignment: organization-defined security safeguards*]].

Supplemental Guidance: Priority protection helps prevent lower-priority processes from delaying or interfering with the information system servicing any higher-priority processes. Quotas prevent users or processes from obtaining more than predetermined amounts of resources. This control does not apply to information system components for which there are only single users/roles.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-7 BOUNDARY PROTECTION

Control: The information system:

a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;

b. Implements subnetworks for publicly accessible system components that are [*Selection: physically; logically*] separated from internal organizational networks; and

c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Supplemental Guidance: Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational information systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external

traffic that appears to be spoofing internal addresses. Organizations consider the shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions. Related controls: AC-4, AC-17, CA-3, CM-7, CP-8, IR-4, RA-3, SC-5, SC-13.

Control Enhancements:

(1) *BOUNDARY PROTECTION | PHYSICALLY SEPARATED SUBNETWORKS*

[Withdrawn: Incorporated into SC-7].

(2) *BOUNDARY PROTECTION | PUBLIC ACCESS*

[Withdrawn: Incorporated into SC-7].

(3) *BOUNDARY PROTECTION | ACCESS POINTS*

The organization limits the number of external network connections to the information system.

Supplemental Guidance: Limiting the number of external network connections facilitates more comprehensive monitoring of inbound and outbound communications traffic. The Trusted Internet Connection (TIC) initiative is an example of limiting the number of external network connections.

(4) *BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES*

The organization:

(a) Implements a managed interface for each external telecommunication service;

(b) Establishes a traffic flow policy for each managed interface;

(c) Protects the confidentiality and integrity of the information being transmitted across each interface;

(d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and

(e) Reviews exceptions to the traffic flow policy [*Assignment: organization-defined frequency*] and removes exceptions that are no longer supported by an explicit mission/business need.

Supplemental Guidance: Related control: SC-8.

(5) *BOUNDARY PROTECTION | DENY BY DEFAULT / ALLOW BY EXCEPTION*

The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).

Supplemental Guidance: This control enhancement applies to both inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.

(6) *BOUNDARY PROTECTION | RESPONSE TO RECOGNIZED FAILURES*

[Withdrawn: Incorporated into SC-7 (18)].

(7) *BOUNDARY PROTECTION | PREVENT SPLIT TUNNELING FOR REMOTE DEVICES*

The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

Supplemental Guidance: This control enhancement is implemented within remote devices (e.g., notebook computers) through configuration settings to disable split tunneling in those devices, and by preventing those configuration settings from being readily configurable by users. This control enhancement is implemented within the information system by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling. Split tunneling might be desirable by remote users to communicate with local information system resources such as printers/file servers. However, split tunneling would in effect allow unauthorized external connections, making the system more vulnerable to attack and to exfiltration of organizational

information. The use of VPNs for remote connections, when adequately provisioned with appropriate security controls, may provide the organization with sufficient assurance that it can effectively treat such connections as non-remote connections from the confidentiality and integrity perspective. VPNs thus provide a means for allowing non-remote communications paths from remote devices. The use of an adequately provisioned VPN does not eliminate the need for preventing split tunneling.

(8) *BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS*

The information system routes [*Assignment: organization-defined internal communications traffic*] to [*Assignment: organization-defined external networks*] through authenticated proxy servers at managed interfaces.

Supplemental Guidance: External networks are networks outside of organizational control. A proxy server is a server (i.e., information system or application) that acts as an intermediary for clients requesting information system resources (e.g., files, connections, web pages, or services) from other organizational servers. Client requests established through an initial connection to the proxy server are evaluated to manage complexity and to provide additional protection by limiting direct connectivity. Web content filtering devices are one of the most common proxy servers providing access to the Internet. Proxy servers support logging individual Transmission Control Protocol (TCP) sessions and blocking specific Uniform Resource Locators (URLs), domain names, and Internet Protocol (IP) addresses. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites. Related controls: AC-3, AU-2.

(9) *BOUNDARY PROTECTION | RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC*

The information system:

(a) Detects and denies outgoing communications traffic posing a threat to external information systems; and

(b) Audits the identity of internal users associated with denied communications.

Supplemental Guidance: Detecting outgoing communications traffic from internal actions that may pose threats to external information systems is sometimes termed extrusion detection. Extrusion detection at information system boundaries as part of managed interfaces includes the analysis of incoming and outgoing communications traffic searching for indications of internal threats to the security of external systems. Such threats include, for example, traffic indicative of denial of service attacks and traffic containing malicious code. Related controls: AU-2, AU-6, SC-38, SC-44, SI-3, SI-4.

(10) *BOUNDARY PROTECTION | PREVENT UNAUTHORIZED EXFILTRATION*

The organization prevents the unauthorized exfiltration of information across managed interfaces.

Supplemental Guidance: Safeguards implemented by organizations to prevent unauthorized exfiltration of information from information systems include, for example: (i) strict adherence to protocol formats; (ii) monitoring for beaconing from information systems; (iii) monitoring for steganography; (iv) disconnecting external network interfaces except when explicitly needed; (v) disassembling and reassembling packet headers; and (vi) employing traffic profile analysis to detect deviations from the volume/types of traffic expected within organizations or call backs to command and control centers. Devices enforcing strict adherence to protocol formats include, for example, deep packet inspection firewalls and XML gateways. These devices verify adherence to protocol formats and specification at the application layer and serve to identify vulnerabilities that cannot be detected by devices operating at the network or transport layers. This control enhancement is closely associated with cross-domain solutions and system guards enforcing information flow requirements. Related control: SI-3.

(11) *BOUNDARY PROTECTION | RESTRICT INCOMING COMMUNICATIONS TRAFFIC*

The information system only allows incoming communications from [*Assignment: organization-defined authorized sources*] routed to [*Assignment: organization-defined authorized destinations*].

Supplemental Guidance: This control enhancement provides determinations that source and destination address pairs represent authorized/allowed communications. Such determinations can be based on several factors including, for example, the presence of source/destination

address pairs in lists of authorized/allowed communications, the absence of address pairs in lists of unauthorized/disallowed pairs, or meeting more general rules for authorized/allowed source/destination pairs. Related control: AC-3.

(12) *BOUNDARY PROTECTION | HOST-BASED PROTECTION*

The organization implements [*Assignment: organization-defined host-based boundary protection mechanisms*] at [*Assignment: organization-defined information system components*].

Supplemental Guidance: Host-based boundary protection mechanisms include, for example, host-based firewalls. Information system components employing host-based boundary protection mechanisms include, for example, servers, workstations, and mobile devices.

(13) *BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS / MECHANISMS / SUPPORT COMPONENTS*

The organization isolates [*Assignment: organization-defined information security tools, mechanisms, and support components*] from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

Supplemental Guidance: Physically separate subnetworks with managed interfaces are useful, for example, in isolating computer network defenses from critical operational processing networks to prevent adversaries from discovering the analysis and forensics techniques of organizations. Related controls: SA-8, SC-2, SC-3.

(14) *BOUNDARY PROTECTION | PROTECTS AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS*

The organization protects against unauthorized physical connections at [*Assignment: organization-defined managed interfaces*].

Supplemental Guidance: Information systems operating at different security categories or classification levels may share common physical and environmental controls, since the systems may share space within organizational facilities. In practice, it is possible that these separate information systems may share common equipment rooms, wiring closets, and cable distribution paths. Protection against unauthorized physical connections can be achieved, for example, by employing clearly identified and physically separated cable trays, connection frames, and patch panels for each side of managed interfaces with physical access controls enforcing limited authorized access to these items. Related controls: PE-4, PE-19.

(15) *BOUNDARY PROTECTION | ROUTE PRIVILEGED NETWORK ACCESSES*

The information system routes all networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.

Supplemental Guidance: Related controls: AC-2, AC-3, AU-2, SI-4.

(16) *BOUNDARY PROTECTION | PREVENT DISCOVERY OF COMPONENTS / DEVICES*

The information system prevents discovery of specific system components composing a managed interface.

Supplemental Guidance: This control enhancement protects network addresses of information system components that are part of managed interfaces from discovery through common tools and techniques used to identify devices on networks. Network addresses are not available for discovery (e.g., network address not published or entered in domain name systems), requiring prior knowledge for access. Another obfuscation technique is to periodically change network addresses.

(17) *BOUNDARY PROTECTION | AUTOMATED ENFORCEMENT OF PROTOCOL FORMATS*

The information system enforces adherence to protocol formats.

Supplemental Guidance: Information system components that enforce protocol formats include, for example, deep packet inspection firewalls and XML gateways. Such system components verify adherence to protocol formats/specifications (e.g., IEEE) at the application layer and identify significant vulnerabilities that cannot be detected by devices operating at the network or transport layers. Related control: SC-4.

(18) *BOUNDARY PROTECTION | FAIL SECURE*

The information system fails securely in the event of an operational failure of a boundary protection device.

Supplemental Guidance: Fail secure is a condition achieved by employing information system mechanisms to ensure that in the event of operational failures of boundary protection devices at managed interfaces (e.g., routers, firewalls, guards, and application gateways residing on protected subnetworks commonly referred to as demilitarized zones), information systems do not enter into unsecure states where intended security properties no longer hold. Failures of boundary protection devices cannot lead to, or cause information external to the devices to enter the devices, nor can failures permit unauthorized information releases. Related controls: CP-2, SC-24.

(19) *BOUNDARY PROTECTION | BLOCKS COMMUNICATION FROM NON-ORGANIZATIONALLY CONFIGURED HOSTS*

The information system blocks both inbound and outbound communications traffic between [*Assignment: organization-defined communication clients*] that are independently configured by end users and external service providers.

Supplemental Guidance: Communication clients independently configured by end users and external service providers include, for example, instant messaging clients. Traffic blocking does not apply to communication clients that are configured by organizations to perform authorized functions.

(20) *BOUNDARY PROTECTION | DYNAMIC ISOLATION / SEGREGATION*

The information system provides the capability to dynamically isolate/segregate [*Assignment: organization-defined information system components*] from other components of the system.

Supplemental Guidance: The capability to dynamically isolate or segregate certain internal components of organizational information systems is useful when it is necessary to partition or separate certain components of dubious origin from those components possessing greater trustworthiness. Component isolation reduces the attack surface of organizational information systems. Isolation of selected information system components is also a means of limiting the damage from successful cyber attacks when those attacks occur.

(21) *BOUNDARY PROTECTION | ISOLATION OF INFORMATION SYSTEM COMPONENTS*

The organization employs boundary protection mechanisms to separate [*Assignment: organization-defined information system components*] supporting [*Assignment: organization-defined missions and/or business functions*].

Supplemental Guidance: Organizations can isolate information system components performing different missions and/or business functions. Such isolation limits unauthorized information flows among system components and also provides the opportunity to deploy greater levels of protection for selected components. Separating system components with boundary protection mechanisms provides the capability for increased protection of individual components and to more effectively control information flows between those components. This type of enhanced protection limits the potential harm from cyber attacks and errors. The degree of separation provided varies depending upon the mechanisms chosen. Boundary protection mechanisms include, for example, routers, gateways, and firewalls separating system components into physically separate networks or subnetworks, cross-domain devices separating subnetworks, virtualization techniques, and encrypting information flows among system components using distinct encryption keys. Related controls: CA-9, SC-3.

(22) *BOUNDARY PROTECTION | SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS*

The information system implements separate network addresses (i.e., different subnets) to connect to systems in different security domains.

Supplemental Guidance: Decomposition of information systems into subnets helps to provide the appropriate level of protection for network connections to different security domains containing information with different security categories or classification levels.

(23) *BOUNDARY PROTECTION | DISABLE SENDER FEEDBACK ON PROTOCOL VALIDATION FAILURE*

The information system disables feedback to senders on protocol format validation failure.

Supplemental Guidance: Disabling feedback to senders when there is a failure in protocol validation format prevents adversaries from obtaining information which would otherwise be unavailable.

References: FIPS Publication 199; NIST Special Publications 800-41, 800-77.

Priority and Baseline Allocation:

P1	**LOW** SC-7	**MOD** SC-7 (3) (4) (5) (7)	**HIGH** SC-7 (3) (4) (5) (7) (8) (18) (21)

SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

Control: The information system protects the [*Selection (one or more): confidentiality; integrity*] of transmitted information.

Supplemental Guidance: This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and/or integrity of organizational information can be accomplished by physical means (e.g., by employing protected distribution systems) or by logical means (e.g., employing encryption techniques). Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality/integrity. In such situations, organizations determine what types of confidentiality/integrity services are available in standard, commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, organizations implement appropriate compensating security controls or explicitly accept the additional risk. Related controls: AC-17, PE-4.

Control Enhancements:

(1) *TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION*

The information system implements cryptographic mechanisms to [*Selection (one or more): prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*Assignment: organization-defined alternative physical safeguards*].

Supplemental Guidance: Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes. Alternative physical security safeguards include, for example, protected distribution systems. Related control: SC-13.

(2) *TRANSMISSION CONFIDENTIALITY AND INTEGRITY | PRE / POST TRANSMISSION HANDLING*

The information system maintains the [*Selection (one or more): confidentiality; integrity*] of information during preparation for transmission and during reception.

Supplemental Guidance: Information can be either unintentionally or maliciously disclosed or modified during preparation for transmission or during reception including, for example, during aggregation, at protocol transformation points, and during packing/unpacking. These unauthorized disclosures or modifications compromise the confidentiality or integrity of the information. Related control: AU-10.

(3) *TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC PROTECTION FOR MESSAGE EXTERNALS*

The information system implements cryptographic mechanisms to protect message externals unless otherwise protected by [*Assignment: organization-defined alternative physical safeguards*].

Supplemental Guidance: This control enhancement addresses protection against unauthorized disclosure of information. Message externals include, for example, message headers/routing information. This control enhancement prevents the exploitation of message externals and applies to both internal and external networks or links that may be visible to individuals who are not authorized users. Header/routing information is sometimes transmitted unencrypted because the information is not properly identified by organizations as having significant value

or because encrypting the information can result in lower network performance and/or higher costs. Alternative physical safeguards include, for example, protected distribution systems. Related controls: SC-12, SC-13.

(4) *TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CONCEAL / RANDOMIZE COMMUNICATIONS*

The information system implements cryptographic mechanisms to conceal or randomize communication patterns unless otherwise protected by [*Assignment: organization-defined alternative physical safeguards*].

Supplemental Guidance: This control enhancement addresses protection against unauthorized disclosure of information. Communication patterns include, for example, frequency, periods, amount, and predictability. Changes to communications patterns can reveal information having intelligence value especially when combined with other available information related to missions/business functions supported by organizational information systems. This control enhancement prevents the derivation of intelligence based on communications patterns and applies to both internal and external networks or links that may be visible to individuals who are not authorized users. Encrypting the links and transmitting in continuous, fixed/random patterns prevents the derivation of intelligence from the system communications patterns. Alternative physical safeguards include, for example, protected distribution systems. Related controls: SC-12, SC-13.

References: FIPS Publications 140-2, 197; NIST Special Publications 800-52, 800-77, 800-81, 800-113; CNSS Policy 15; NSTISSI No. 7003.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-8 (1)	**HIGH** SC-8 (1)

SC-9 TRANSMISSION CONFIDENTIALITY

[Withdrawn: Incorporated into SC-8].

SC-10 NETWORK DISCONNECT

Control: The information system terminates the network connection associated with a communications session at the end of the session or after [*Assignment: organization-defined time period*] of inactivity.

Supplemental Guidance: This control applies to both internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. Time periods of inactivity may be established by organizations and include, for example, time periods by type of network access or for specific network accesses.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** SC-10	**HIGH** SC-10

SC-11 TRUSTED PATH

Control: The information system establishes a trusted communications path between the user and the following security functions of the system: [*Assignment: organization-defined security functions to include at a minimum, information system authentication and re-authentication*].

Supplemental Guidance: Trusted paths are mechanisms by which users (through input devices) can communicate directly with security functions of information systems with the requisite assurance to support information security policies. The mechanisms can be activated only by users or the security functions of organizational information systems. User responses via trusted paths are protected from modifications by or disclosure to untrusted applications. Organizations employ trusted paths for high-assurance connections between security functions of information systems and users (e.g., during system logons). Enforcement of trusted communications paths is typically provided via an implementation that meets the reference monitor concept. Related controls: AC-16, AC-25.

Control Enhancements:

(1) *TRUSTED PATH | LOGICAL ISOLATION*

The information system provides a trusted communications path that is logically isolated and distinguishable from other paths.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Control: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction*].

Supplemental Guidance: Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance, specifying appropriate options, levels, and parameters. Organizations manage trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to organizational information systems and certificates related to the internal operations of systems. Related controls: SC-13, SC-17.

Control Enhancements:

(1) *CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY*

The organization maintains availability of information in the event of the loss of cryptographic keys by users.

Supplemental Guidance: Escrowing of encryption keys is a common practice for ensuring availability in the event of loss of keys (e.g., due to forgotten passphrase).

(2) *CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | SYMMETRIC KEYS*

The organization produces, controls, and distributes symmetric cryptographic keys using [*Selection: NIST FIPS-compliant; NSA-approved*] key management technology and processes.

(3) *CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | ASYMMETRIC KEYS*

The organization produces, controls, and distributes asymmetric cryptographic keys using [*Selection: NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key*].

(4) *CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES*
[Withdrawn: Incorporated into SC-12].

(5) *CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES / HARDWARE TOKENS*
[Withdrawn: Incorporated into SC-12].

References: NIST Special Publications 800-56, 800-57.

Priority and Baseline Allocation:

P1	**LOW** SC-12	**MOD** SC-12	**HIGH** SC-12 (1)

SC-13 CRYPTOGRAPHIC PROTECTION

Control: The information system implements [*Assignment: organization-defined cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Supplemental Guidance: Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography). Related controls: AC-2, AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7.

Control Enhancements: None.

(1) *CRYPTOGRAPHIC PROTECTION | FIPS-VALIDATED CRYPTOGRAPHY*
[Withdrawn: Incorporated into SC-13].

(2) *CRYPTOGRAPHIC PROTECTION | NSA-APPROVED CRYPTOGRAPHY*
[Withdrawn: Incorporated into SC-13].

(3) *CRYPTOGRAPHIC PROTECTION | INDIVIDUALS WITHOUT FORMAL ACCESS APPROVALS*
[Withdrawn: Incorporated into SC-13].

(4) *CRYPTOGRAPHIC PROTECTION | DIGITAL SIGNATURES*
[Withdrawn: Incorporated into SC-13].

References: FIPS Publication 140; Web: http://csrc.nist.gov/cryptval, http://www.cnss.gov.

Priority and Baseline Allocation:

P1	**LOW** SC-13	**MOD** SC-13	**HIGH** SC-13

SC-14 PUBLIC ACCESS PROTECTIONS

[Withdrawn: Capability provided by AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, SI-7, SI-10].

SC-15 COLLABORATIVE COMPUTING DEVICES

Control: The information system:

a. Prohibits remote activation of collaborative computing devices with the following exceptions: [*Assignment: organization-defined exceptions where remote activation is to be allowed*]; and

b. Provides an explicit indication of use to users physically present at the devices.

Supplemental Guidance: Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated. Related control: AC-21.

Control Enhancements:

(1) *COLLABORATIVE COMPUTING DEVICES | PHYSICAL DISCONNECT*

The information system provides physical disconnect of collaborative computing devices in a manner that supports ease of use.

Supplemental Guidance: Failing to physically disconnect from collaborative computing devices can result in subsequent compromises of organizational information. Providing easy methods to physically disconnect from such devices after a collaborative computing session helps to ensure that participants actually carry out the disconnect activity without having to go through complex and tedious procedures.

(2) *COLLABORATIVE COMPUTING DEVICES | BLOCKING INBOUND / OUTBOUND COMMUNICATIONS TRAFFIC*

[Withdrawn: Incorporated into SC-7].

(3) *COLLABORATIVE COMPUTING DEVICES | DISABLING / REMOVAL IN SECURE WORK AREAS*

The organization disables or removes collaborative computing devices from [*Assignment: organization-defined information systems or information system components*] in [*Assignment: organization-defined secure work areas*].

Supplemental Guidance: Failing to disable or remove collaborative computing devices from information systems or information system components can result in subsequent compromises of organizational information including, for example, eavesdropping on conversations.

(4) *COLLABORATIVE COMPUTING DEVICES | EXPLICITLY INDICATE CURRENT PARTICIPANTS*

The information system provides an explicit indication of current participants in [*Assignment: organization-defined online meetings and teleconferences*].

Supplemental Guidance: This control enhancement helps to prevent unauthorized individuals from participating in collaborative computing sessions without the explicit knowledge of other participants.

References: None.

Priority and Baseline Allocation:

P1	**LOW** SC-15	**MOD** SC-15	**HIGH** SC-15

SC-16 TRANSMISSION OF SECURITY ATTRIBUTES

Control: The information system associates [*Assignment: organization-defined security attributes*] with information exchanged between information systems and between system components.

Supplemental Guidance: Security attributes can be explicitly or implicitly associated with the information contained in organizational information systems or system components. Related controls: AC-3, AC-4, AC-16.

Control Enhancements:

(1) *TRANSMISSION OF SECURITY ATTRIBUTES | INTEGRITY VALIDATION*

The information system validates the integrity of transmitted security attributes.

Supplemental Guidance: This control enhancement ensures that the verification of the integrity of transmitted information includes security attributes. Related controls: AU-10, SC-8.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Control: The organization issues public key certificates under an [*Assignment: organization-defined certificate policy*] or obtains public key certificates from an approved service provider.

Supplemental Guidance: For all certificates, organizations manage information system trust stores to ensure only approved trust anchors are in the trust stores. This control addresses both certificates with visibility external to organizational information systems and certificates related to the internal operations of systems, for example, application-specific time services. Related control: SC-12.

Control Enhancements: None.

References: OMB Memorandum 05-24; NIST Special Publications 800-32, 800-63.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-17	**HIGH** SC-17

SC-18 MOBILE CODE

Control: The organization:

a. Defines acceptable and unacceptable mobile code and mobile code technologies;

b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and

c. Authorizes, monitors, and controls the use of mobile code within the information system.

Supplemental Guidance: Decisions regarding the employment of mobile code within organizational information systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices (e.g., smart phones). Mobile code policy and procedures address preventing the development, acquisition, or introduction of unacceptable mobile code within organizational information systems. Related controls: AU-2, AU-12, CM-2, CM-6, SI-3.

Control Enhancements:

(1) *MOBILE CODE | IDENTIFY UNACCEPTABLE CODE / TAKE CORRECTIVE ACTIONS*

The information system identifies [*Assignment: organization-defined unacceptable mobile code*] and takes [*Assignment: organization-defined corrective actions*].

Supplemental Guidance: Corrective actions when unacceptable mobile code is detected include, for example, blocking, quarantine, or alerting administrators. Blocking includes, for example, preventing transmission of word processing files with embedded macros when such macros have been defined to be unacceptable mobile code.

(2) *MOBILE CODE | ACQUISITION / DEVELOPMENT / USE*

The organization ensures that the acquisition, development, and use of mobile code to be deployed in the information system meets [*Assignment: organization-defined mobile code requirements*].

(3) *MOBILE CODE | PREVENT DOWNLOADING / EXECUTION*

The information system prevents the download and execution of [*Assignment: organization-defined unacceptable mobile code*].

(4) *MOBILE CODE | PREVENT AUTOMATIC EXECUTION*

The information system prevents the automatic execution of mobile code in [*Assignment: organization-defined software applications*] and enforces [*Assignment: organization-defined actions*] prior to executing the code.

Supplemental Guidance: Actions enforced before executing mobile code, include, for example, prompting users prior to opening electronic mail attachments. Preventing automatic execution of mobile code includes, for example, disabling auto execute features on information system components employing portable storage devices such as Compact Disks (CDs), Digital Video Disks (DVDs), and Universal Serial Bus (USB) devices.

(5) *MOBILE CODE | ALLOW EXECUTION ONLY IN CONFINED ENVIRONMENTS*

The organization allows execution of permitted mobile code only in confined virtual machine environments.

References: NIST Special Publication 800-28; DoD Instruction 8552.01.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** SC-18	**HIGH** SC-18

SC-19 VOICE OVER INTERNET PROTOCOL

Control: The organization:

a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and

b. Authorizes, monitors, and controls the use of VoIP within the information system.

Supplemental Guidance: Related controls: CM-6, SC-7, SC-15.

Control Enhancements: None.

References: NIST Special Publication 800-58.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-19	**HIGH** SC-19

SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

Control: The information system:

a. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and

b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

Supplemental Guidance: This control enables external clients including, for example, remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers. Additional artifacts include, for example, DNS Security (DNSSEC) digital signatures and cryptographic keys. DNS resource records are examples of authoritative data. The means to indicate the security status of child zones includes, for example, the use of delegation signer resource records in the DNS. The DNS security controls reflect (and are referenced from) OMB Memorandum 08-23. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data. Related controls: AU-10, SC-8, SC-12, SC-13, SC-21, SC-22.

Control Enhancements:

(1) *SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) | CHILD SUBSPACES*
[Withdrawn: Incorporated into SC-20].

(2) *SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) | DATA ORIGIN / INTEGRITY*
The information system provides data origin and integrity protection artifacts for internal name/address resolution queries.

References: OMB Memorandum 08-23; NIST Special Publication 800-81.

Priority and Baseline Allocation:

P1	**LOW** SC-20	**MOD** SC-20	**HIGH** SC-20

SC-21 SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

Control: The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Supplemental Guidance: Each client of name resolution services either performs this validation on its own, or has authenticated channels to trusted validation providers. Information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching domain name system (DNS) servers. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to enable clients to verify the authenticity and integrity of response data. Related controls: SC-20, SC-22.

Control Enhancements: None.

(1) *SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER) | DATA ORIGIN / INTEGRITY*
[Withdrawn: Incorporated into SC-21].

References: NIST Special Publication 800-81.

Priority and Baseline Allocation:

P1	**LOW** SC-21	**MOD** SC-21	**HIGH** SC-21

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE

Control: The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

Supplemental Guidance: Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers. To eliminate single points of failure and to enhance redundancy, organizations employ at least two authoritative domain name system servers, one configured as the primary server and the other configured as the secondary server. Additionally, organizations typically deploy the servers in two geographically separated network subnetworks (i.e., not located in the same physical facility). For role separation, DNS servers with internal roles only process name and address resolution requests from within organizations (i.e., from internal clients). DNS servers with external roles only process name and address resolution information requests from clients external to organizations (i.e., on external networks including the Internet). Organizations specify clients that can access authoritative DNS servers in particular roles (e.g., by address ranges, explicit lists). Related controls: SC-2, SC-20, SC-21, SC-24.

Control Enhancements: None.

References: NIST Special Publication 800-81.

Priority and Baseline Allocation:

P1	**LOW** SC-22	**MOD** SC-22	**HIGH** SC-22

SC-23 SESSION AUTHENTICITY

Control: The information system protects the authenticity of communications sessions.

Supplemental Guidance: This control addresses communications protection at the session, versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. Authenticity protection includes, for example, protecting against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions. Related controls: SC-8, SC-10, SC-11.

Control Enhancements:

(1) *SESSION AUTHENTICITY | INVALIDATE SESSION IDENTIFIERS AT LOGOUT*

The information system invalidates session identifiers upon user logout or other session termination.

Supplemental Guidance: This control enhancement curtails the ability of adversaries from capturing and continuing to employ previously valid session IDs.

(2) *SESSION AUTHENTICITY | USER-INITIATED LOGOUTS / MESSAGE DISPLAYS*

[Withdrawn: Incorporated into AC-12 (1)].

(3) *SESSION AUTHENTICITY | UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION*

The information system generates a unique session identifier for each session with [*Assignment: organization-defined randomness requirements*] and recognizes only session identifiers that are system-generated.

Supplemental Guidance: This control enhancement curtails the ability of adversaries from reusing previously valid session IDs. Employing the concept of randomness in the generation of unique session identifiers helps to protect against brute-force attacks to determine future session identifiers. Related control: SC-13.

(4) *SESSION AUTHENTICITY | UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION*

[Withdrawn: Incorporated into SC-23 (3)].

(5) *SESSION AUTHENTICITY | ALLOWED CERTIFICATE AUTHORITIES*

The information system only allows the use of [*Assignment: organization-defined certificate authorities*] for verification of the establishment of protected sessions.

Supplemental Guidance: Reliance on certificate authorities (CAs) for the establishment of secure sessions includes, for example, the use of Secure Socket Layer (SSL) and/or Transport Layer Security (TLS) certificates. These certificates, after verification by the respective

certificate authorities, facilitate the establishment of protected sessions between web clients and web servers. Related control: SC-13.

References: NIST Special Publications 800-52, 800-77, 800-95.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-23	**HIGH** SC-23

SC-24 FAIL IN KNOWN STATE

Control: The information system fails to a [*Assignment: organization-defined known-state*] for [*Assignment: organization-defined types of failures*] preserving [*Assignment: organization-defined system state information*] in failure.

Supplemental Guidance: Failure in a known state addresses security concerns in accordance with the mission/business needs of organizations. Failure in a known secure state helps to prevent the loss of confidentiality, integrity, or availability of information in the event of failures of organizational information systems or system components. Failure in a known safe state helps to prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving information system state information facilitates system restart and return to the operational mode of organizations with less disruption of mission/business processes. Related controls: CP-2, CP-10, CP-12, SC-7, SC-22.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SC-24

SC-25 THIN NODES

Control: The organization employs [*Assignment: organization-defined information system components*] with minimal functionality and information storage.

Supplemental Guidance: The deployment of information system components with reduced/minimal functionality (e.g., diskless nodes and thin client technologies) reduces the need to secure every user endpoint, and may reduce the exposure of information, information systems, and services to cyber attacks. Related control: SC-30.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-26 HONEYPOTS

Control: The information system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks.

Supplemental Guidance: A honeypot is set up as a decoy to attract adversaries and to deflect their attacks away from the operational systems supporting organizational missions/business function.

Depending upon the specific usage of the honeypot, consultation with the Office of the General Counsel before deployment may be needed. Related controls: SC-30, SC-44, SI-3, SI-4.

Control Enhancements: None.

(1) *HONEYPOTS | DETECTION OF MALICIOUS CODE*

[Withdrawn: Incorporated into SC-35].

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-27 PLATFORM-INDEPENDENT APPLICATIONS

Control: The information system includes: [*Assignment: organization-defined platform-independent applications*].

Supplemental Guidance: Platforms are combinations of hardware and software used to run software applications. Platforms include: (i) operating systems; (ii) the underlying computer architectures, or (iii) both. Platform-independent applications are applications that run on multiple platforms. Such applications promote portability and reconstitution on different platforms, increasing the availability of critical functions within organizations while information systems with specific operating systems are under attack. Related control: SC-29.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-28 PROTECTION OF INFORMATION AT REST

Control: The information system protects the [*Selection (one or more): confidentiality; integrity*] of [*Assignment: organization-defined information at rest*].

Supplemental Guidance: This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems. System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing Write-Once-Read-Many (WORM) technologies. Organizations may also employ other security controls including, for example, secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved and/or continuous monitoring to identify malicious code at rest. Related controls: AC-3, AC-6, CA-7, CM-3, CM-5, CM-6, PE-3, SC-8, SC-13, SI-3, SI-7.

Control Enhancements:

(1) *PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION*

The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [*Assignment: organization-defined information*] on [*Assignment: organization-defined information system components*].

Supplemental Guidance: Selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of organizational information. The strength of mechanism is commensurate with the security category and/or classification of the information. This control enhancement applies to significant concentrations of digital media in organizational areas designated for media storage and also to limited quantities of media generally associated with information system components in operational environments (e.g., portable storage devices, mobile devices). Organizations have the flexibility to either encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields). Organizations employing cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions. Related controls: AC-19, SC-12.

(2) *PROTECTION OF INFORMATION AT REST | OFF-LINE STORAGE*

The organization removes from online storage and stores off-line in a secure location [*Assignment: organization-defined information*].

Supplemental Guidance: Removing organizational information from online information system storage to off-line storage eliminates the possibility of individuals gaining unauthorized access to the information through a network. Therefore, organizations may choose to move information to off-line storage in lieu of protecting such information in online storage.

References: NIST Special Publications 800-56, 800-57, 800-111.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-28	**HIGH** SC-28

SC-29 HETEROGENEITY

Control: The organization employs a diverse set of information technologies for [*Assignment: organization-defined information system components*] in the implementation of the information system.

Supplemental Guidance: Increasing the diversity of information technologies within organizational information systems reduces the impact of potential exploitations of specific technologies and also defends against common mode failures, including those failures induced by supply chain attacks. Diversity in information technologies also reduces the likelihood that the means adversaries use to compromise one information system component will be equally effective against other system components, thus further increasing the adversary work factor to successfully complete planned cyber attacks. An increase in diversity may add complexity and management overhead which could ultimately lead to mistakes and unauthorized configurations. Related controls: SA-12, SA-14, SC-27.

Control Enhancements:

(1) *HETEROGENEITY | VIRTUALIZATION TECHNIQUES*

The organization employs virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed [*Assignment: organization-defined frequency*].

Supplemental Guidance: While frequent changes to operating systems and applications pose configuration management challenges, the changes can result in an increased work factor for adversaries in order to carry out successful cyber attacks. Changing virtual operating systems or applications, as opposed to changing actual operating systems/applications, provide virtual changes that impede attacker success while reducing configuration management efforts. In addition, virtualization techniques can assist organizations in isolating untrustworthy software and/or software of dubious provenance into confined execution environments.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-30 CONCEALMENT AND MISDIRECTION

Control: The organization employs [*Assignment: organization-defined concealment and misdirection techniques*] for [*Assignment: organization-defined information systems*] at [*Assignment: organization-defined time periods*] to confuse and mislead adversaries.

Supplemental Guidance: Concealment and misdirection techniques can significantly reduce the targeting capability of adversaries (i.e., window of opportunity and available attack surface) to initiate and complete cyber attacks. For example, virtualization techniques provide organizations with the ability to disguise information systems, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms. Increased use of concealment/misdirection techniques including, for example, randomness, uncertainty, and virtualization, may sufficiently confuse and mislead adversaries and subsequently increase the risk of discovery and/or exposing tradecraft. Concealment/misdirection techniques may also provide organizations additional time to successfully perform core missions and business functions. Because of the time and effort required to support concealment/misdirection techniques, it is anticipated that such techniques would be used by organizations on a very limited basis. Related controls: SC-26, SC-29, SI-14.

Control Enhancements:

(1) *CONCEALMENT AND MISDIRECTION | VIRTUALIZATION TECHNIQUES*

[Withdrawn: Incorporated into SC-29 (1)].

(2) *CONCEALMENT AND MISDIRECTION | RANDOMNESS*

The organization employs [*Assignment: organization-defined techniques*] to introduce randomness into organizational operations and assets.

Supplemental Guidance: Randomness introduces increased levels of uncertainty for adversaries regarding the actions organizations take in defending against cyber attacks. Such actions may impede the ability of adversaries to correctly target information resources of organizations supporting critical missions/business functions. Uncertainty may also cause adversaries to hesitate before initiating or continuing attacks. Misdirection techniques involving randomness include, for example, performing certain routine actions at different times of day, employing different information technologies (e.g., browsers, search engines), using different suppliers, and rotating roles and responsibilities of organizational personnel.

(3) *CONCEALMENT AND MISDIRECTION | CHANGE PROCESSING / STORAGE LOCATIONS*

The organization changes the location of [*Assignment: organization-defined processing and/or storage*] [*Selection:* [*Assignment: organization-defined time frequency*]*; at random time intervals*]].

Supplemental Guidance: Adversaries target critical organizational missions/business functions and the information resources supporting those missions and functions while at the same time, trying to minimize exposure of their existence and tradecraft. The static, homogeneous, and deterministic nature of organizational information systems targeted by adversaries, make such systems more susceptible to cyber attacks with less adversary cost and effort to be successful. Changing organizational processing and storage locations (sometimes referred to as moving target defense) addresses the advanced persistent threat (APT) using techniques such as virtualization, distributed processing, and replication. This enables organizations to relocate the information resources (i.e., processing and/or storage) supporting critical missions and business functions. Changing locations of processing activities and/or storage sites introduces uncertainty into the targeting activities by adversaries. This uncertainty increases the work factor of adversaries making compromises or breaches to organizational information systems much more difficult and time-consuming, and increases the chances that adversaries may inadvertently disclose aspects of tradecraft while attempting to locate critical organizational resources.

(4) *CONCEALMENT AND MISDIRECTION | MISLEADING INFORMATION*

The organization employs realistic, but misleading information in [*Assignment: organization-defined information system components*] with regard to its security state or posture.

Supplemental Guidance: This control enhancement misleads potential adversaries regarding the nature and extent of security safeguards deployed by organizations. As a result, adversaries may employ incorrect (and as a result ineffective) attack techniques. One way of misleading adversaries is for organizations to place misleading information regarding the specific security controls deployed in external information systems that are known to be accessed or targeted by adversaries. Another technique is the use of deception nets (e.g., honeynets, virtualized environments) that mimic actual aspects of organizational information systems but use, for example, out-of-date software configurations.

(5) *CONCEALMENT AND MISDIRECTION | CONCEALMENT OF SYSTEM COMPONENTS*

The organization employs [*Assignment: organization-defined techniques*] to hide or conceal [*Assignment: organization-defined information system components*].

Supplemental Guidance: By hiding, disguising, or otherwise concealing critical information system components, organizations may be able to decrease the probability that adversaries target and successfully compromise those assets. Potential means for organizations to hide and/or conceal information system components include, for example, configuration of routers or the use of honeynets or virtualization techniques.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-31 COVERT CHANNEL ANALYSIS

Control: The organization:

a. Performs a covert channel analysis to identify those aspects of communications within the information system that are potential avenues for covert [*Selection (one or more): storage; timing*] channels; and

b. Estimates the maximum bandwidth of those channels.

Supplemental Guidance: Developers are in the best position to identify potential areas within systems that might lead to covert channels. Covert channel analysis is a meaningful activity when there is the potential for unauthorized information flows across security domains, for example, in the case of information systems containing export-controlled information and having connections to external networks (i.e., networks not controlled by organizations). Covert channel analysis is also meaningful for multilevel secure (MLS) information systems, multiple security level (MSL) systems, and cross-domain systems. Related controls: AC-3, AC-4, PL-2.

Control Enhancements:

(1) *COVERT CHANNEL ANALYSIS | TEST COVERT CHANNELS FOR EXPLOITABILITY*

The organization tests a subset of the identified covert channels to determine which channels are exploitable.

(2) *COVERT CHANNEL ANALYSIS | MAXIMUM BANDWIDTH*

The organization reduces the maximum bandwidth for identified covert [*Selection (one or more); storage; timing*] channels to [*Assignment: organization-defined values*].

Supplemental Guidance: Information system developers are in the best position to reduce the maximum bandwidth for identified covert storage and timing channels.

(3) *COVERT CHANNEL ANALYSIS | MEASURE BANDWIDTH IN OPERATIONAL ENVIRONMENTS*

The organization measures the bandwidth of [*Assignment: organization-defined subset of identified covert channels*] in the operational environment of the information system.

Supplemental Guidance: This control enhancement addresses covert channel bandwidth in operational environments versus developmental environments. Measuring covert channel bandwidth in operational environments helps organizations to determine how much information can be covertly leaked before such leakage adversely affects organizational missions/business functions. Covert channel bandwidth may be significantly different when measured in those settings that are independent of the particular environments of operation (e.g., laboratories or development environments).

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-32 INFORMATION SYSTEM PARTITIONING

Control: The organization partitions the information system into [*Assignment: organization-defined information system components*] residing in separate physical domains or environments based on [*Assignment: organization-defined circumstances for physical separation of components*].

Supplemental Guidance: Information system partitioning is a part of a defense-in-depth protection strategy. Organizations determine the degree of physical separation of system components from physically distinct components in separate racks in the same room, to components in separate rooms for the more critical components, to more significant geographical separation of the most critical components. Security categorization can guide the selection of appropriate candidates for domain partitioning. Managed interfaces restrict or prohibit network access and information flow among partitioned information system components. Related controls: AC-4, SA-8, SC-2, SC-3, SC-7.

Control Enhancements: None.

References: FIPS Publication 199.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-33 TRANSMISSION PREPARATION INTEGRITY

[Withdrawn: Incorporated into SC-8].

SC-34 NON-MODIFIABLE EXECUTABLE PROGRAMS

Control: The information system at [*Assignment: organization-defined information system components*]:

a. Loads and executes the operating environment from hardware-enforced, read-only media; and

b. Loads and executes [*Assignment: organization-defined applications*] from hardware-enforced, read-only media.

Supplemental Guidance: The term *operating environment* is defined as the specific code that hosts applications, for example, operating systems, executives, or monitors including virtual machine monitors (i.e., hypervisors). It can also include certain applications running directly on hardware platforms. Hardware-enforced, read-only media include, for example, Compact Disk-Recordable

(CD-R)/Digital Video Disk-Recordable (DVD-R) disk drives and one-time programmable read-only memory. The use of non-modifiable storage ensures the integrity of software from the point of creation of the read-only image. The use of reprogrammable read-only memory can be accepted as read-only media provided: (i) integrity can be adequately protected from the point of initial writing to the insertion of the memory into the information system; and (ii) there are reliable hardware protections against reprogramming the memory while installed in organizational information systems. Related controls: AC-3, SI-7.

Control Enhancements:

(1) *NON-MODIFIABLE EXECUTABLE PROGRAMS | NO WRITABLE STORAGE*

The organization employs [*Assignment: organization-defined information system components*] with no writeable storage that is persistent across component restart or power on/off.

Supplemental Guidance: This control enhancement: (i) eliminates the possibility of malicious code insertion via persistent, writeable storage within the designated information system components; and (ii) applies to both fixed and removable storage, with the latter being addressed directly or as specific restrictions imposed through access controls for mobile devices. Related controls: AC-19, MP-7.

(2) *NON-MODIFIABLE EXECUTABLE PROGRAMS | INTEGRITY PROTECTION / READ-ONLY MEDIA*

The organization protects the integrity of information prior to storage on read-only media and controls the media after such information has been recorded onto the media.

Supplemental Guidance: Security safeguards prevent the substitution of media into information systems or the reprogramming of programmable read-only media prior to installation into the systems. Security safeguards include, for example, a combination of prevention, detection, and response. Related controls: AC-5, CM-3, CM-5, CM-9, MP-2, MP-4, MP-5, SA-12, SC-28, SI-3.

(3) *NON-MODIFIABLE EXECUTABLE PROGRAMS | HARDWARE-BASED PROTECTION*

The organization:

(a) Employs hardware-based, write-protect for [*Assignment: organization-defined information system firmware components*]; and

(b) Implements specific procedures for [*Assignment: organization-defined authorized individuals*] to manually disable hardware write-protect for firmware modifications and re-enable the write-protect prior to returning to operational mode.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-35 HONEYCLIENTS

Control: The information system includes components that proactively seek to identify malicious websites and/or web-based malicious code.

Supplemental Guidance: Honeyclients differ from honeypots in that the components actively probe the Internet in search of malicious code (e.g., worms) contained on external websites. As with honeypots, honeyclients require some supporting isolation measures (e.g., virtualization) to ensure that any malicious code discovered during the search and subsequently executed does not infect organizational information systems. Related controls: SC-26, SC-44, SI-3, SI-4.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-36 DISTRIBUTED PROCESSING AND STORAGE

Control: The organization distributes [*Assignment: organization-defined processing and storage*] across multiple physical locations.

Supplemental Guidance: Distributing processing and storage across multiple physical locations provides some degree of redundancy or overlap for organizations, and therefore increases the work factor of adversaries to adversely impact organizational operations, assets, and individuals. This control does not assume a single primary processing or storage location, and thus allows for parallel processing and storage. Related controls: CP-6, CP-7.

Control Enhancements:

(1) *DISTRIBUTED PROCESSING AND STORAGE | POLLING TECHNIQUES*

The organization employs polling techniques to identify potential faults, errors, or compromises to [*Assignment: organization-defined distributed processing and storage components*].

Supplemental Guidance: Distributed processing and/or storage may be employed to reduce opportunities for adversaries to successfully compromise the confidentiality, integrity, or availability of information and information systems. However, distribution of processing and/or storage components does not prevent adversaries from compromising one (or more) of the distributed components. Polling compares the processing results and/or storage content from the various distributed components and subsequently voting on the outcomes. Polling identifies potential faults, errors, or compromises in distributed processing and/or storage components. Related control: SI-4.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-37 OUT-OF-BAND CHANNELS

Control: The organization employs [*Assignment: organization-defined out-of-band channels*] for the physical delivery or electronic transmission of [*Assignment: organization-defined information, information system components, or devices*] to [*Assignment: organization-defined individuals or information systems*].

Supplemental Guidance: Out-of-band channels include, for example, local (nonnetwork) accesses to information systems, network paths physically separate from network paths used for operational traffic, or nonelectronic paths such as the US Postal Service. This is in contrast with using the same channels (i.e., in-band channels) that carry routine operational traffic. Out-of-band channels do not have the same vulnerability/exposure as in-band channels, and hence the confidentiality, integrity, or availability compromises of in-band channels will not compromise the out-of-band channels. Organizations may employ out-of-band channels in the delivery or transmission of many organizational items including, for example, identifiers/authenticators, configuration management changes for hardware, firmware, or software, cryptographic key management information, security updates, system/data backups, maintenance information, and malicious code protection updates. Related controls: AC-2, CM-3, CM-5, CM-7, IA-4, IA-5, MA-4, SC-12, SI-3, SI-4, SI-7.

Control Enhancements:

(1) *OUT-OF-BAND CHANNELS | ENSURE DELIVERY / TRANSMISSION*

The organization employs [*Assignment: organization-defined security safeguards*] to ensure that only [*Assignment: organization-defined individuals or information systems*] receive the [*Assignment: organization-defined information, information system components, or devices*].

Supplemental Guidance: Techniques and/or methods employed by organizations to ensure that only designated information systems or individuals receive particular information, system components, or devices include, for example, sending authenticators via courier service but requiring recipients to show some form of government-issued photographic identification as a condition of receipt.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-38 OPERATIONS SECURITY

Control: The organization employs [*Assignment: organization-defined operations security safeguards*] to protect key organizational information throughout the system development life cycle.

Supplemental Guidance: Operations security (OPSEC) is a systematic process by which potential adversaries can be denied information about the capabilities and intentions of organizations by identifying, controlling, and protecting generally unclassified information that specifically relates to the planning and execution of sensitive organizational activities. The OPSEC process involves five steps: (i) identification of critical information (e.g., the security categorization process); (ii) analysis of threats; (iii) analysis of vulnerabilities; (iv) assessment of risks; and (v) the application of appropriate countermeasures. OPSEC safeguards are applied to both organizational information systems and the environments in which those systems operate. OPSEC safeguards help to protect the confidentiality of key information including, for example, limiting the sharing of information with suppliers and potential suppliers of information system components, information technology products and services, and with other non-organizational elements and individuals. Information critical to mission/business success includes, for example, user identities, element uses, suppliers, supply chain processes, functional and security requirements, system design specifications, testing protocols, and security control implementation details. Related controls: RA-2, RA-5, SA-12.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-39 PROCESS ISOLATION

Control: The information system maintains a separate execution domain for each executing process.

Supplemental Guidance: Information systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each information system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes can be

achieved, for example, by implementing separate address spaces. This capability is available in most commercial operating systems that employ multi-state processor technologies. Related controls: AC-3, AC-4, AC-6, SA-4, SA-5, SA-8, SC-2, SC-3.

Control Enhancements:

(1) *PROCESS ISOLATION | HARDWARE SEPARATION*

The information system implements underlying hardware separation mechanisms to facilitate process separation.

Supplemental Guidance: Hardware-based separation of information system processes is generally less susceptible to compromise than software-based separation, thus providing greater assurance that the separation will be enforced. Underlying hardware separation mechanisms include, for example, hardware memory management.

(2) *PROCESS ISOLATION | THREAD ISOLATION*

The information system maintains a separate execution domain for each thread in [*Assignment: organization-defined multi-threaded processing*].

References: None.

Priority and Baseline Allocation:

P1	**LOW** SC-39	**MOD** SC-39	**HIGH** SC-39

SC-40 WIRELESS LINK PROTECTION

Control: The information system protects external and internal [*Assignment: organization-defined wireless links*] from [*Assignment: organization-defined types of signal parameter attacks or references to sources for such attacks*].

Supplemental Guidance: This control applies to internal and external wireless communication links that may be visible to individuals who are not authorized information system users. Adversaries can exploit the signal parameters of wireless links if such links are not adequately protected. There are many ways to exploit the signal parameters of wireless links to gain intelligence, deny service, or to spoof users of organizational information systems. This control reduces the impact of attacks that are unique to wireless systems. If organizations rely on commercial service providers for transmission services as commodity items rather than as fully dedicated services, it may not be possible to implement this control. Related controls: AC-18, SC-5.

Control Enhancements:

(1) *WIRELESS LINK PROTECTION | ELECTROMAGNETIC INTERFERENCE*

The information system implements cryptographic mechanisms that achieve [*Assignment: organization-defined level of protection*] against the effects of intentional electromagnetic interference.

Supplemental Guidance: This control enhancement protects against intentional jamming that might deny or impair communications by ensuring that wireless spread spectrum waveforms used to provide anti-jam protection are not predictable by unauthorized individuals. The control enhancement may also coincidentally help to mitigate the effects of unintentional jamming due to interference from legitimate transmitters sharing the same spectrum. Mission requirements, projected threats, concept of operations, and applicable legislation, directives, regulations, policies, standards, and guidelines determine levels of wireless link availability and performance/cryptography needed. Related controls: SC-12, SC-13.

(2) *WIRELESS LINK PROTECTION | REDUCE DETECTION POTENTIAL*

The information system implements cryptographic mechanisms to reduce the detection potential of wireless links to [*Assignment: organization-defined level of reduction*].

Supplemental Guidance: This control enhancement is needed for covert communications and protecting wireless transmitters from being geo-located by their transmissions. The control enhancement ensures that spread spectrum waveforms used to achieve low probability of

detection are not predictable by unauthorized individuals. Mission requirements, projected threats, concept of operations, and applicable legislation, directives, regulations, policies, standards, and guidelines determine the levels to which wireless links should be undetectable. Related controls: SC-12, SC-13.

(3) *WIRELESS LINK PROTECTION | IMITATIVE OR MANIPULATIVE COMMUNICATIONS DECEPTION*

The information system implements cryptographic mechanisms to identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters.

Supplemental Guidance: This control enhancement ensures that the signal parameters of wireless transmissions are not predictable by unauthorized individuals. Such unpredictability reduces the probability of imitative or manipulative communications deception based upon signal parameters alone. Related controls: SC-12, SC-13.

(4) *WIRELESS LINK PROTECTION | SIGNAL PARAMETER IDENTIFICATION*

The information system implements cryptographic mechanisms to prevent the identification of [*Assignment: organization-defined wireless transmitters*] by using the transmitter signal parameters.

Supplemental Guidance: Radio fingerprinting techniques identify the unique signal parameters of transmitters to fingerprint such transmitters for purposes of tracking and mission/user identification. This control enhancement protects against the unique identification of wireless transmitters for purposes of intelligence exploitation by ensuring that anti-fingerprinting alterations to signal parameters are not predictable by unauthorized individuals. This control enhancement helps assure mission success when anonymity is required. Related controls: SC-12, SC-13.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-41 PORT AND I/O DEVICE ACCESS

Control: The organization physically disables or removes [*Assignment: organization-defined connection ports or input/output devices*] on [*Assignment: organization-defined information systems or information system components*].

Supplemental Guidance: Connection ports include, for example, Universal Serial Bus (USB) and Firewire (IEEE 1394). Input/output (I/O) devices include, for example, Compact Disk (CD) and Digital Video Disk (DVD) drives. Physically disabling or removing such connection ports and I/O devices helps prevent exfiltration of information from information systems and the introduction of malicious code into systems from those ports/devices.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-42 SENSOR CAPABILITY AND DATA

Control: The information system:

a. Prohibits the remote activation of environmental sensing capabilities with the following exceptions: [*Assignment: organization-defined exceptions where remote activation of sensors is allowed*]; and

b. Provides an explicit indication of sensor use to [*Assignment: organization-defined class of users*].

Supplemental Guidance: This control often applies to types of information systems or system components characterized as mobile devices, for example, smart phones, tablets, and E-readers. These systems often include sensors that can collect and record data regarding the environment where the system is in use. Sensors that are embedded within mobile devices include, for example, cameras, microphones, Global Positioning System (GPS) mechanisms, and accelerometers. While the sensors on mobiles devices provide an important function, if activated covertly, such devices can potentially provide a means for adversaries to learn valuable information about individuals and organizations. For example, remotely activating the GPS function on a mobile device could provide an adversary with the ability to track the specific movements of an individual.

Control Enhancements:

(1) *SENSOR CAPABILITY AND DATA | REPORTING TO AUTHORIZED INDIVIDUALS OR ROLES*

The organization ensures that the information system is configured so that data or information collected by the [*Assignment: organization-defined sensors*] is only reported to authorized individuals or roles.

Supplemental Guidance: In situations where sensors are activated by authorized individuals (e.g., end users), it is still possible that the data/information collected by the sensors will be sent to unauthorized entities.

(2) *SENSOR CAPABILITY AND DATA | AUTHORIZED USE*

The organization employs the following measures: [*Assignment: organization-defined measures*], so that data or information collected by [*Assignment: organization-defined sensors*] is only used for authorized purposes.

Supplemental Guidance: Information collected by sensors for a specific authorized purpose potentially could be misused for some unauthorized purpose. For example, GPS sensors that are used to support traffic navigation could be misused to track movements of individuals. Measures to mitigate such activities include, for example, additional training to ensure that authorized parties do not abuse their authority, or (in the case where sensor data/information is maintained by external parties) contractual restrictions on the use of the data/information.

(3) *SENSOR CAPABILITY AND DATA | PROHIBIT USE OF DEVICES*

The organization prohibits the use of devices possessing [*Assignment: organization-defined environmental sensing capabilities*] in [*Assignment: organization-defined facilities, areas, or systems*].

Supplemental Guidance: For example, organizations may prohibit individuals from bringing cell phones or digital cameras into certain facilities or specific controlled areas within facilities where classified information is stored or sensitive conversations are taking place.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-43 USAGE RESTRICTIONS

Control: The organization:

a. Establishes usage restrictions and implementation guidance for [*Assignment: organization-defined information system components*] based on the potential to cause damage to the information system if used maliciously; and

b. Authorizes, monitors, and controls the use of such components within the information system.

Supplemental Guidance: Information system components include hardware, software, or firmware components (e.g., Voice Over Internet Protocol, mobile code, digital copiers, printers, scanners, optical devices, wireless technologies, mobile devices). Related controls: CM-6, SC-7.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-44 DETONATION CHAMBERS

Control: The organization employs a detonation chamber capability within [*Assignment: organization-defined information system, system component, or location*].

Supplemental Guidance: Detonation chambers, also known as dynamic execution environments, allow organizations to open email attachments, execute untrusted or suspicious applications, and execute Universal Resource Locator (URL) requests in the safety of an isolated environment or virtualized sandbox. These protected and isolated execution environments provide a means of determining whether the associated attachments/applications contain malicious code. While related to the concept of deception nets, the control is not intended to maintain a long-term environment in which adversaries can operate and their actions can be observed. Rather, it is intended to quickly identify malicious code and reduce the likelihood that the code is propagated to user environments of operation (or prevent such propagation completely). Related controls: SC-7, SC-25, SC-26, SC-30.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: SYSTEM AND INFORMATION INTEGRITY

SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

   1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and

b. Reviews and updates the current:

   1. System and information integrity policy [*Assignment: organization-defined frequency*]; and

   2. System and information integrity procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SI family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** SI-1	**MOD** SI-1	**HIGH** SI-1

SI-2 FLAW REMEDIATION

Control: The organization:

a. Identifies, reports, and corrects information system flaws;

b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

c. Installs security-relevant software and firmware updates within [*Assignment: organization-defined time period*] of the release of the updates; and

d. Incorporates flaw remediation into the organizational configuration management process.

Supplemental Guidance: Organizations identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. Organizations also address flaws discovered during security assessments,

continuous monitoring, incident response activities, and system error handling. Organizations take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By incorporating flaw remediation into ongoing configuration management processes, required/anticipated remediation actions can be tracked and verified. Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow US-CERT guidance and Information Assurance Vulnerability Alerts. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Organizations determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and also the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software and/or firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature updates. Organizations may also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures. Related controls: CA-2, CA-7, CM-3, CM-5, CM-8, MA-2, IR-4, RA-5, SA-10, SA-11, SI-11.

Control Enhancements:

(1) *FLAW REMEDIATION | CENTRAL MANAGEMENT*

The organization centrally manages the flaw remediation process.

Supplemental Guidance: Central management is the organization-wide management and implementation of flaw remediation processes. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw remediation security controls.

(2) *FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS*

The organization employs automated mechanisms [*Assignment: organization-defined frequency*] to determine the state of information system components with regard to flaw remediation.

Supplemental Guidance: Related controls: CM-6, SI-4.

(3) *FLAW REMEDIATION | TIME TO REMEDIATE FLAWS / BENCHMARKS FOR CORRECTIVE ACTIONS*

The organization:

(a) Measures the time between flaw identification and flaw remediation; and

(b) Establishes [*Assignment: organization-defined benchmarks*] for taking corrective actions.

Supplemental Guidance: This control enhancement requires organizations to determine the current time it takes on the average to correct information system flaws after such flaws have been identified, and subsequently establish organizational benchmarks (i.e., time frames) for taking corrective actions. Benchmarks can be established by type of flaw and/or severity of the potential vulnerability if the flaw can be exploited.

(4) *FLAW REMEDIATION | AUTOMATED PATCH MANAGEMENT TOOLS*

[Withdrawn: Incorporated into SI-2].

(5) *FLAW REMEDIATION | AUTOMATIC SOFTWARE / FIRMWARE UPDATES*

The organization installs [*Assignment: organization-defined security-relevant software and firmware updates*] automatically to [*Assignment: organization-defined information system components*].

Supplemental Guidance: Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates. Organizations must balance the need to ensure that the updates are installed as soon as possible with the need to maintain configuration management and with any mission or operational impacts that automatic updates might impose.

(6) *FLAW REMEDIATION | REMOVAL OF PREVIOUS VERSIONS OF SOFTWARE / FIRMWARE*

The organization removes [*Assignment: organization-defined software and firmware components*] after updated versions have been installed.

Supplemental Guidance: Previous versions of software and/or firmware components that are not removed from the information system after updates have been installed may be exploited by adversaries. Some information technology products may remove older versions of software and/or firmware automatically from the information system.

References: NIST Special Publications 800-40, 800-128.

Priority and Baseline Allocation:

P1	**LOW** SI-2	**MOD** SI-2 (2)	**HIGH** SI-2 (1) (2)

SI-3 MALICIOUS CODE PROTECTION

Control: The organization:

a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;

b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;

c. Configures malicious code protection mechanisms to:

1. Perform periodic scans of the information system [*Assignment: organization-defined frequency*] and real-time scans of files from external sources at [*Selection (one or more); endpoint; network entry/exit points*] as the files are downloaded, opened, or executed in accordance with organizational security policy; and

2. [*Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator;* [*Assignment: organization-defined action*]] in response to malicious code detection; and

d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Supplemental Guidance: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means including, for example, web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of information system vulnerabilities. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and/or actions in response to detection of maliciousness when attempting to open or execute files. Related controls: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7.

Control Enhancements:

(1) *MALICIOUS CODE PROTECTION | CENTRAL MANAGEMENT*

The organization centrally manages malicious code protection mechanisms.

Supplemental Guidance: Central management is the organization-wide management and implementation of malicious code protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw malicious code protection security controls. Related controls: AU-2, SI-8.

(2) *MALICIOUS CODE PROTECTION | AUTOMATIC UPDATES*

The information system automatically updates malicious code protection mechanisms.

Supplemental Guidance: Malicious code protection mechanisms include, for example, signature definitions. Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates. Related control: SI-8.

(3) *MALICIOUS CODE PROTECTION | NON-PRIVILEGED USERS*

[Withdrawn: Incorporated into AC-6 (10)].

(4) *MALICIOUS CODE PROTECTION | UPDATES ONLY BY PRIVILEGED USERS*

The information system updates malicious code protection mechanisms only when directed by a privileged user.

Supplemental Guidance: This control enhancement may be appropriate for situations where for reasons of security or operational continuity, updates are only applied when selected/approved by designated organizational personnel. Related controls: AC-6, CM-5.

(5) *MALICIOUS CODE PROTECTION | PORTABLE STORAGE DEVICES*

[Withdrawn: Incorporated into MP-7].

(6) *MALICIOUS CODE PROTECTION | TESTING / VERIFICATION*

The organization:

(a) Tests malicious code protection mechanisms [*Assignment: organization-defined frequency*] by introducing a known benign, non-spreading test case into the information system; and

(b) Verifies that both detection of the test case and associated incident reporting occur.

Supplemental Guidance: Related controls: CA-2, CA-7, RA-5.

(7) *MALICIOUS CODE PROTECTION | NONSIGNATURE-BASED DETECTION*

The information system implements nonsignature-based malicious code detection mechanisms.

Supplemental Guidance: Nonsignature-based detection mechanisms include, for example, the use of heuristics to detect, analyze, and describe the characteristics or behavior of malicious code and to provide safeguards against malicious code for which signatures do not yet exist or for which existing signatures may not be effective. This includes polymorphic malicious code (i.e., code that changes signatures when it replicates). This control enhancement does not preclude the use of signature-based detection mechanisms.

(8) *MALICIOUS CODE PROTECTION | DETECT UNAUTHORIZED COMMANDS*

The information system detects [*Assignment: organization-defined unauthorized operating system commands*] through the kernel application programming interface at [*Assignment: organization-defined information system hardware components*] and [*Selection (one or more): issues a warning; audits the command execution; prevents the execution of the command*].

Supplemental Guidance: This control enhancement can also be applied to critical interfaces other than kernel-based interfaces, including for example, interfaces with virtual machines and privileged applications. Unauthorized operating system commands include, for example, commands for kernel functions from information system processes that are not trusted to initiate such commands, or commands for kernel functions that are suspicious even though commands of that type are reasonable for processes to initiate. Organizations can define the malicious commands to be detected by a combination of command types, command classes, or specific instances of commands. Organizations can define hardware components by specific component, component type, location in the network, or combination therein.

Organizations may select different actions for different types/classes/specific instances of potentially malicious commands. Related control: AU-6.

(9) *MALICIOUS CODE PROTECTION | AUTHENTICATE REMOTE COMMANDS*

The information system implements [*Assignment: organization-defined security safeguards*] to authenticate [*Assignment: organization-defined remote commands*].

Supplemental Guidance: This control enhancement protects against unauthorized commands and replay of authorized commands. This capability is important for those remote information systems whose loss, malfunction, misdirection, or exploitation would have immediate and/or serious consequences (e.g., injury or death, property damage, loss of high-valued assets or sensitive information, or failure of important missions/business functions). Authentication safeguards for remote commands help to ensure that information systems accept and execute in the order intended, only authorized commands, and that unauthorized commands are rejected. Cryptographic mechanisms can be employed, for example, to authenticate remote commands. Related controls: SC-12, SC-13, SC-23.

(10) *MALICIOUS CODE PROTECTION | MALICIOUS CODE ANALYSIS*

The organization:

(a) Employs [*Assignment: organization-defined tools and techniques*] to analyze the characteristics and behavior of malicious code; and

(b) Incorporates the results from malicious code analysis into organizational incident response and flaw remediation processes.

Supplemental Guidance: The application of selected malicious code analysis tools and techniques provides organizations with a more in-depth understanding of adversary tradecraft (i.e., tactics, techniques, and procedures) and the functionality and purpose of specific instances of malicious code. Understanding the characteristics of malicious code facilitates more effective organizational responses to current and future threats. Organizations can conduct malicious code analyses by using reverse engineering techniques or by monitoring the behavior of executing code.

References: NIST Special Publication 800-83.

Priority and Baseline Allocation:

P1	**LOW** SI-3	**MOD** SI-3 (1) (2)	**HIGH** SI-3 (1) (2)

SI-4 INFORMATION SYSTEM MONITORING

Control: The organization:

a. Monitors the information system to detect:

1. Attacks and indicators of potential attacks in accordance with [*Assignment: organization-defined monitoring objectives*]; and

2. Unauthorized local, network, and remote connections;

b. Identifies unauthorized use of the information system through [*Assignment: organization-defined techniques and methods*];

c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;

d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;

e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or

the Nation based on law enforcement information, intelligence information, or other credible sources of information;

f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and

g. Provides [*Assignment: organization-defined information system monitoring information*] to [*Assignment: organization-defined personnel or roles*] [*Selection (one or more): as needed;* [*Assignment: organization-defined frequency*]].

Supplemental Guidance: Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system. Organizations can monitor information systems, for example, by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. Einstein network monitoring devices from the Department of Homeland Security can also be included as monitoring devices. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of information systems to support such objectives. Specific types of transactions of interest include, for example, Hyper Text Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. Information system monitoring is an integral part of organizational continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless. Related controls: AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, IR-4, PE-3, RA-5, SC-7, SC-26, SC-35, SI-3, SI-7.

Control Enhancements:

(1) *INFORMATION SYSTEM MONITORING | SYSTEM-WIDE INTRUSION DETECTION SYSTEM*

The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.

(2) *INFORMATION SYSTEM MONITORING | AUTOMATED TOOLS FOR REAL-TIME ANALYSIS*

The organization employs automated tools to support near real-time analysis of events.

Supplemental Guidance: Automated tools include, for example, host-based, network-based, transport-based, or storage-based event monitoring tools or Security Information and Event Management (SIEM) technologies that provide real time analysis of alerts and/or notifications generated by organizational information systems.

(3) *INFORMATION SYSTEM MONITORING | AUTOMATED TOOL INTEGRATION*

The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.

(4) *INFORMATION SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC*

The information system monitors inbound and outbound communications traffic [*Assignment: organization-defined frequency*] for unusual or unauthorized activities or conditions.

Supplemental Guidance: Unusual/unauthorized activities or conditions related to information system inbound and outbound communications traffic include, for example, internal traffic that indicates the presence of malicious code within organizational information systems or propagating among system components, the unauthorized exporting of information, or

signaling to external information systems. Evidence of malicious code is used to identify potentially compromised information systems or information system components.

(5) *INFORMATION SYSTEM MONITORING | SYSTEM-GENERATED ALERTS*

The information system alerts [*Assignment: organization-defined personnel or roles*] when the following indications of compromise or potential compromise occur: [*Assignment: organization-defined compromise indicators*].

Supplemental Guidance: Alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be transmitted, for example, telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the notification list can include, for example, system administrators, mission/business owners, system owners, or information system security officers. Related controls: AU-5, PE-6.

(6) *INFORMATION SYSTEM MONITORING | RESTRICT NON-PRIVILEGED USERS*

[Withdrawn: Incorporated into AC-6 (10)].

(7) *INFORMATION SYSTEM MONITORING | AUTOMATED RESPONSE TO SUSPICIOUS EVENTS*

The information system notifies [*Assignment: organization-defined incident response personnel (identified by name and/or by role)*] of detected suspicious events and takes [*Assignment: organization-defined least-disruptive actions to terminate suspicious events*].

Supplemental Guidance: Least-disruptive actions may include, for example, initiating requests for human responses.

(8) *INFORMATION SYSTEM MONITORING | PROTECTION OF MONITORING INFORMATION*

[Withdrawn: Incorporated into SI-4].

(9) *INFORMATION SYSTEM MONITORING | TESTING OF MONITORING TOOLS*

The organization tests intrusion-monitoring tools [*Assignment: organization-defined frequency*].

Supplemental Guidance: Testing intrusion-monitoring tools is necessary to ensure that the tools are operating correctly and continue to meet the monitoring objectives of organizations. The frequency of testing depends on the types of tools used by organizations and methods of deployment. Related control: CP-9.

(10) *INFORMATION SYSTEM MONITORING | VISIBILITY OF ENCRYPTED COMMUNICATIONS*

The organization makes provisions so that [*Assignment: organization-defined encrypted communications traffic*] is visible to [*Assignment: organization-defined information system monitoring tools*].

Supplemental Guidance: Organizations balance the potentially conflicting needs for encrypting communications traffic and for having insight into such traffic from a monitoring perspective. For some organizations, the need to ensure the confidentiality of communications traffic is paramount; for others, mission-assurance is of greater concern. Organizations determine whether the visibility requirement applies to internal encrypted traffic, encrypted traffic intended for external destinations, or a subset of the traffic types.

(11) *INFORMATION SYSTEM MONITORING | ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES*

The organization analyzes outbound communications traffic at the external boundary of the information system and selected [*Assignment: organization-defined interior points within the system (e.g., subnetworks, subsystems)*] to discover anomalies.

Supplemental Guidance: Anomalies within organizational information systems include, for example, large file transfers, long-time persistent connections, unusual protocols and ports in use, and attempted communications with suspected malicious external addresses.

(12) *INFORMATION SYSTEM MONITORING | AUTOMATED ALERTS*

The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined activities that trigger alerts*].

Supplemental Guidance: This control enhancement focuses on the security alerts generated by organizations and transmitted using automated means. In contrast to the alerts generated by information systems in SI-4 (5), which tend to focus on information sources internal to the

systems (e.g., audit records), the sources of information for this enhancement can include other entities as well (e.g., suspicious activity reports, reports on potential insider threats). Related controls: AC-18, IA-3.

(13) *INFORMATION SYSTEM MONITORING | ANALYZE TRAFFIC / EVENT PATTERNS*

The organization:

(a) Analyzes communications traffic/event patterns for the information system;

(b) Develops profiles representing common traffic patterns and/or events; and

(c) Uses the traffic/event profiles in tuning system-monitoring devices to reduce the number of false positives and the number of false negatives.

(14) *INFORMATION SYSTEM MONITORING | WIRELESS INTRUSION DETECTION*

The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.

Supplemental Guidance: Wireless signals may radiate beyond the confines of organization-controlled facilities. Organizations proactively search for unauthorized wireless connections including the conduct of thorough scans for unauthorized wireless access points. Scans are not limited to those areas within facilities containing information systems, but also include areas outside of facilities as needed, to verify that unauthorized wireless access points are not connected to the systems. Related controls: AC-18, IA-3.

(15) *INFORMATION SYSTEM MONITORING | WIRELESS TO WIRELINE COMMUNICATIONS*

The organization employs an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.

Supplemental Guidance: Related control: AC-18.

(16) *INFORMATION SYSTEM MONITORING | CORRELATE MONITORING INFORMATION*

The organization correlates information from monitoring tools employed throughout the information system.

Supplemental Guidance: Correlating information from different monitoring tools can provide a more comprehensive view of information system activity. The correlation of monitoring tools that usually work in isolation (e.g., host monitoring, network monitoring, anti-virus software) can provide an organization-wide view and in so doing, may reveal otherwise unseen attack patterns. Understanding the capabilities/limitations of diverse monitoring tools and how to maximize the utility of information generated by those tools can help organizations to build, operate, and maintain effective monitoring programs. Related control: AU-6.

(17) *INFORMATION SYSTEM MONITORING | INTEGRATED SITUATIONAL AWARENESS*

The organization correlates information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness.

Supplemental Guidance: This control enhancement correlates monitoring information from a more diverse set of information sources to achieve integrated situational awareness. Integrated situational awareness from a combination of physical, cyber, and supply chain monitoring activities enhances the capability of organizations to more quickly detect sophisticated cyber attacks and investigate the methods and techniques employed to carry out such attacks. In contrast to SI-4 (16) which correlates the various cyber monitoring information, this control enhancement correlates monitoring beyond just the cyber domain. Such monitoring may help reveal attacks on organizations that are operating across multiple attack vectors. Related control: SA-12.

(18) *INFORMATION SYSTEM MONITORING | ANALYZE TRAFFIC / COVERT EXFILTRATION*

The organization analyzes outbound communications traffic at the external boundary of the information system (i.e., system perimeter) and at [*Assignment: organization-defined interior points within the system (e.g., subsystems, subnetworks)*] to detect covert exfiltration of information.

Supplemental Guidance: Covert means that can be used for the unauthorized exfiltration of organizational information include, for example, steganography.

(19) *INFORMATION SYSTEM MONITORING | INDIVIDUALS POSING GREATER RISK*

The organization implements [*Assignment: organization-defined additional monitoring*] of individuals who have been identified by [*Assignment: organization-defined sources*] as posing an increased level of risk.

Supplemental Guidance: Indications of increased risk from individuals can be obtained from a variety of sources including, for example, human resource records, intelligence agencies, law enforcement organizations, and/or other credible sources. The monitoring of individuals is closely coordinated with management, legal, security, and human resources officials within organizations conducting such monitoring and complies with federal legislation, Executive Orders, policies, directives, regulations, and standards.

(20) *INFORMATION SYSTEM MONITORING | PRIVILEGED USER*

The organization implements [*Assignment: organization-defined additional monitoring*] of privileged users.

(21) *INFORMATION SYSTEM MONITORING | PROBATIONARY PERIODS*

The organization implements [*Assignment: organization-defined additional monitoring*] of individuals during [*Assignment: organization-defined probationary period*].

(22) *INFORMATION SYSTEM MONITORING | UNAUTHORIZED NETWORK SERVICES*

The information system detects network services that have not been authorized or approved by [*Assignment: organization-defined authorization or approval processes*] and [*Selection (one or more): audits; alerts* [*Assignment: organization-defined personnel or roles*]].

Supplemental Guidance: Unauthorized or unapproved network services include, for example, services in service-oriented architectures that lack organizational verification or validation and therefore may be unreliable or serve as malicious rogues for valid services. Related controls: AC-6, CM-7, SA-5, SA-9.

(23) *INFORMATION SYSTEM MONITORING | HOST-BASED DEVICES*

The organization implements [*Assignment: organization-defined host-based monitoring mechanisms*] at [*Assignment: organization-defined information system components*].

Supplemental Guidance: Information system components where host-based monitoring can be implemented include, for example, servers, workstations, and mobile devices. Organizations consider employing host-based monitoring mechanisms from multiple information technology product developers.

(24) *INFORMATION SYSTEM MONITORING | INDICATORS OF COMPROMISE*

The information system discovers, collects, distributes, and uses indicators of compromise.

Supplemental Guidance: Indicators of compromise (IOC) are forensic artifacts from intrusions that are identified on organizational information systems (at the host or network level). IOCs provide organizations with valuable information on objects or information systems that have been compromised. IOCs for the discovery of compromised hosts can include for example, the creation of registry key values. IOCs for network traffic include, for example, Universal Resource Locator (URL) or protocol elements that indicate malware command and control servers. The rapid distribution and adoption of IOCs can improve information security by reducing the time that information systems and organizations are vulnerable to the same exploit or attack.

References: NIST Special Publications 800-61, 800-83, 800-92, 800-94, 800-137.

Priority and Baseline Allocation:

P1	**LOW** SI-4	**MOD** SI-4 (2) (4) (5)	**HIGH** SI-4 (2) (4) (5)

SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

Control: The organization:

a. Receives information system security alerts, advisories, and directives from [*Assignment: organization-defined external organizations*] on an ongoing basis;

b. Generates internal security alerts, advisories, and directives as deemed necessary;

c. Disseminates security alerts, advisories, and directives to: [*Selection (one or more):* [*Assignment: organization-defined personnel or roles*]; [*Assignment: organization-defined elements within the organization*]; [*Assignment: organization-defined external organizations*]]; and

d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

Supplemental Guidance: The United States Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner. External organizations include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supporting organizations. Related control: SI-2.

Control Enhancements:

(1) *SECURITY ALERTS, ADVISORIES, AND DIRECTIVES | AUTOMATED ALERTS AND ADVISORIES*

The organization employs automated mechanisms to make security alert and advisory information available throughout the organization.

Supplemental Guidance: The significant number of changes to organizational information systems and the environments in which those systems operate requires the dissemination of security-related information to a variety of organizational entities that have a direct interest in the success of organizational missions and business functions. Based on the information provided by the security alerts and advisories, changes may be required at one or more of the three tiers related to the management of information security risk including the governance level, mission/business process/enterprise architecture level, and the information system level.

References: NIST Special Publication 800-40.

Priority and Baseline Allocation:

P1	**LOW** SI-5	**MOD** SI-5	**HIGH** SI-5 (1)

SI-6 SECURITY FUNCTION VERIFICATION

Control: The information system:

a. Verifies the correct operation of [*Assignment: organization-defined security functions*];

b. Performs this verification [*Selection (one or more):* [*Assignment: organization-defined system transitional states*]*; upon command by user with appropriate privilege;* [*Assignment: organization-defined frequency*]];

c. Notifies [*Assignment: organization-defined personnel or roles*] of failed security verification tests; and

d. [*Selection (one or more): shuts the information system down; restarts the information system;* [*Assignment: organization-defined alternative action(s)*]] when anomalies are discovered.

Supplemental Guidance: Transitional states for information systems include, for example, system startup, restart, shutdown, and abort. Notifications provided by information systems include, for example, electronic alerts to system administrators, messages to local computer consoles, and/or hardware indications such as lights. Related controls: CA-7, CM-6.

Control Enhancements:

(1) *SECURITY FUNCTION VERIFICATION | NOTIFICATION OF FAILED SECURITY TESTS*

[Withdrawn: Incorporated into SI-6].

(2) *SECURITY FUNCTION VERIFICATION | AUTOMATION SUPPORT FOR DISTRIBUTED TESTING*

The information system implements automated mechanisms to support for the management of distributed security testing.

Supplemental Guidance: Related control: SI-2.

(3) *SECURITY FUNCTION VERIFICATION | REPORT VERIFICATION RESULTS*

The organization reports the results of security function verification to [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: Organizational personnel with potential interest in security function verification results include, for example, senior information security officers, information system security managers, and information systems security officers. Related controls: SA-12, SI-4, SI-5.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SI-6

SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

Control: The organization employs integrity verification tools to detect unauthorized changes to [*Assignment: organization-defined software, firmware, and information*].

Supplemental Guidance: Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity (e.g., tampering). Software includes, for example, operating systems (with key internal components such as kernels, drivers), middleware, and applications. Firmware includes, for example, the Basic Input Output System (BIOS). Information includes metadata such as security attributes associated with information. State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications. Related controls: SA-12, SC-8, SC-13, SI-3.

Control Enhancements:

(1) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS*

The information system performs an integrity check of [*Assignment: organization-defined software, firmware, and information*] [*Selection (one or more):* **at startup; at [*Assignment: organization-defined transitional states or security-relevant events*]; [*Assignment: organization-defined frequency*]].

Supplemental Guidance: Security-relevant events include, for example, the identification of a new threat to which organizational information systems are susceptible, and the installation of new hardware, software, or firmware. Transitional states include, for example, system startup, restart, shutdown, and abort.

(2) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS*

The organization employs automated tools that provide notification to [*Assignment: organization-defined personnel or roles*] upon discovering discrepancies during integrity verification.

Supplemental Guidance: The use of automated tools to report integrity violations and to notify organizational personnel in a timely matter is an essential precursor to effective risk response.

Personnel having an interest in integrity violations include, for example, mission/business owners, information system owners, systems administrators, software developers, systems integrators, and information security officers.

(3) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CENTRALLY-MANAGED INTEGRITY TOOLS*

The organization employs centrally managed integrity verification tools.

Supplemental Guidance: Related controls: AU-3, SI-2, SI-8.

(4) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | TAMPER-EVIDENT PACKAGING*

[Withdrawn: Incorporated into SA-12].

(5) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS*

The information system automatically [*Selection (one or more): shuts the information system down; restarts the information system; implements* [*Assignment: organization-defined security safeguards*]] when integrity violations are discovered.

Supplemental Guidance: Organizations may define different integrity checking and anomaly responses: (i) by type of information (e.g., firmware, software, user data); (ii) by specific information (e.g., boot firmware, boot firmware for a specific types of machines); or (iii) a combination of both. Automatic implementation of specific safeguards within organizational information systems includes, for example, reversing the changes, halting the information system, or triggering audit alerts when unauthorized modifications to critical security files occur.

(6) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CRYPTOGRAPHIC PROTECTION*

The information system implements cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.

Supplemental Guidance: Cryptographic mechanisms used for the protection of integrity include, for example, digital signatures and the computation and application of signed hashes using asymmetric cryptography, protecting the confidentiality of the key used to generate the hash, and using the public key to verify the hash information. Related control: SC-13.

(7) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE*

The organization incorporates the detection of unauthorized [*Assignment: organization-defined security-relevant changes to the information system*] into the organizational incident response capability.

Supplemental Guidance: This control enhancement helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important both for being able to identify and discern adversary actions over an extended period of time and for possible legal actions. Security-relevant changes include, for example, unauthorized changes to established configuration settings or unauthorized elevation of information system privileges. Related controls: IR-4, IR-5, SI-4.

(8) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUDITING CAPABILITY FOR SIGNIFICANT EVENTS*

The information system, upon detection of a potential integrity violation, provides the capability to audit the event and initiates the following actions: [*Selection (one or more): generates an audit record; alerts current user; alerts* [*Assignment: organization-defined personnel or roles*]; [*Assignment: organization-defined other actions*]].

Supplemental Guidance: Organizations select response actions based on types of software, specific software, or information for which there are potential integrity violations. Related controls: AU-2, AU-6, AU-12.

(9) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | VERIFY BOOT PROCESS*

The information system verifies the integrity of the boot process of [*Assignment: organization-defined devices*].

Supplemental Guidance: Ensuring the integrity of boot processes is critical to starting devices in known/trustworthy states. Integrity verification mechanisms provide organizational personnel with assurance that only trusted code is executed during boot processes.

(10) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | PROTECTION OF BOOT FIRMWARE*

The information system implements [*Assignment: organization-defined security safeguards*] to protect the integrity of boot firmware in [*Assignment: organization-defined devices*].

Supplemental Guidance: Unauthorized modifications to boot firmware may be indicative of a sophisticated, targeted cyber attack. These types of cyber attacks can result in a permanent denial of service (e.g., if the firmware is corrupted) or a persistent malicious code presence (e.g., if code is embedded within the firmware). Devices can protect the integrity of the boot firmware in organizational information systems by: (i) verifying the integrity and authenticity of all updates to the boot firmware prior to applying changes to the boot devices; and (ii) preventing unauthorized processes from modifying the boot firmware.

(11) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES*

The organization requires that [*Assignment: organization-defined user-installed software*] execute in a confined physical or virtual machine environment with limited privileges.

Supplemental Guidance: Organizations identify software that may be of greater concern with regard to origin or potential for containing malicious code. For this type of software, user installations occur in confined environments of operation to limit or contain damage from malicious code that may be executed.

(12) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY VERIFICATION*

The organization requires that the integrity of [*Assignment: organization-defined user-installed software*] be verified prior to execution.

Supplemental Guidance: Organizations verify the integrity of user-installed software prior to execution to reduce the likelihood of executing malicious code or code that contains errors from unauthorized modifications. Organizations consider the practicality of approaches to verifying software integrity including, for example, availability of checksums of adequate trustworthiness from software developers or vendors.

(13) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE EXECUTION IN PROTECTED ENVIRONMENTS*

The organization allows execution of binary or machine-executable code obtained from sources with limited or no warranty and without the provision of source code only in confined physical or virtual machine environments and with the explicit approval of [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: This control enhancement applies to all sources of binary or machine-executable code including, for example, commercial software/firmware and open source software.

(14) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | BINARY OR MACHINE EXECUTABLE CODE*

The organization:

(a) Prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code; and

(b) Provides exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the authorizing official.

Supplemental Guidance: This control enhancement applies to all sources of binary or machine-executable code including, for example, commercial software/firmware and open source software. Organizations assess software products without accompanying source code from sources with limited or no warranty for potential security impacts. The assessments address the fact that these types of software products may be very difficult to review, repair, or extend, given that organizations, in most cases, do not have access to the original source code, and there may be no owners who could make such repairs on behalf of organizations. Related control: SA-5.

(15) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE AUTHENTICATION*

The information system implements cryptographic mechanisms to authenticate [*Assignment: organization-defined software or firmware components*] prior to installation.

Supplemental Guidance: Cryptographic authentication includes, for example, verifying that software or firmware components have been digitally signed using certificates recognized and approved by organizations. Code signing is an effective method to protect against malicious code.

(16) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | TIME LIMIT ON PROCESS EXECUTION W/O SUPERVISION*

The organization does not allow processes to execute without supervision for more than [*Assignment: organization-defined time period*].

Supplemental Guidance: This control enhancement addresses processes for which normal execution periods can be determined and situations in which organizations exceed such periods. Supervision includes, for example, operating system timers, automated responses, or manual oversight and response when information system process anomalies occur.

References: NIST Special Publications 800-147, 800-155.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SI-7 (1) (7)	**HIGH** SI-7 (1) (2) (5) (7) (14)

SI-8 SPAM PROTECTION

Control: The organization:

a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and

b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

Supplemental Guidance: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, mobile devices, and notebook/laptop computers. Spam can be transported by different means including, for example, electronic mail, electronic mail attachments, and web accesses. Spam protection mechanisms include, for example, signature definitions. Related controls: AT-2, AT-3, SC-5, SC-7, SI-3.

Control Enhancements:

(1) *SPAM PROTECTION | CENTRAL MANAGEMENT*

The organization centrally manages spam protection mechanisms.

Supplemental Guidance: Central management is the organization-wide management and implementation of spam protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed spam protection security controls. Related controls: AU-3, SI-2, SI-7.

(2) *SPAM PROTECTION | AUTOMATIC UPDATES*

The information system automatically updates spam protection mechanisms.

(3) *SPAM PROTECTION | CONTINUOUS LEARNING CAPABILITY*

The information system implements spam protection mechanisms with a learning capability to more effectively identify legitimate communications traffic.

Supplemental Guidance: Learning mechanisms include, for example, Bayesian filters that respond to user inputs identifying specific traffic as spam or legitimate by updating algorithm parameters and thereby more accurately separating types of traffic.

References: NIST Special Publication 800-45.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** SI-8 (1) (2)	**HIGH** SI-8 (1) (2)

SI-9 INFORMATION INPUT RESTRICTIONS

[Withdrawn: Incorporated into AC-2, AC-3, AC-5, AC-6].

SI-10 INFORMATION INPUT VALIDATION

Control: The information system checks the validity of [*Assignment: organization-defined information inputs*].

Supplemental Guidance: Checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content. Software applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the tainted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing to interpreters prevents the content from being unintentionally interpreted as commands. Input validation helps to ensure accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks.

Control Enhancements:

(1) *INFORMATION INPUT VALIDATION | MANUAL OVERRIDE CAPABILITY*

The information system:

(a) Provides a manual override capability for input validation of [*Assignment: organization-defined inputs*];

(b) Restricts the use of the manual override capability to only [*Assignment: organization-defined authorized individuals*]; and

(c) Audits the use of the manual override capability.

Supplemental Guidance: Related controls: CM-3, CM-5.

(2) *INFORMATION INPUT VALIDATION | REVIEW / RESOLUTION OF ERRORS*

The organization ensures that input validation errors are reviewed and resolved within [*Assignment: organization-defined time period*].

Supplemental Guidance: Resolution of input validation errors includes, for example, correcting systemic causes of errors and resubmitting transactions with corrected input.

(3) *INFORMATION INPUT VALIDATION | PREDICTABLE BEHAVIOR*

The information system behaves in a predictable and documented manner that reflects organizational and system objectives when invalid inputs are received.

Supplemental Guidance: A common vulnerability in organizational information systems is unpredictable behavior when invalid inputs are received. This control enhancement ensures that there is predictable behavior in the face of invalid inputs by specifying information system responses that facilitate transitioning the system to known states without adverse, unintended side effects.

(4) *INFORMATION INPUT VALIDATION | REVIEW / TIMING INTERACTIONS*

The organization accounts for timing interactions among information system components in determining appropriate responses for invalid inputs.

Supplemental Guidance: In addressing invalid information system inputs received across protocol interfaces, timing interfaces become relevant, where one protocol needs to consider the impact of the error response on other protocols within the protocol stack. For example, 802.11 standard wireless network protocols do not interact well with Transmission Control Protocols (TCP) when packets are dropped (which could be due to invalid packet input). TCP assumes packet losses are due to congestion, while packets lost over 802.11 links are typically dropped due to collisions or noise on the link. If TCP makes a congestion response, it takes

precisely the wrong action in response to a collision event. Adversaries may be able to use apparently acceptable individual behaviors of the protocols in concert to achieve adverse effects through suitable construction of invalid input.

(5) *INFORMATION INPUT VALIDATION | RESTRICT INPUTS TO TRUSTED SOURCES AND APPROVED FORMATS*

The organization restricts the use of information inputs to [*Assignment: organization-defined trusted sources*] and/or [*Assignment: organization-defined formats*].

Supplemental Guidance: This control enhancement applies the concept of whitelisting to information inputs. Specifying known trusted sources for information inputs and acceptable formats for such inputs can reduce the probability of malicious activity.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SI-10	**HIGH** SI-10

SI-11 ERROR HANDLING

Control: The information system:

a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and

b. Reveals error messages only to [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: Organizations carefully consider the structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business information that can be derived from (if not stated explicitly by) information recorded, and personal information such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitting information. Related controls: AU-2, AU-3, SC-31.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** SI-11	**HIGH** SI-11

SI-12 INFORMATION HANDLING AND RETENTION

Control: The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Supplemental Guidance: Information handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of information systems. The National Archives and Records Administration provides guidance on records retention. Related controls: AC-16, AU-5, AU-11, MP-2, MP-4.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** SI-12	**MOD** SI-12	**HIGH** SI-12

SI-13 PREDICTABLE FAILURE PREVENTION

Control: The organization:

a. Determines mean time to failure (MTTF) for [*Assignment: organization-defined information system components*] in specific environments of operation; and

b. Provides substitute information system components and a means to exchange active and standby components at [*Assignment: organization-defined MTTF substitution criteria*].

Supplemental Guidance: While MTTF is primarily a reliability issue, this control addresses potential failures of specific information system components that provide security capability. Failure rates reflect installation-specific consideration, not industry-average. Organizations define criteria for substitution of information system components based on MTTF value with consideration for resulting potential harm from component failures. Transfer of responsibilities between active and standby components does not compromise safety, operational readiness, or security capability (e.g., preservation of state variables). Standby components remain available at all times except for maintenance issues or recovery failures in progress. Related controls: CP-2, CP-10, MA-6.

Control Enhancements:

(1) *PREDICTABLE FAILURE PREVENTION | TRANSFERRING COMPONENT RESPONSIBILITIES*

The organization takes information system components out of service by transferring component responsibilities to substitute components no later than [*Assignment: organization-defined fraction or percentage*] of mean time to failure.

(2) *PREDICTABLE FAILURE PREVENTION | TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION*

[Withdrawn: Incorporated into SI-7 (16)].

(3) *PREDICTABLE FAILURE PREVENTION | MANUAL TRANSFER BETWEEN COMPONENTS*

The organization manually initiates transfers between active and standby information system components [*Assignment: organization-defined frequency*] if the mean time to failure exceeds [*Assignment: organization-defined time period*].

(4) *PREDICTABLE FAILURE PREVENTION | STANDBY COMPONENT INSTALLATION / NOTIFICATION*

The organization, if information system component failures are detected:

(a) Ensures that the standby components are successfully and transparently installed within [*Assignment: organization-defined time period*]; and

(b) [*Selection (one or more): activates [Assignment: organization-defined alarm]; automatically shuts down the information system*].

Supplemental Guidance: Automatic or manual transfer of components from standby to active mode can occur, for example, upon detection of component failures.

(5) *PREDICTABLE FAILURE PREVENTION | FAILOVER CAPABILITY*

The organization provides [*Selection: real-time; near real-time*] [*Assignment: organization-defined failover capability*] for the information system.

Supplemental Guidance: Failover refers to the automatic switchover to an alternate information system upon the failure of the primary information system. Failover capability includes, for example, incorporating mirrored information system operations at alternate processing sites or periodic data mirroring at regular intervals defined by recovery time periods of organizations.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SI-14 NON-PERSISTENCE

Control: The organization implements non-persistent [*Assignment: organization-defined information system components and services*] that are initiated in a known state and terminated [*Selection (one or more): upon end of session of use; periodically at* [*Assignment: organization-defined frequency*]].

Supplemental Guidance: This control mitigates risk from advanced persistent threats (APTs) by significantly reducing the targeting capability of adversaries (i.e., window of opportunity and available attack surface) to initiate and complete cyber attacks. By implementing the concept of non-persistence for selected information system components, organizations can provide a known state computing resource for a specific period of time that does not give adversaries sufficient time on target to exploit vulnerabilities in organizational information systems and the environments in which those systems operate. Since the advanced persistent threat is a high-end threat with regard to capability, intent, and targeting, organizations assume that over an extended period of time, a percentage of cyber attacks will be successful. Non-persistent information system components and services are activated as required using protected information and terminated periodically or upon the end of sessions. Non-persistence increases the work factor of adversaries in attempting to compromise or breach organizational information systems.

Non-persistent system components can be implemented, for example, by periodically re-imaging components or by using a variety of common virtualization techniques. Non-persistent services can be implemented using virtualization techniques as part of virtual machines or as new instances of processes on physical machines (either persistent or non-persistent).The benefit of periodic refreshes of information system components/services is that it does not require organizations to first determine whether compromises of components or services have occurred (something that may often be difficult for organizations to determine). The refresh of selected information system components and services occurs with sufficient frequency to prevent the spread or intended impact of attacks, but not with such frequency that it makes the information system unstable. In some instances, refreshes of critical components and services may be done periodically in order to hinder the ability of adversaries to exploit optimum windows of vulnerabilities. Related controls: SC-30, SC-34.

Control Enhancements:

(1) *NON-PERSISTENCE | REFRESH FROM TRUSTED SOURCES*

The organization ensures that software and data employed during information system component and service refreshes are obtained from [*Assignment: organization-defined trusted sources*].

Supplemental Guidance: Trusted sources include, for example, software/data from write-once, read-only media or from selected off-line secure storage facilities.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SI-15 INFORMATION OUTPUT FILTERING

Control: The information system validates information output from [*Assignment: organization-defined software programs and/or applications*] to ensure that the information is consistent with the expected content.

Supplemental Guidance: Certain types of cyber attacks (e.g., SQL injections) produce output results that are unexpected or inconsistent with the output results that would normally be expected from software programs or applications. This control enhancement focuses on detecting extraneous content, preventing such extraneous content from being displayed, and alerting monitoring tools that anomalous behavior has been discovered. Related controls: SI-3, SI-4.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SI-16 MEMORY PROTECTION

Control: The information system implements [*Assignment: organization-defined security safeguards*] to protect its memory from unauthorized code execution.

Supplemental Guidance: Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced with hardware providing the greater strength of mechanism. Related controls: AC-25, SC-3.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SI-16	**HIGH** SI-16

SI-17 FAIL-SAFE PROCEDURES

Control: The information system implements [*Assignment: organization-defined fail-safe procedures*] when [*Assignment: organization-defined failure conditions occur*].

Supplemental Guidance: Failure conditions include, for example, loss of communications among critical system components or between system components and operational facilities. Fail-safe procedures include, for example, alerting operator personnel and providing specific instructions on subsequent steps to take (e.g., do nothing, reestablish system settings, shut down processes, restart the system, or contact designated organizational personnel). Related controls: CP-12, CP-13, SC-24, SI-13.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

APPENDIX G

INFORMATION SECURITY PROGRAMS

ORGANIZATION-WIDE INFORMATION SECURITY PROGRAM MANAGEMENT CONTROLS

The Federal Information Security Management Act (FISMA) requires organizations to develop and implement an organization-wide information security program to address information security for the information and information systems that support the operations and assets of the organization, including those provided or managed by another organization, contractor, or other source. The information security program management (PM) controls described in this appendix are typically implemented at the organization level and not directed at individual organizational information systems. The program management controls have been designed to facilitate compliance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. The controls are independent of any FIPS Publication 200 impact levels and therefore, are not directly associated with any of the security control baselines described in Appendix D. The program management controls do, however, complement the security controls in Appendix F and focus on the programmatic, organization-wide information security requirements that are independent of any particular information system and are essential for managing information security programs. Tailoring guidance can be applied to the program management controls in a manner similar to how the guidance is applied to security controls in Appendix F. Organizations specify the individual or individuals responsible and accountable for the development, implementation, assessment, authorization, and monitoring of the program management controls. Organizations document program management controls in the *information security program plan*. The organization-wide information security program plan supplements the individual security plans developed for each organizational information system. Together, the security plans for the individual information systems and the information security program cover the totality of security controls employed by the organization.

In addition to documenting the information security program management controls, the security program plan provides a vehicle for the organization, in a central repository, to document all security controls from Appendix F that have been designated as *common controls* (i.e., security controls inheritable by organizational information systems).[111] The information security program management controls and common controls contained in the information security program plan are implemented, assessed for effectiveness,[112] and authorized by a senior organizational official, with the same or similar authority and responsibility for managing risk as the authorization officials for information systems. Plans of action and milestones are developed and maintained for the program management and common controls that are deemed through assessment to be less than effective. Information security program management and common controls are also subject to the same continuous monitoring requirements as security controls employed in individual organizational information systems.

Table G-1 provides a summary of the security controls in the program management family from Appendix G. Organizations can use the recommended *priority code* designation associated with each program management control to assist in making sequencing decisions for implementation

[111] Common controls are those security controls that are inheritable by one or more organizational information systems, and thus are separate and distinct from information security program management controls.

[112] Assessment procedures for program management controls and common controls can be found in NIST Special Publication 800-53A.

(i.e., a Priority Code 1 [P1] control has a higher priority for implementation than a Priority Code 2 [P2] control; and a Priority Code 2 [P2] control has a higher priority for implementation than a Priority Code 3 [P3] control.

TABLE G-1: PROGRAM MANAGEMENT CONTROLS

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
PM-1	Information Security Program Plan	P1	**Deployed organization-wide. Supporting information security program. Not associated with security control baselines. Independent of any system impact level.**		
PM-2	Senior Information Security Officer	P1			
PM-3	Information Security Resources	P1			
PM-4	Plan of Action and Milestones Process	P1			
PM-5	Information System Inventory	P1			
PM-6	Information Security Measures of Performance	P1			
PM-7	Enterprise Architecture	P1			
PM-8	Critical Infrastructure Plan	P1			
PM-9	Risk Management Strategy	P1			
PM-10	Security Authorization Process	P1			
PM-11	Mission/Business Process Definition	P1			
PM-12	Insider Threat Program	P1			
PM-13	Information Security Workforce	P1			
PM-14	Testing, Training, and Monitoring	P1			
PM-15	Contacts with Security Groups and Associations	P3			
PM-16	Threat Awareness Program	P1			

Cautionary Note

Organizations are required to implement security program management controls to provide a foundation for the organizational information security program. The successful implementation of security controls for organizational information systems depends on the successful implementation of organization-wide program management controls. However, the manner in which organizations implement the program management controls depends on specific organizational characteristics including, for example, the size, complexity, and mission/business requirements of the respective organizations.

PM-1 INFORMATION SECURITY PROGRAM PLAN

Control: The organization:

a. Develops and disseminates an organization-wide information security program plan that:

   1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;

   2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;

   3. Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and

   4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;

b. Reviews the organization-wide information security program plan [*Assignment: organization-defined frequency*];

c. Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and

d. Protects the information security program plan from unauthorized disclosure and modification.

Supplemental Guidance: Information security program plans can be represented in single documents or compilations of documents at the discretion of organizations. The plans document the program management controls and organization-defined common controls. Information security program plans provide sufficient information about the program management controls/common controls (including specification of parameters for any *assignment* and *selection* statements either explicitly or by reference) to enable implementations that are unambiguously compliant with the intent of the plans and a determination of the risk to be incurred if the plans are implemented as intended.

The security plans for individual information systems and the organization-wide information security program plan together, provide complete coverage for all security controls employed within the organization. Common controls are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for an information system (e.g., security controls employed as part of an intrusion detection system providing organization-wide boundary protection inherited by one or more organizational information systems). The organization-wide information security program plan will indicate which separate security plans contain descriptions of common controls.

Organizations have the flexibility to describe common controls in a single document or in multiple documents. In the case of multiple documents, the documents describing common controls are included as attachments to the information security program plan. If the information security program plan contains multiple documents, the organization specifies in each document the organizational official or officials responsible for the development, implementation, assessment, authorization, and monitoring of the respective common controls. For example, the organization may require that the Facilities Management Office develop, implement, assess, authorize, and continuously monitor common physical and environmental protection controls from the PE family when such controls are not associated with a particular information system but instead, support multiple information systems. Related control: PM-8.

Control Enhancements: None.

References: None.

PM-2 SENIOR INFORMATION SECURITY OFFICER

Control: The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

Supplemental Guidance: The security officer described in this control is an organizational official. For a federal agency (as defined in applicable federal laws, Executive Orders, directives, policies, or regulations) this official is the Senior Agency Information Security Officer. Organizations may also refer to this official as the Senior Information Security Officer or Chief Information Security Officer.

Control Enhancements: None.

References: None.

PM-3 INFORMATION SECURITY RESOURCES

Control: The organization:

a. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement;

b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and

c. Ensures that information security resources are available for expenditure as planned.

Supplemental Guidance: Organizations consider establishing champions for information security efforts and as part of including the necessary resources, assign specialized expertise and resources as needed. Organizations may designate and empower an Investment Review Board (or similar group) to manage and provide oversight for the information security-related aspects of the capital planning and investment control process. Related controls: PM-4, SA-2.

Control Enhancements: None.

References: NIST Special Publication 800-65.

PM-4 PLAN OF ACTION AND MILESTONES PROCESS

Control: The organization:

a. Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems:

   1. Are developed and maintained;

   2. Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and

   3. Are reported in accordance with OMB FISMA reporting requirements.

b. Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Supplemental Guidance: The plan of action and milestones is a key document in the information security program and is subject to federal reporting requirements established by OMB. With the increasing emphasis on organization-wide risk management across all three tiers in the risk management hierarchy (i.e., organization, mission/business process, and information system), organizations view plans of action and milestones from an organizational perspective, prioritizing risk response actions and ensuring consistency with the goals and objectives of the organization. Plan of action and milestones updates are based on findings from security control assessments and

continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones. Related control: CA-5.

Control Enhancements: None.

References: OMB Memorandum 02-01; NIST Special Publication 800-37.

PM-5 INFORMATION SYSTEM INVENTORY

Control: The organization develops and maintains an inventory of its information systems.

Supplemental Guidance: This control addresses the inventory requirements in FISMA. OMB provides guidance on developing information systems inventories and associated reporting requirements. For specific information system inventory reporting requirements, organizations consult OMB annual FISMA reporting guidance.

Control Enhancements: None.

References: Web: http://www.omb.gov.

PM-6 INFORMATION SECURITY MEASURES OF PERFORMANCE

Control: The organization develops, monitors, and reports on the results of information security measures of performance.

Supplemental Guidance: Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security program and the security controls employed in support of the program.

Control Enhancements: None.

References: NIST Special Publication 800-55.

PM-7 ENTERPRISE ARCHITECTURE

Control: The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.

Supplemental Guidance: The enterprise architecture developed by the organization is aligned with the Federal Enterprise Architecture. The integration of information security requirements and associated security controls into the organization's enterprise architecture helps to ensure that security considerations are addressed by organizations early in the system development life cycle and are directly and explicitly related to the organization's mission/business processes. This process of security requirements integration also embeds into the enterprise architecture, an integral *information security architecture* consistent with organizational risk management and information security strategies. For PM-7, the information security architecture is developed at a system-of-systems level (organization-wide), representing all of the organizational information systems. For PL-8, the information security architecture is developed at a level representing an individual information system but at the same time, is consistent with the information security architecture defined for the organization. Security requirements and security control integration are most effectively accomplished through the application of the Risk Management Framework and supporting security standards and guidelines. The Federal Segment Architecture Methodology provides guidance on integrating information security requirements and security controls into enterprise architectures. Related controls: PL-2, PL-8, PM-11, RA-2, SA-3.

Control Enhancements: None.

References: NIST Special Publication 800-39.

PM-8 CRITICAL INFRASTRUCTURE PLAN

Control: The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

Supplemental Guidance: Protection strategies are based on the prioritization of critical assets and resources. The requirement and guidance for defining critical infrastructure and key resources and for preparing an associated critical infrastructure protection plan are found in applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Related controls: PM-1, PM-9, PM-11, RA-3.

Control Enhancements: None.

References: HSPD 7; National Infrastructure Protection Plan.

PM-9 RISK MANAGEMENT STRATEGY

Control: The organization:

a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems;

b. Implements the risk management strategy consistently across the organization; and

c. Reviews and updates the risk management strategy [*Assignment: organization-defined frequency*] or as required, to address organizational changes.

Supplemental Guidance: An organization-wide risk management strategy includes, for example, an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time. The use of a risk executive function can facilitate consistent, organization-wide application of the risk management strategy. The organization-wide risk management strategy can be informed by risk-related inputs from other sources both internal and external to the organization to ensure the strategy is both broad-based and comprehensive. Related control: RA-3.

Control Enhancements: None.

References: NIST Special Publications 800-30, 800-39.

PM-10 SECURITY AUTHORIZATION PROCESS

Control: The organization:

a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems and the environments in which those systems operate through security authorization processes;

b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and

c. Fully integrates the security authorization processes into an organization-wide risk management program.

Supplemental Guidance: Security authorization processes for information systems and environments of operation require the implementation of an organization-wide risk management process, a Risk Management Framework, and associated security standards and guidelines. Specific roles within the risk management process include an organizational risk executive (function) and designated authorizing officials for each organizational information system and common control provider. Security authorization processes are integrated with organizational continuous monitoring

processes to facilitate ongoing understanding and acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation. Related control: CA-6.

Control Enhancements: None.

References: NIST Special Publications 800-37, 800-39.

PM-11 MISSION/BUSINESS PROCESS DEFINITION

Control: The organization:

a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and

b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained.

Supplemental Guidance: Information protection needs are technology-independent, required capabilities to counter threats to organizations, individuals, or the Nation through the compromise of information (i.e., loss of confidentiality, integrity, or availability). Information protection needs are derived from the mission/business needs defined by the organization, the mission/business processes selected to meet the stated needs, and the organizational risk management strategy. Information protection needs determine the required security controls for the organization and the associated information systems supporting the mission/business processes. Inherent in defining an organization's information protection needs is an understanding of the level of adverse impact that could result if a compromise of information occurs. The security categorization process is used to make such potential impact determinations. Mission/business process definitions and associated information protection requirements are documented by the organization in accordance with organizational policy and procedure. Related controls: PM-7, PM-8, RA-2.

Control Enhancements: None.

References: FIPS Publication 199; NIST Special Publication 800-60.

PM-12 INSIDER THREAT PROGRAM

Control: The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.

Supplemental Guidance: Organizations handling classified information are required, under Executive Order 13587 and the National Policy on Insider Threat, to establish insider threat programs. The standards and guidelines that apply to insider threat programs in classified environments can also be employed effectively to improve the security of Controlled Unclassified Information in non-national security systems. Insider threat programs include security controls to detect and prevent malicious insider activity through the centralized integration and analysis of both technical and non-technical information to identify potential insider threat concerns. A senior organizational official is designated by the department/agency head as the responsible individual to implement and provide oversight for the program. In addition to the centralized integration and analysis capability, insider threat programs as a minimum, prepare department/agency insider threat policies and implementation plans, conduct host-based user monitoring of individual employee activities on government-owned classified computers, provide insider threat awareness training to employees, receive access to information from all offices within the department/agency (e.g., human resources, legal, physical security, personnel security, information technology, information system security, and law enforcement) for insider threat analysis, and conduct self-assessments of department/agency insider threat posture.

Insider threat programs can leverage the existence of incident handling teams organizations may already have in place, such as computer security incident response teams. Human resources

records are especially important in this effort, as there is compelling evidence to show that some types of insider crimes are often preceded by nontechnical behaviors in the workplace (e.g., ongoing patterns of disgruntled behavior and conflicts with coworkers and other colleagues). These precursors can better inform and guide organizational officials in more focused, targeted monitoring efforts. The participation of a legal team is important to ensure that all monitoring activities are performed in accordance with appropriate legislation, directives, regulations, policies, standards, and guidelines. Related controls: AC-6, AT-2, AU-6, AU-7- AU-10, AU-12, AU-13, CA-7, IA-4, IR-4, MP-7, PE-2, PS-3, PS-4, PS-5, PS-8, SC-7, SC-38, SI-4, PM-1, PM-14.

Control Enhancements: None.

References: Executive Order 13587.

PM-13 INFORMATION SECURITY WORKFORCE

Control: The organization establishes an information security workforce development and improvement program.

Supplemental Guidance: Information security workforce development and improvement programs include, for example: (i) defining the knowledge and skill levels needed to perform information security duties and tasks; (ii) developing role-based training programs for individuals assigned information security roles and responsibilities; and (iii) providing standards for measuring and building individual qualifications for incumbents and applicants for information security-related positions. Such workforce programs can also include associated information security career paths to encourage: (i) information security professionals to advance in the field and fill positions with greater responsibility; and (ii) organizations to fill information security-related positions with qualified personnel. Information security workforce development and improvement programs are complementary to organizational security awareness and training programs. Information security workforce development and improvement programs focus on developing and institutionalizing core information security capabilities of selected personnel needed to protect organizational operations, assets, and individuals. Related controls: AT-2, AT-3.

Control Enhancements: None.

References: None.

PM-14 TESTING, TRAINING, AND MONITORING

Control: The organization:

a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems:

   1. Are developed and maintained; and

   2. Continue to be executed in a timely manner;

b. Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Supplemental Guidance: This control ensures that organizations provide oversight for the security testing, training, and monitoring activities conducted organization-wide and that those activities are coordinated. With the importance of continuous monitoring programs, the implementation of information security across the three tiers of the risk management hierarchy, and the widespread use of common controls, organizations coordinate and consolidate the testing and monitoring activities that are routinely conducted as part of ongoing organizational assessments supporting a variety of security controls. Security training activities, while typically focused on individual information systems and specific roles, also necessitate coordination across all organizational elements. Testing, training, and monitoring plans and activities are informed by current threat and vulnerability assessments. Related controls: AT-3, CA-7, CP-4, IR-3, SI-4.

Control Enhancements: None.

References: NIST Special Publications 800-16, 800-37, 800-53A, 800-137.

PM-15 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS

Control: The organization establishes and institutionalizes contact with selected groups and associations within the security community:

a. To facilitate ongoing security education and training for organizational personnel;

b. To maintain currency with recommended security practices, techniques, and technologies; and

c. To share current security-related information including threats, vulnerabilities, and incidents.

Supplemental Guidance: Ongoing contact with security groups and associations is of paramount importance in an environment of rapidly changing technologies and threats. Security groups and associations include, for example, special interest groups, forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. Organizations select groups and associations based on organizational missions/business functions. Organizations share threat, vulnerability, and incident information consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Related control: SI-5.

Control Enhancements: None.

References: None.

PM-16 THREAT AWARENESS PROGRAM

Control: The organization implements a threat awareness program that includes a cross-organization information-sharing capability.

Supplemental Guidance: Because of the constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat (APT), it is becoming more likely that adversaries may successfully breach or compromise organizational information systems. One of the best techniques to address this concern is for organizations to share threat information. This can include, for example, sharing threat events (i.e., tactics, techniques, and procedures) that organizations have experienced, mitigations that organizations have found are effective against certain types of threats, threat intelligence (i.e., indications and warnings about threats that are likely to occur). Threat information sharing may be bilateral (e.g., government-commercial cooperatives, government-government cooperatives), or multilateral (e.g., organizations taking part in threat-sharing consortia). Threat information may be highly sensitive requiring special agreements and protection, or less sensitive and freely shared. Related controls: PM-12, PM-16.

Control Enhancements: None.

References: None.

APPENDIX H

INTERNATIONAL INFORMATION SECURITY STANDARDS

SECURITY CONTROL MAPPINGS FOR ISO/IEC 27001 AND 15408

The mapping tables in this appendix provide organizations with a *general* indication of security control coverage with respect to ISO/IEC 27001, *Information technology–Security techniques–Information security management systems–Requirements*[113] and ISO/IEC 15408, *Information technology -- Security techniques -- Evaluation criteria for IT security*.[114] ISO/IEC 27001 applies to all types of organizations and specifies requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented information security management system (ISMS) within the context of business risks. NIST Special Publication 800-39 includes guidance on managing risk at the organizational level, mission/business process level, and information system level, is consistent with ISO/IEC 27001, and provides additional implementation detail for the federal government and its contractors. ISO/IEC 15408 (also known as the Common Criteria) provides functionality and assurance requirements for developers of information systems and information system components (i.e., information technology products). Since many of the technical security controls defined in Appendix F are implemented in hardware, software, and firmware components of information systems, organizations can obtain significant benefit from the acquisition and employment of information technology products evaluated against the requirements of ISO/IEC 15408. The use of such products can provide evidence that certain security controls are implemented correctly, operating as intended, and producing the desired effect in satisfying stated security requirements.

[113] ISO/IEC 27001 was published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

[114] ISO/IEC 15408 was published in September 2012 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

Table H-1 provides a mapping from the security controls in NIST Special Publication 800-53 to the security controls in ISO/IEC 27001. The mappings are created by using the primary security topic identified in each of the Special Publication 800-53 and searching for a similar security topic in ISO/IEC 27001. Security controls with similar functional meaning are included in the mapping table. For example, Special Publication 800-53 contingency planning and ISO/IEC 27001 business continuity were deemed to have similar, but not the same, functionality. In some cases, similar topics are addressed in the security control sets but provide a different context, perspective, or scope. For example, Special Publication 800-53 addresses information flow control broadly in terms of approved authorizations for controlling access between source and destination objects, whereas ISO/IEC 27001 addresses the information flow more narrowly as it applies to interconnected network domains. Table H-2 provides a reverse mapping from the security controls in ISO/IEC 27001 to the security controls in Special Publication 800-53.[115]

TABLE H-1: MAPPING NIST SP 800-53 TO ISO/IEC 27001

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS
AC-1	Access Control Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.10.8.1, A.11.1.1, A.11.3.3, A.11.4.1, A.11.6.1, A.11.7.1, A.11.7.2, A.12.3.2, A.15.1.1, A.15.2.1
AC-2	Account Management	A.8.3.3, A.11.2.1, A.11.2.2, A.11.2.4, A.11.5.2, A.11.5.5, A.11.5.6
AC-3	Access Enforcement	A.7.2.2, A.10.6.1, A.10.7.3, A.10.7.4, A.10.8.1 A.10.9.1, A.10.9.2, A.10.9.3, A.11.2.2, A.11.5.4, A.11.6.1, A.12.4.3, A.15.1.3
AC-4	Information Flow Enforcement	A.7.2.2, A.10.7.3, A.10.8.1, A.11.4.5, A.11.4.7, A.12.5.4
AC-5	Separation of Duties	A.10.1.3
AC-6	Least Privilege	A.11.2.2, A.11.4.1, A.11.4.4, A.11.5.4, A.11.6.1, A.12.4.3
AC-7	Unsuccessful Logon Attempts	A.11.5.1
AC-8	System Use Notification	A.6.2.2, A.11.5.1, A.15.1.5
AC-9	Previous Logon (Access) Notification	A.11.5.1
AC-10	Concurrent Session Control	None
AC-11	Session Lock	A.11.3.2, A.11.3.3, A.11.5.5
AC-12	Session Termination	A.11.5.5
AC-13	**Withdrawn**	---
AC-14	Permitted Actions without Identification or Authentication	None
AC-15	**Withdrawn**	---
AC-16	Security Attributes	A.7.2.2, A.10.7.3
AC-17	Remote Access	A.10.6.1, A.10.8.1, A.10.8.5, A.11.4.1, A.11.4.2, A.11.4.6, A.11.7.1, A.11.7.2
AC-18	Wireless Access	A.10.6.1, A.10.8.1, A.11.4.1, A.11.4.2, A.11.4.6, A.11.7.1
AC-19	Access Control for Mobile Devices	A.9.2.5, A.10.4.1, A.10.7.3, A.11.4.3, A.11.4.6, A.11.7.1
AC-20	Use of External Information Systems	A.6.2.1, A.7.1.3, A.9.2.5, A.10.6.1, A.10.8.1, A.11.4.1, A.11.4.2, A.11.4.6
AC-21	Information Sharing	None
AC-22	Publicly Accessible Content	A.10.9.3, A.11.6.1
AC-23	Data Mining Protection	None
AC-24	Access Control Decisions	A.11.6.1
AC-25	Reference Monitor	None
AT-1	Security Awareness and Training Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
AT-2	Security Awareness Training	A.6.2.2, A.8.2.2, A.10.4.1
AT-3	Role-Based Security Training	A.6.2.2, A.8.2.2, A.10.4.1

[115] The use of the term *XX-1 controls* in mapping Table H-2 refers to the set of security controls represented by the first control in each family in Appendix F, where *XX* is a placeholder for the two-letter family identifier.

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS
AT-4	Security Training Records	None
AT-5	**Withdrawn**	---
AU-1	Audit and Accountability Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1, A.15.3.1
AU-2	Audit Events	A.10.10.1, A.10.10.2, A.10.10.4, A.10.10.5, A.11.5.4, A.15.3.1
AU-3	Content of Audit Records	A.10.10.1, A.10.10.2, A.10.10.4
AU-4	Audit Storage Capacity	A.10.3.1, A.10.10.3
AU-5	Response to Audit Processing Failures	A.10.3.1, A.10.10.3
AU-6	Audit Review, Analysis, and Reporting	A.10.10.2, A.10.10.5, A.13.1.1, A.15.1.5
AU-7	Audit Reduction and Report Generation	A.10.10.2, A.13.2.3
AU-8	Time Stamps	A.10.10.1, A.10.10.6, A.13.2.3
AU-9	Protection of Audit Information	A.10.10.3, A.13.2.3, A.15.1.3, A.15.3.2
AU-10	Non-repudiation	A.10.8.4, A.10.9.1, A.10.9.2, A.12.2.3
AU-11	Audit Record Retention	A.10.10.1, A.13.2.3, A.15.1.3
AU-12	Audit Generation	A.10.10.1, A.10.10.2, A.10.10.4, A.10.10.5
AU-13	Monitoring for Information Disclosure	A.12.5.4
AU-14	Session Audit	A.10.10.1
AU-15	Alternate Audit Capability	None
AU-16	Cross-Organizational Auditing	None
CA-1	Security Assessment and Authorization Policies and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3 A.6.1.4, A.6.1.8, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
CA-2	Security Assessments	A.6.1.8, A.6.2.2, A.10.3.2, A.13.1.2, A.15.2.1, A.15.2.2
CA-3	System Interconnections	A.6.2.1, A.6.2.2, A.6.2.3, A.10.6.1, A.10.6.2, A.10.8.1, A.10.8.2, A.10.8.5, A.11.4.2
CA-4	**Withdrawn**	---
CA-5	Plan of Action and Milestones	None
CA-6	Security Authorization	A.6.1.4, A.10.3.2
CA-7	Continuous Monitoring	A.6.1.8, A.12.6.1, A.13.1.2, A.15.2.1, A.15.2.2
CA-8	Penetration Testing	None
CA-9	Internal System Connections	None
CM-1	Configuration Management Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.12.4.1, A.12.5.1, A.15.1.1, A.15.2.1
CM-2	Baseline Configuration	A.10.1.2, A.10.1.4, A.12.4.1
CM-3	Configuration Change Control	A.10.1.2, A.10.3.2, A.12.4.1, A.12.5.1, A.12.5.2, A.12.5.3
CM-4	Security Impact Analysis	A.10.1.2, A.10.1.4, A.10.3.2, A.12.4.1, A.12.5.2, A.12.5.3
CM-5	Access Restrictions for Change	A.10.1.2, A.12.4.1, A.12.4.3, A.12.5.3
CM-6	Configuration Settings	A.10.10.2
CM-7	Least Functionality	A.11.4.1, A.11.4.4, A.11.4.6, A.12.4.1
CM-8	Information System Component Inventory	A.7.1.1, A.7.1.2
CM-9	Configuration Management Plan	A.6.1.3. A.7.1.1, A.7.1.2, A.10.1.2, A.10.1.4, A.10.3.2, A.12.4.1, A.12.4.3, A.12.5.1, A.12.5.2, A.12.5.3
CM-10	Software Usage Restrictions	A.12.4.1, A.15.1.2
CM-11	User-Installed Software	A.10.4.1, A.10.10.2, A.12.4.1, A.15.1.5
CP-1	Contingency Planning Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.14.1.1, A.14.1.3, A.15.1.1, A.15.2.1
CP-2	Contingency Plan	A.6.1.2, A.6.1.3, A.9.1.4, A.10.3.1, A.14.1.1, A.14.1.2, A.14.1.3, A.14.1.4, A.14.1.5
CP-3	Contingency Training	A.8.2.2
CP-4	Contingency Plan Testing	A.6.1.2, A.14.1.4, A.14.1.5
CP-5	**Withdrawn**	---
CP-6	Alternate Storage Site	A.9.1.4, A.14.1.3
CP-7	Alternate Processing Site	A.9.1.4, A.14.1.3
CP-8	Telecommunications Services	A.9.2.2, A.14.1.3
CP-9	Information System Backup	A.10.5.1, A.14.1.3, A.15.1.3

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS
CP-10	Information System Recovery and Reconstitution	A.14.1.3
CP-11	Alternate Communications Protocols	A.14.1.3
CP-12	Safe Mode	None
CP-13	Alternative Security Mechanisms	A.14.1.3
IA-1	Identification and Authentication Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
IA-2	Identification and Authentication (Organizational Users)	A.10.9.1, A.10.9.2, A.11.4.2, A.11.5.1, A.11.5.2
IA-3	Device Identification and Authentication	A.11.4.2, A.11.4.3
IA-4	Identifier Management	A.11.2.1, A.11.5.2
IA-5	Authenticator Management	A.11.2.1, A.11.2.3, A.11.3.1, A.11.5.1, A.11.5.2, A.11.5.3
IA-6	Authenticator Feedback	A.11.5.1, A.11.5.3
IA-7	Cryptographic Module Authentication	A.15.1.6
IA-8	Identification and Authentication (Non-Organizational Users)	A.10.9.1, A.10.9.2, A.11.4.2, A.11.5.1, A.11.5.2
IA-9	Service Identification and Authentication	None
IA-10	Adaptive Identification and Authentication	None
IA-11	Re-authentication	A.11.5.6
IR-1	Incident Response Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.13.1.1, A.13.2.1, A.15.1.1, A.15.2.1
IR-2	Incident Response Training	A.8.2.2, A.10.4.1
IR-3	Incident Response Testing	None
IR-4	Incident Handling	A.6.1.2, A.6.1.6, A.13.2.1, A.13.2.2, A.13.2.3
IR-5	Incident Monitoring	None
IR-6	Incident Reporting	A.6.1.6, A.13.1.1
IR-7	Incident Response Assistance	A.6.1.6
IR-8	Incident Response Plan	A.10.4.1
IR-9	Information Spillage Response	None
IR-10	Integrated Information Security Analysis Team	A.13.2.2
MA-1	System Maintenance Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
MA-2	Controlled Maintenance	A.9.2.4, A.9.2.7, A.11.4.4
MA-3	Maintenance Tools	A.9.2.4, A.10.4.1
MA-4	Nonlocal Maintenance	A.9.2.4, A.11.4.4
MA-5	Maintenance Personnel	A.9.1.1, A.9.2.4, A.12.4.3
MA-6	Timely Maintenance	A.9.2.4
MP-1	Media Protection Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.10.7.1, A.11.1.1, A.11.3.3, A.12.3.1, A.15.1.1, A.15.1.3, A.15.2.1
MP-2	Media Access	A.7.2.2, A.10.7.3, A.11.3.3
MP-3	Media Marking	A.7.2.2, A.10.7.3, A.10.7.4
MP-4	Media Storage	A.10.7.1, A.10.7.4, A.11.3.3, A.15.1.3
MP-5	Media Transport	A.9.2.5, A.9.2.7, A.10.7.1, A.10.8.3
MP-6	Media Sanitization	A.9.2.6, A.10.7.1, A.10.7.2
MP-7	Media Use	A.10.4.1, A.10.7.1
MP-8	Media Downgrading	None
PE-1	Physical and Environmental Protection Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.9.1.4, A.9.1.5, A.10.1.1, A.15.1.1, A.15.2.1
PE-2	Physical Access Authorizations	A.8.3.3, A.9.1.2
PE-3	Physical Access Control	A.9.1.1, A.9.1.2, A.9.1.3, A.9.1.6, A.11.4.4
PE-4	Access Control for Transmission Medium	A.9.1.1, A.9.1.2, A.9.1.3, A.9.2.3
PE-5	Access Control for Output Devices	A.9.1.1, A.9.1.2, A.9.1.3
PE-6	Monitoring Physical Access	A.9.1.2, A.10.10.2

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS
PE-7	**Withdrawn**	---
PE-8	Visitor Access Records	A.9.1.2, A.10.10.2
PE-9	Power Equipment and Cabling	A.9.1.4, A.9.2.2, A.9.2.3
PE-10	Emergency Shutoff	A.9.2.2
PE-11	Emergency Power	A.9.2.2
PE-12	Emergency Lighting	A.9.2.2
PE-13	Fire Protection	A.6.1.6, A.9.1.4, A.9.2.1
PE-14	Temperature and Humidity Controls	A.9.2.1, A.9.2.2
PE-15	Water Damage Protection	A.9.1.4, A.9.2.1
PE-16	Delivery and Removal	A.9.1.6, A.9.2.7
PE-17	Alternate Work Site	A.9.2.5, A.11.7.2
PE-18	Location of Information System Components	A.9.1.4, A.9.2.1
PE-19	Information Leakage	A.9.1.4, A.9.2.1, A.12.5.4
PE-20	Asset Monitoring and Tracking	None
PL-1	Security Planning Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
PL-2	System Security Plan	A.6.1.2
PL-3	**Withdrawn**	---
PL-4	Rules of Behavior	A.6.1.5, A.6.2.2, A.6.2.3, A.7.1.3. A.8.1.1, A.8.1.3, A.8.2.1, A.10.8.1, A.11.7.1, A.11.7.2, A.13.1.2, A.15.1.5
PL-5	**Withdrawn**	---
PL-6	**Withdrawn**	---
PL-7	Security Concept of Operations	A.12.1.1
PL-8	Information Security Architecture	A.12.1.1
PL-9	Central Management	None
PS-1	Personnel Security Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
PS-2	Position Risk Designation	A.8.1.1
PS-3	Personnel Screening	A.8.1.2
PS-4	Personnel Termination	A.8.3.1, A.8.3.2, A.8.3.3
PS-5	Personnel Transfer	A.8.3.1, A.8.3.2, A.8.3.3
PS-6	Access Agreements	A.6.1.5, A.6.2.3, A.7.1.3, A.8.1.1, A.8.1.3, A.8.2.1, A.10.8.1, A.11.7.1, A.11.7.2, A.15.1.5
PS-7	Third-Party Personnel Security	A.6.1.3, A.6.2.3, A.8.1.1, A.8.2.1
PS-8	Personnel Sanctions	A.8.2.3, A.15.1.5
RA-1	Risk Assessment Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
RA-2	Security Categorization	A.7.2.1, A.12.1.1
RA-3	Risk Assessment	A.6.2.1, A.12.6.1, A.14.1.2
RA-4	**Withdrawn**	---
RA-5	Vulnerability Scanning	A.12.6.1, A.15.2.2
RA-6	Technical Surveillance Countermeasures Survey	None
SA-1	System and Services Acquisition Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.12.5.5, A.15.1.1, A.15.2.1
SA-2	Allocation of Resources	A.6.1.2, A.10.3.1
SA-3	System Development Life Cycle	A.6.1.3, A.12.1.1
SA-4	Acquisition Process	A.10.3.2, A.12.1.1, A.12.5.5
SA-5	Information System Documentation	A.10.1.1, A.10.7.4, A.13.1.2, A.15.1.3
SA-6	**Withdrawn**	---
SA-7	**Withdrawn**	---
SA-8	Security Engineering Principles	A.10.4.2, A.12.1.1
SA-9	External Information System Services	A.6.1.3, A.6.1.5, A.6.2.1, A.6.2.2, A.6.2.3, A.8.2.1, A.10.2.1, A.10.2.2, A.10.2.3, A.10.6.2, A.10.8.2, A.12.5.5

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS
SA-10	Developer Configuration Management	A.10.1.2, A.10.1.4, A.10.2.3, A.10.3.2, A.12.4.3, A.12.5.1, A.12.5.3, A.12.5.5
SA-11	Developer Security Testing and Evaluation	A.6.1.8, A.10.3.2, A.12.5.5, A.13.1.2
SA-12	Supply Chain Protections	A.12.5.5
SA-13	Trustworthiness	A.12.5.5
SA-14	Criticality Analysis	None
SA-15	Development Process, Standards, and Tools	A.12.4.2, A.12.5.5
SA-16	Developer-Provided Training	A.8.2.2
SA-17	Developer Security Architecture and Design	None
SA-18	Tamper Resistance and Detection	None
SA-19	Component Authenticity	None
SA-20	Customized Development of Critical Components	None
SA-21	Developer Screening	A.8.1.2
SA-22	Unsupported System Components	None
SC-1	System and Communications Protection Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.10.8.1, A.11.4.1, A.12.3.1, A.15.1.1, A.15.2.1
SC-2	Application Partitioning	A.10.4.2, A.10.9.2, A.11.4.5, A.11.5.4
SC-3	Security Function Isolation	A.10.4.2, A.10.9.2
SC-4	Information In Shared Resources	None
SC-5	Denial of Service Protection	A.10.3.1, A.10.6.1
SC-6	Resource Availability	None
SC-7	Boundary Protection	A.10.4.1, A.10.4.2, A.10.6.1, A.10.8.1, A.10.8.4, A.10.9.1, A.10.9.2, A.10.10.2, A.11.4.1, A.11.4.5, A.11.4.6, A.11.4.7, A.11.6.2
SC-8	Transmission Confidentiality and Integrity	A.10.6.1, A.10.8.1, A.10.8.4, A.10.9.1, A.10.9.2, A.12.2.3
SC-9	**Withdrawn**	---
SC-10	Network Disconnect	A.10.6.1, A.11.3.2, A.11.5.5
SC-11	Trusted Path	None
SC-12	Cryptographic Key Establishment and Management	A.12.3.2
SC-13	Cryptographic Protection	A.10.9.1, A.10.9.2, A.15.1.6
SC-14	**Withdrawn**	---
SC-15	Collaborative Computing Devices	A.10.8.1
SC-16	Transmission of Security Attributes	A.7.2.2
SC-17	Public Key Infrastructure Certificates	A.12.3.2
SC-18	Mobile Code	A.10.4.2, A.12.4.1
SC-19	Voice Over Internet Protocol	None
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	A.10.6.1
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	A.10.6.1
SC-22	Architecture and Provisioning for Name/Address Resolution Service	A.10.6.1
SC-23	Session Authenticity	None
SC-24	Fail in Known State	None
SC-25	Thin Nodes	None
SC-26	Honeypots	None
SC-27	Platform-Independent Applications	None
SC-28	Protection of Information at Rest	None
SC-29	Heterogeneity	None
SC-30	Concealment and Misdirection	None
SC-31	Covert Channel Analysis	A.12.5.4

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS
SC-32	Information System Partitioning	A.11.6.2
SC-33	**Withdrawn**	---
SC-34	Non-Modifiable Executable Programs	None
SC-35	Honeyclients	None
SC-36	Distributed Processing and Storage	None
SC-37	Out-of-Band Channels	None
SC-38	Operations Security	A.12.5.4
SC-39	Process Isolation	None
SC-40	Wireless Link Protection	None
SC-41	Port and I/O Device Access	None
SC-42	Sensor Capability and Data	A.10.4.1
SC-43	Usage Restrictions	A.11.5.6
SC-44	Detonation Chambers	A.10.8.4
SI-1	System and Information Integrity Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.10.4.1, A.15.1.1, A.15.2.1
SI-2	Flaw Remediation	A.12.6.1, A.13.1.2
SI-3	Malicious Code Protection	A.10.4.1, A.10.9.3
SI-4	Information System Monitoring	A.10.9.3, A.10.10.2, A.10.10.3, A.15.3.1
SI-5	Security Alerts, Advisories, and Directives	A.6.1.6, A.6.1.7, A.10.4.1, A.10.9.3, A.12.6.1, A.13.1.2
SI-6	Security Function Verification	A.10.10.2, A.10.10.6, A.12.2.2
SI-7	Software, Firmware, and Information Integrity	A.10.4.1, A.10.9.3, A.10.10.2, A.12.2.2, A.12.2.3, A.12.4.1
SI-8	Spam Protection	None
SI-9	**Withdrawn**	---
SI-10	Information Input Validation	A.10.7.3, A.10.9.3, A.12.2.1, A.12.2.2
SI-11	Error Handling	None
SI-12	Information Handling and Retention	A.10.7.3, A.15.1.3, A.15.1.4
SI-13	Predictable Failure Prevention	None
SI-14	Non-Persistence	None
SI-15	Information Output Filtering	A.12.2.4
SI-16	Memory Protection	None
SI-17	Fail-Safe Procedures	None
PM-1	Information Security Program Plan	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3
PM-2	Senior Information Security Officer	A.6.1.1, A.6.1.2, A.6.1.3
PM-3	Information Security Resources	A.6.1.1
PM-4	Plan of Action and Milestones Process	None
PM-5	Information System Inventory	A.7.1.1, A.7.1.2
PM-6	Information Security Measures of Performance	None
PM-7	Enterprise Architecture	None
PM-8	Critical Infrastructure Plan	None
PM-9	Risk Management Strategy	A.6.1.8, A.6.2.1, A.14.1.2
PM-10	Security Authorization Process	A.6.1.3, A.6.1.4
PM-11	Mission/Business Process Definition	None
PM-12	Insider Threat Program	None
PM-13	Information Security Workforce	A.8.2.2
PM-14	Testing, Training, and Monitoring	A.8.2.2
PM-15	Contacts with Security Groups and Associations	A.6.1.7
PM-16	Threat Awareness Program	None.

TABLE H-2: MAPPING ISO/IEC 27001 TO NIST SP 800-53

ISO/IEC 27001 CONTROLS	NIST SP 800-53 CONTROLS
A.5 Security Policy	
A.5.1 Information security policy	
A.5.1.1 Information security policy document	XX-1 controls, PM-1
A.5.1.2 Review of the information security policy	XX-1 controls, PM-1
A.6 Organization of information security	
A.6.1 Internal	
A.6.1.1 Management commitment to information security	XX-1 controls, PM-1, PM-2, PM-3
A.6.1.2 Information security coordination	XX-1 controls, PM-1, PM-2, CP-2, CP-4, IR-4, PL-1, PL-2, SA-2
A.6.1.3 Allocation of information security responsibilities	XX-1 controls, PM-1, PM-2, PM-10, CM-9, CP-2, PS-7, SA-3, SA-9,
A.6.1.4 Authorization process for information processing facilities	PM-10, CA-1, CA-6
A.6.1.5 Confidentiality agreements	PL-4, PS-6, SA-9
A.6.1.6 Contact with authorities	IR-4, IR-6, IR-7, PE-13, SA-19, SI-5
A.6.1.7 Contact with special interest groups	PM-15, SI-5
A.6.1.8 Independent review of information security	PM-9, CA-1, CA-2, CA-7, SA-11
A.6.2 External Parties	
A.6.2.1 Identification of risks related to external parties	PM-9, AC-20, CA-3, RA-3, SA-9
A.6.2.2 Addressing security when dealing with customers	AC-8 , AT-2, AT-3, CA-2, CA-3, PL-4, SA-9
A.6.2.3 Addressing security in third party agreements	CA-3, PL-4, PS-6, PS-7, SA-9
A.7 Asset Management	
A.7.1 Responsibility for assets	
A.7.1.1 Inventory of assets	PM-5, CM-8, CM-9
A.7.1.2 Ownership of assets	PM-5, CM-8, CM-9
A.7.1.3 Acceptable use of assets	AC-20, PL-4, PS-6
A.7.2 Information Classification	
A.7.2.1 Classification Guidelines	RA-2
A.7.2.2 Information labeling and handling	AC-3, AC-4, AC-16, MP-2, MP-3, SC-16
A.8 Human Resources Security	
A.8.1 Prior to Employment	
A.8.1.1 Roles and Responsibilities	XX-1 controls, PL-4, PS-2, PS-6, PS-7
A.8.1.2 Screening	PS-3, SA-21
A.8.1.3 Terms and conditions of employment	PL-4, PS-6
A.8.2 During employment	
A.8.2.1 Management responsibilities	PL-4, PS-6, PS-7, SA-9
A.8.2.2 Awareness, education, and training	PM-13, PM-14, AT-2, AT-3, CP-3, IR-2, SA-16
A.8.2.3 Disciplinary process	PS-8
A.8.3 Termination or change of employment	
A.8.3.1 Termination responsibilities	PS-4, PS-5
A.8.3.2 Return of assets	PS-4, PS-5
A.8.3.3 Removal of access rights	AC-2, PE-2, PS-4, PS-5
A.9 Physical and environmental security	
A.9.1 Secure areas	
A.9.1.1 Physical security perimeter	PE-3, PE-4, PE-5
A.9.1.2 Physical entry controls	MA-5, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
A.9.1.3 Securing offices, rooms, facilities	PE-3, PE-4, PE-5
A.9.1.4 Protecting against external and environmental threats	CP-2, CP-6, CP-7, PE-1, PE-9, PE-13, PE-15, PE-18, PE-19
A.9.1.5 Working in secure areas	PE-1
A.9.1.6 Public access, delivery and loading areas	PE-3 , PE-16
A.9.2 Equipment security	
A.9.2.1 Equipment siting and protection	PE-13, PE-14, PE-15, PE-18, PE-19
A.9.2.2 Supporting utilities	CP-8, PE-9, PE-10, PE-11, PE-12, PE-14

ISO/IEC 27001 CONTROLS	NIST SP 800-53 CONTROLS
A.9.2.3 Cabling security	PE-4, PE-9
A.9.2.4 Equipment maintenance	MA-2, MA-3, MA-4, MA-5, MA-6
A.9.2.5 Security of equipment off-premises	AC-19, AC-20, MP-5, PE-17
A.9.2.6 Secure disposal or reuse of equipment	MP-6
A.9.2.7 Removal of property	MA-2, MP-5, PE-16
A.10 Communications and operations management	
A.10.1 Operational procedures and responsibilities	
A.10.1.1 Documented operating procedures	XX-1 controls, SA-5
A.10.1.2 Change management	CM-2, CM-3, CM-4, CM-5, CM-9, SA-10
A.10.1.3 Segregation of duties	AC-5
A.10.1.4 Separation of development, test and operational facilities	CM-2, CM-4, CM-9, SA-10
A.10.2 Third-party service delivery management	
A.10.2.1 Service delivery	SA-9
A.10.2.2 Monitoring and review of third-party services	SA-9
A.10.2.3 Managing changes to third-party services	SA-9, SA-10
A.10.3 System planning and acceptance	
A.10.3.1 Capacity management	AU-4, AU-5, CP-2, SA-2, SC-5
A.10.3.2 System acceptance	CA-2, CA-6, CM-3, CM-4, CM-9, SA-4, SA-10, SA-11
A.10.4 Protection against malicious and mobile code	
A.10.4.1 Controls against malicious code	AC-19, AT-2, AT-3, CM-11, IR-2, IR-8, MA-3, MP-7, SC-7, SC-42, SI-1, SI-3, SI-5, SI-7
A.10.4.2 Controls against mobile code	SA-8, SC-2, SC-3, SC-7, SC-18
A.10.5 Backup	
A.10.5.1 Information backup	CP-9
A.10.6 Network security management	
A.10.6.1 Network controls	AC-3, AC-17, AC-18, AC-20, CA-3, SC-5, SC-7, SC-8, SC-10
A.10.6.2 Security of network services	CA-3, SA-9
A.10.7 Media handling	
A.10.7.1 Management of removable media	MP-1, MP-4, MP-5, MP-6, MP-7
A.10.7.2 Disposal of media	MP-6
A.10.7.3 Information handling procedures	AC-3, AC-4, AC-16, AC-19, MP-2, MP-3, SI-10, SI-12
A.10.7.4 Security of system documentation	AC-3, MP-3, MP-4, SA-5
A.10.8 Exchange of information	
A.10.8.1 Information exchange policies and procedures	AC-1, AC-3, AC-4, AC-17, AC-18, AC-20, CA-3, PL-4, PS-6, SC-1, SC-7, SC-8, SC-15
A.10.8.2 Exchange agreements	CA-3, SA-9
A.10.8.3 Physical media in transit	MP-5
A.10.8.4 Electronic messaging	AU-10, SC-7, SC-8, SC-44
A.10.8.5 Business information systems	AC-17, CA-3
A.10.9 Electronic commerce services	
A.10.9.1 Electronic commerce	AC-3, AU-10, IA-2, IA-8, SC-7, SC-8, SC-13
A.10.9.2 Online transactions	AC-3, AU-10, IA-2, IA-8, SC-2, SC-3, SC-7, SC-8, SC-13
A.10.9.3 Publicly available information	AC-3, AC-22, SI-3, SI-4, SI-5, SI-7, SI-10
A.10.10 Monitoring	
A.10.10.1 Audit logging	AU-2, AU-3, AU-8, AU-11, AU-12, AU-14
A.10.10.2 Monitoring system use	AU-2, AU-3, AU-6, AU-7, AU-12, CM-6, CM-11, PE-6, PE-8, SC-7, SI-4, SI-6, SI-7
A.10.10.3 Protection of log information	AU-4, AU-5, AU-9, SI-4
A.10.10.4 Administrator and operator logs	AU-2, AU-3, AU-12
A.10.10.5 Fault logging	AU-2, AU-6, AU-12, SI-6
A.10.10.6 Clock synchronization	AU-8

ISO/IEC 27001 CONTROLS	NIST SP 800-53 CONTROLS
A.11 Access Control	
A.11.1 Business requirement for access control	
A.11.1.1 Access control policy	AC-1, MP-1
A.11.2 User access management	
A.11.2.1 User registration	AC-2, IA-4, IA-5
A.11.2.2 Privilege management	AC-2, AC-3, AC-6
A.11.2.3 User password management	IA-5
A.11.2.4 Review of user access rights	AC-2
A.11.3 User responsibilities	
A.11.3.1 Password use	IA-5
A.11.3.2 Unattended user equipment	AC-11, SC-10
A.11.3.3 Clear desk and clear screen policy	AC-1, AC-11, MP-1, MP-2, MP-4
A.11.4 Network access control	
A.11.4.1 Policy on use of network services	AC-1, AC-6, AC-17, AC-18, AC-20, CM-7, SC-1, SC-7
A.11.4.2 User authentication for external connections	AC-17, AC-18, AC-20, CA-3, IA-2, IA-3, IA-8
A.11.4.3 Equipment identification in networks	AC-19, IA-3
A.11.4.4 Remote diagnostic and configuration port protection	AC-6, CM-7, MA-2, MA-4, PE-3
A.11.4.5 Segregation in networks	AC-4, SC-2, SC-7
A.11.4.6 Network connection control	AC-17, AC-18, AC-19, AC-20, CM-7, SC-7
A.11.4.7 Network routing control	AC-4, SC-7
A.11.5 Operating system access control	
A.11.5.1 Secure log-on procedures	AC-7, AC-8, AC-9, IA-2, IA-5, IA-6, IA-8
A.11.5.2 User identification and authentication	AC-2, IA-2, IA-4, IA-5, IA-8
A.11.5.3 Password management system	IA-5, IA-6
A.11.5.4 Use of system utilities	AC-3, AC-6, AU-2, SC-2
A.11.5.5 Session time-out	AC-2, AC-11, AC-12, SC-10
A.11.5.6 Limitation of connection time	AC-2, IA-11, SC-43
A.11.6 Application and information access control	
A.11.6.1 Information access restriction	AC-1, AC-3, AC-6, AC-22, AC-24
A.11.6.2 Sensitive system isolation	SC-7, SC-32
A.11.7 Mobile computing and teleworking	
A.11.7.1 Mobile computing and communications	AC-1, AC-17, AC-18, AC-19, PL-4, PS-6
A.11.7.2 Teleworking	AC-1, AC-17, PE-17, PL-4, PS-6
A.12 Information systems acquisition, development and maintenance	
A.12.1 Security requirements of information systems	
A.12.1.1 Security requirements analysis and specification	PL-7, PL-8, RA-2, SA-3, SA-4, SA-8
A.12.2 Correct processing in applications	
A.12.2.1 Input data validation	SI-10
A.12.2.2 Control of internal processing	SI-6, SI-7, SI-10
A.12.2.3 Message integrity	AU-10, SC-8, SC-23, SI-7
A.12.2.4 Output data validation	SI-15
A.12.3 Cryptographic controls	
A.12.3.1 Policy on the use of cryptographic controls	AC-1, MP-1, SC-1
A.12.3.2 Key management	SC-12, SC-17
A.12.4 Security of system files	
A.12.4.1 Control of operational software	CM-1, CM-2, CM-3, CM-4, CM-5, CM-7, CM-9, CM-10, CM-11, SC-18, SI-7
A.12.4.2 Protection of system test data	SA-15
A.12.4.3 Access control to program source code	AC-3, AC-6, CM-5, CM-9, MA-5, SA-10
A.12.5 Security in development and support processes	
A.12.5.1 Change control procedures	CM-1, CM-3, CM-9, SA-10

ISO/IEC 27001 CONTROLS	NIST SP 800-53 CONTROLS
A.12.5.2 Technical review of applications after operating system changes	CM-3, CM-4, CM-9
A.12.5.3 Restrictions on changes to software packages	CM-3, CM-4, CM-5, CM-9, SA-10
A.12.5.4 Information leakage	AC-4, AU-13, PE-19, SC-31, SC-38
A.12.5.5 Outsourced software development	SA-1, SA-4, SA-9, SA-10, SA-11, SA-12, SA-13, SA-15
A.12.6 Technical Vulnerability Management	
A.12.6.1 Control of technical vulnerabilities	CA-7, RA-3, RA-5, SI-2, SI-5
A.13 Information security incident management	
A.13.1 Reporting information security events and weaknesses	
A.13.1.1 Reporting information security events	AU-6, IR-1, IR-6
A.13.1.2 Reporting security weaknesses	CA-2, CA-7, PL-4, SA-5, SA-11, SI-2, SI-5
A.13.2 Management of information security incidents and improvements	
A.13.2.1 Responsibilities and procedures	IR-1, IR-4
A.13.2.2 Learning from information security incidents	IR-4, IR-10
A.13.2.3 Collection of evidence	AU-7, AU-8, AU-9, AU-11, IR-4
A.14 Business continuity management	
A.14.1 Information security aspects of business continuity management	
A.14.1.1 Including information security in the business continuity management process	CP-1, CP-2
A.14.1.2 Business continuity and risk assessment	PM-9, CP-2, RA-3
A.14.1.3 Developing and implementing continuity plans including information security	CP-1, CP-2, CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13
A.14.1.4 Business continuity planning framework	CP-2, CP-4
A.14.1.5 Testing, maintaining and reassessing business continuity plans	CP-2, CP-4
A.15 Compliance	
A.15.1 Compliance with legal requirements	
A.15.1.1 Identification of applicable legislation	XX-1 controls
A.15.1.2 Intellectual property rights (IPR)	CM-10
A.15.1.3 Protection of organizational records	AC-3, AU-9, AU-11, CP-9, MP-4, SA-5, SI-12
A.15.1.4 Data protection and privacy of personal information	Appendix J Privacy controls, SI-12
A.15.1.5 Prevention of misuse of information processing facilities	AC-8, AU-6, CM-11, PL-4, PS-6, PS-8
A.15.1.6 Regulation of cryptographic controls	IA-7, SC-13
A.15.2 Compliance with security policies and standards, and technical compliance	
A.15.2.1 Compliance with security policies and standards	XX-1 controls, CA-2, CA-7
A.15.2.2 Technical compliance checking	CA-2, CA-7, RA-5
A.15.3 Information systems audit considerations	
A.15.3.1 Information systems audit controls	AU-1, AU-2, SI-4
A.15.3.2 Protection of information systems audit tools	AU-9

Table H-3 provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the security controls in Special Publication 800-53. The table represents an *informal* correspondence between security requirements and security controls (i.e., the table is not intended to determine whether the ISO/IEC 15408 security requirements are fully, partially, or not satisfied by the associated security controls). However, the table can serve as a beneficial starting point for further correspondence analysis. Organizations are cautioned that satisfying ISO/IEC 15408 security requirements for an particular evaluated and validated information technology product as represented by the presence of certain security controls from Appendix F, does not imply that such requirements have been satisfied throughout the entire information system (which may consist of multiple, integrated individual component products). Additional information explaining the specific mappings that appear in Table H-3 is available at the National Information Assurance Partnership (NIAP) website at: http://www.niap-ccevs.org.

TABLE H-3: MAPPING ISO/IEC 15408 TO NIST SP 800-53

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
Functional Requirements			
FAU_ARP.1	**Security Audit Automatic Response** Security Alarms	AU-5	**Response to Audit Processing Failures**
		AU-5 (1)	**Response to Audit Processing Failures** *Audit Storage Capacity*
		AU-5 (2)	**Response to Audit Processing Failures** *Real-Time Alerts*
		AU-5 (3)	**Response to Audit Processing Failures** *Configurable Traffic Volume Thresholds*
		AU-5 (4)	**Response to Audit Processing Failures** *Shutdown on Failure*
		PE-6 (2)	**Monitoring Physical Access** *Automated Intrusion Recognition / Responses*
		SI-3	**Malicious Code Protection**
		SI-3 (8)	**Malicious Code Protection** *Detect Unauthorized Commands*
		SI-4 (5)	**Information System Monitoring** *System-Generated Alerts*
		SI-4 (7)	**Information Systems Monitoring** *Automated Response to Suspicious Events*
		SI-4 (22)	**Information Systems Monitoring** *Unauthorized Network Services*
		SI-7 (2)	**Software, Firmware, and Information Integrity** *Automated Notifications of Integrity Violations*
		SI-7 (5)	**Software, Firmware, and Information Integrity** *Automated Response to Integrity Violations*
		SI-7 (8)	**Software, Firmware, and Information Integrity** *Auditing Capability for Significant Events*
FAU_GEN.1	**Security Audit Data Generation** Audit Data Generation	AU-2	**Audit Events**
		AU-3	**Content of Audit Records**
		AU-3 (1)	**Content of Audit Records** *Additional Audit Information*
		AU-12	**Audit Generation**

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
FAU_GEN.2	**Security Audit Data Generation** User Identity Association	AU-3	**Content of Audit Records**
FAU_SAA.1	**Security Audit Analysis** Potential Violation Analysis	SI-4	**Information System Monitoring**
FAU_SAA.2	**Security Audit Analysis** Profile-Based Anomaly Detection	AC-2 (12)	**Account Management** *Account Monitoring / Atypical Usage*
		SI-4	**Information System Monitoring**
FAU_SAA.3	**Security Audit Analysis** Simple Attack Heuristics	SI-3 (7)	**Malicious Code Protection** *Non Signature-Based Protection*
		SI-4	**Information System Monitoring**
FAU_SAA.4	**Security Audit Analysis** Complex Attack Heuristics	SI-3 (7)	**Malicious Code Protection** *Non Signature-Based Protection*
		SI-4	**Information System Monitoring**
FAU_SAR.1	**Security Audit Review** Audit Review	AU-7	**Audit Reduction and Report Generation**
FAU_SAR.2	**Security Audit Review** Restricted Audit Review	AU-9 (6)	**Protection of Audit Information** *Read Only Access*
FAU_SAR.3	**Security Audit Review** Selectable Audit Review	AU-7	**Audit Reduction and Report Generation**
		AU-7 (1)	**Audit Reduction and Report Generation** *Automatic Processing*
		AU-7 (2)	**Audit Reduction and Report Generation** *Automatic Sort and Search*
FAU_SEL.1	**Security Audit Event Selection** Selective Audit	AU-12	**Audit Generation**
FAU_STG.1	**Security Audit Event Storage** Protected Audit Trail Storage	AU-9	**Protection of Audit Information**
FAU_STG.2	**Security Audit Event Storage** Guarantees of Audit Data Availability	AU-9	**Protection of Audit Information** *Alternate audit capability*
FAU_STG.3	**Security Audit Event Storage** Action In Case of Possible Audit Data Loss	AU-5	**Response to Audit Processing Failures**
		AU-5 (1)	**Response to Audit Processing Failures** *Audit Storage Capacity*
		AU-5 (2)	**Response To Audit Processing Failures** *Real-Time Alerts*
		AU-5 (4)	**Response To Audit Processing Failures** *Shutdown on Failure*
FAU_STG.4	**Security Audit Event Storage** Prevention of Audit Data Loss	AU-4	**Audit Storage Capacity**
		AU-5	**Response to Audit Processing Failures**
		AU-5 (2)	**Response To Audit Processing Failures** *Real-Time Alerts*
		AU-5 (4)	**Response To Audit Processing Failures** *Shutdown on Failure*
FCO_NRO.1	**Non-Repudiation of Origin** Selective Proof of Origin	AU-10	**Non-Repudiation**
		AU-10 (1)	**Non-Repudiation** *Association Of Identities*
		AU-10 (2)	**Non-Repudiation** *Validate Binding of Information Producer Identity*

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
FCO_NRO.2	**Non-Repudiation of Origin** Enforced Proof of Origin	AU-10	**Non-Repudiation**
		AU-10 (1)	**Non-Repudiation** *Association Of Identities*
		AU-10 (2)	**Non-Repudiation** *Validate Binding of Information Producer Identity*
FCO_NRR.1	**Non-Repudiation of Receipt** Selective Proof of Receipt	AU-10	**Non-Repudiation**
		AU-10 (1)	**Non-Repudiation** *Association Of Identities*
		AU-10 (2)	**Non-Repudiation** *Validate Binding of Information Producer Identity*
FCO_NRR.2	**Non-Repudiation of Receipt** Enforced Proof of Receipt	AU-10	**Non-Repudiation**
		AU-10 (1)	**Non-Repudiation** *Association Of Identities*
		AU-10 (2)	**Non-Repudiation** *Validate Binding of Information Producer Identity*
FCS_CKM.1	**Cryptographic Key Management** Cryptographic Key Generation	SC-12	**Cryptographic Key Establishment and Management**
FCS_CKM.2	**Cryptographic Key Management** Cryptographic Key Distribution	SC-12	**Cryptographic Key Establishment and Management**
FCS_CKM.3	**Cryptographic Key Management** Cryptographic Key Access	SC-12	**Cryptographic Key Establishment and Management**
FCS_CKM.4	**Cryptographic Key Management** Cryptographic Key Destruction	SC-12	**Cryptographic Key Establishment and Management**
FCS_COP.1	**Cryptographic Operation** Cryptographic Operation	SC-13	**Cryptographic Protection**
FDP_ACC.1	**Access Control Policy** Subset Access Control	AC-3	**Access Enforcement**
		AC-3 (3)	**Access Enforcement** *Mandatory Access Control*
		AC-3 (4)	**Access Enforcement** *Discretionary Access Control*
		AC-3 (7)	**Access Enforcement** *Role-Based Access Control*
FDP_ACC.2	**Access Control Policy** Complete Access Control	AC-3	**Access Enforcement**
		AC-3 (3)	**Access Enforcement** *Mandatory Access Control*
		AC-3 (4)	**Access Enforcement** *Discretionary Access Control*
		AC-3 (7)	**Access Enforcement** *Role-Based Access Control*
FDP_ACF.1	**Access Control Functions** Security Attribute Based Access Control	AC-3	**Access Enforcement**
		AC-3 (3)	**Access Enforcement** *Mandatory Access Control*
		AC-3 (4)	**Access Enforcement** *Discretionary Access Control*
		AC-3 (7)	**Access Enforcement** *Role-Based Access Control*
		AC-16	**Security Attributes**

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
		SC-16	**Transmission of Security Attributes**
FDP_DAU.1	**Data Authentication** Basic Data Authentication	SI-7	**Software, Firmware, and Information Integrity**
		SI-7 (1)	**Software, Firmware, and Information Integrity** *Integrity Checks*
		SI-7 (6)	**Software, Firmware, And Information Integrity** *Cryptographic Protection*
		SI-10	**Information Input Validation**
FDP_DAU.2	**Data Authentication** Data Authentication With Identity of Guarantor	SI-7	**Software, Firmware, and Information Integrity**
		SI-7 (1)	**Software, Firmware, and Information Integrity** *Integrity Checks*
		SI-7 (6)	**Software, Firmware, And Information Integrity** *Cryptographic Protection*
		SI-10	**Information Input Validation**
FDP_ETC.1	**Export from the TOE** Export of User Data without Security Attributes	No Mapping.	
FDP_ETC.2	**Export from the TOE** Export of User Data with Security Attributes	AC-4 (18)	**Information Flow Enforcement** *Security Attribute Binding*
		AC-16	**Security Attributes**
		AC-16 (5)	**Security Attributes** *Attribute Displays for Output Devices*
		SC-16	**Transmission of Security Attributes**
FDP_IFC.1	**Information Flow Control Policy** Subset Information Flow Control	AC-3	**Access Enforcement**
		AC-3 (3)	**Access Enforcement** *Mandatory Access Control*
		AC-4	**Information Flow Enforcement**
		AC-4 (1)	**Information Flow Enforcement** *Object Security Attributes*
FDP_IFC.2	**Information Flow Control Policy** Complete Information Flow Control	AC-3	**Access Enforcement**
		AC-3 (3)	**Access Enforcement** *Mandatory Access Control*
		AC-4	**Information Flow Enforcement**
FDP_IFF.1	**Information Flow Control Functions** Simple Security Attributes	AC-3	**Access Enforcement**
		AC-3 (3)	**Access Enforcement** *Mandatory Access Control*
		AC-4	**Information Flow Enforcement**
		AC-4 (1)	**Information Flow Enforcement** *Object Security Attributes*
		AC-4 (2)	**Information Flow Enforcement** *Processing Domains*
		AC-4 (7)	**Information Flow Enforcement** *One-Way Flow Mechanisms*
		AC-16	**Security Attributes**
		SC-7	**Boundary Protection**

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
FDP_IFF.2	**Information Flow Control Functions** Hierarchical Security Attributes	AC-3	**Access Enforcement**
		AC-3 (3)	**Access Enforcement** *Mandatory Access Control*
		AC-4 (1)	**Information Flow Enforcement** *Object Security Attributes*
		AC-16	**Security Attributes**
FDP_IFF.3	**Information Flow Control Functions** Limited Illicit Information Flows	SC-31	**Covert Channel Analysis**
		SC-31 (2)	**Covert Channel Analysis** *Maximum Bandwidth*
FDP_IFF.4	**Information Flow Control Functions** Partial Elimination of Illicit Information Flows	SC-31	**Covert Channel Analysis**
		SC-31 (2)	**Covert Channel Analysis** *Maximum Bandwidth*
FDP_IFF.5	**Information Flow Control Functions** No Illicit Information Flows	SC-31	**Covert Channel Analysis**
		SC-31 (2)	**Covert Channel Analysis** *Maximum Bandwidth*
FDP_IFF.6	**Information Flow Control Functions** Illicit Information Flow Monitoring	SC-31	**Covert Channel Analysis**
		SI-4 (18)	**Information System Monitoring** *Analyze Traffic / Covert Exfiltration*
FDP_ITC.1	**Import from Outside of the TOE** Import of User Data without Security Attributes	AC-4 (9)	**Information Flow Enforcement** *Human Reviews*
		AC-4 (12)	**Information Flow Enforcement** *Data Type Identifiers*
FDP_ITC.2	**Import from Outside of the TOE** Import of User Data with Security Attributes	AC-4 (18)	**Information Flow Enforcement** *Security Attribute Binding*
		AC-16	**Security Attributes**
		SC-16	**Transmission of Security Attributes**
FDP_ITT.1	**Internal TOE Transfer** Basic Internal Transfer Protection	SC-8	**Transmission Confidentiality and Integrity**
		SC-8 (1)	**Transmission Confidentiality and Integrity** *Cryptographic or Alternate Physical Protection*
		SC-5	**Denial of Service Protection**
FDP_ITT.2	**Internal TOE Transfer** Transmission Separation by Attribute	SC-8	**Transmission Confidentiality and Integrity**
		SC-8 (1)	**Transmission Confidentiality and Integrity** *Cryptographic or Alternate Physical Protection*
		SC-5	**Denial of Service Protection**
		AC-4 (21)	**Information Flow Enforcement** *Physical / Logical Separation of Information Flows*
FDP_ITT.3	**Internal TOE Transfer** Integrity Monitoring	SI-7	**Software, Firmware, and Information Integrity**
		SI-7 (1)	**Software, Firmware, and Information Integrity** *Integrity Checks*
		SC-8 (1)	**Transmission Integrity** *Cryptographic or Alternate Physical Protection*
		SI-7 (5)	**Software, Firmware, and Information Integrity** *Automated Response to Integrity Violations*

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
FDP_ITT.4	**Internal TOE Transfer** Attribute-Based Integrity Monitoring	SI-7	**Software, Firmware, and Information Integrity**
		SI-7 (1)	**Software, Firmware, and Information Integrity** *Integrity Checks*
		SC-8 (1)	**Transmission Integrity** *Cryptographic or Alternate Physical Protection*
		AC-4 (21)	**Information Flow Enforcement** *Physical / Logical Separation of Information Flows*
		SI-7 (5)	**Software, Firmware, and Information Integrity** *Automated Response to Integrity Violations*
FDP_RIP.1	**Residual Information Protection** Subset Residual Information Protection	SC-4	**Information in Shared Resources**
FDP_RIP.2	**Residual Information Protection** Full Residual Information Protection	SC-4	**Information in Shared Resources**
FDP_ROL.1	**Rollback** Basic Rollback	CP-10 (2)	**Information System Recovery and Reconstitution** *Transaction Recovery*
FDP_ROL.2	**Rollback** Advanced Rollback	CP-10 (2)	**Information System Recovery and Reconstitution** *Transaction Recovery*
FDP_SDI.1	**Stored Data Integrity** Stored Data Integrity Monitoring	SI-7	**Software, Firmware, and Information Integrity**
		SI-7 (1)	**Software, Firmware, and Information Integrity** *Integrity Scans*
FDP_SDI.2	**Stored Data Integrity** Stored Data Integrity Monitoring and Action	SI-7	**Software, Firmware, and Information Integrity**
		SI-7 (1)	**Software, Firmware, and Information Integrity** *Integrity Scans*
		SI-7 (5)	**Software, Firmware, and Information Integrity** *Automated Response to Integrity Violations*
FDP_UCT.1	**Inter-TSF User Data Confidentiality Transfer Protection** Basic Data Exchange Confidentiality	SC-8	**Transmission Confidentiality and Integrity**
		SC-8 (1)	**Transmission Confidentiality and Integrity** *Cryptographic or Alternate Physical Protection*
FDP_UIT.1	**Inter-TSF User Data Integrity Transfer Protection** Data Exchange Integrity	SC-8	**Transmission Confidentiality and Integrity**
		SC-8 (1)	**Transmission Confidentiality and Integrity** *Cryptographic or Alternate Physical Protection*
		SI-7	**Software, Firmware, and Information Integrity**
		SI-7 (6)	**Software, Firmware, and Information Integrity** *Cryptographic Protection*
FDP_UIT.2	**Inter-TSF User Data Integrity Transfer Protection** Source Data Exchange Recovery	No Mapping.	

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
FDP_UIT.3	**Inter-TSF User Data Integrity Transfer Protection** Destination Data Exchange Recovery	No Mapping.	
FIA_AFL.1	**Authentication Failure** Authentication Failure Handling	AC-7	**Unsuccessful Logon Attempts**
FIA_ATD.1	**User Attribute Definition** User Attribute Definition	AC-2	**Account Management**
		IA-2	**Identification and Authentication (Organizational Users)**
FIA_SOS.1	**Specification of Secrets** Verification of Secrets	IA-5	**Authenticator Management**
		IA-5 (1)	**Authenticator Management** Password-Based Authentication
		IA-5 (12)	**Authenticator Management** Biometric Authentication
FIA_SOS.2	**Specification of Secrets** TSF Generation of Secrets	IA-5	**Authenticator Management**
		IA-5 (1)	**Authenticator Management** Password-Based Authentication
		IA-5 (12)	**Authenticator Management** Biometric Authentication
FIA_UAU.1	**User Authentication** Timing of Authentication	AC-14	**Permitted Actions without Identification or Authentication**
		IA-2	**Identification and Authentication (Organizational Users)**
		IA-8	**Identification and Authentication (Non-Organizational Users)**
FIA_UAU.2	**User Authentication** User Authentication Before Any Action	AC-14	**Permitted Actions without Identification or Authentication**
		IA-2	**Identification and Authentication (Organizational Users)**
		IA-8	**Identification and Authentication (Non-Organizational Users)**
FIA_UAU.3	**User Authentication** Unforgeable Authentication	IA-2 (8)	**Identification and Authentication (Organizational Users)** *Network Access To Privileged Accounts - Replay Resistant*
		IA-2 (9)	**Identification and Authentication (Organizational Users)** *Network Access To Non-Privileged Accounts - Replay Resistant*
FIA_UAU.4	**User Authentication** Single-Use Authentication Mechanisms	IA-2 (8)	**Identification and Authentication (Organizational Users)** *Network Access To Privileged Accounts - Replay Resistant*
		IA-2 (9)	**Identification and Authentication (Organizational Users)** *Network Access To Non-Privileged Accounts - Replay Resistant*
FIA_UAU.5	**User Authentication** Multiple Authentication Mechanisms	IA-2 (1)	**Identification and Authentication (Organizational Users)** Network Access To Privileged Accounts
		IA-2 (2)	**Identification and Authentication (Organizational Users)** Network Access To Non-Privileged Accounts

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
		IA-2 (3)	**Identification and Authentication (Organizational Users)** Local Access To Privileged Accounts
		IA-2 (4)	**Identification and Authentication (Organizational Users)** Local Access To Non-Privileged Accounts
		IA-2 (6)	**Identification and Authentication (Organizational Users)** Network Access To Privileged Accounts - Separate Device
		IA-2 (7)	**Identification and Authentication (Organizational Users)** Network Access To Non-Privileged Accounts - Separate Device
		IA-2 (11)	**Identification and Authentication (Organizational Users)** Remote Access - Separate Device
FIA_UAU.6	**User Authentication** Re-Authenticating	IA-11	**Re-authentication**
FIA_UAU.7	**User Authentication** Protected Authentication Feedback	IA-6	**Authenticator Feedback**
FIA_UID.1	**User Identification** Timing of Identification	AC-14	**Permitted Actions without Identification or Authentication**
		IA-2	**Identification and Authentication (Organizational Users)**
		IA-8	**Identification and Authentication (Non-Organizational Users)**
FIA_UID.2	**User Identification** User Identification Before Any Action	AC-14	**Permitted Actions without Identification or Authentication**
		IA-2	**Identification and Authentication (Organizational Users)**
		IA-8	**Identification and Authentication (Non-Organizational Users)**
FIA_USB.1	**User-Subject Binding** User-Subject Binding	AC-16 (3)	**Security Attributes** Maintenance Of Attribute Associations By Information System
FMT_MOF.1	**Management of Functions in TSF** Management of Security Functions Behavior	AC-3 (7)	**Access Enforcement** Role-Based Access Control
		AC-6	**Least Privilege**
		AC-6 (1)	**Least Privilege** Authorize Access To Security Functions
FMT_MSA.1	**Management of Security Attributes** Management of Security Attributes	AC-6	**Least Privilege**
		AC-6 (1)	**Least Privilege** Authorize Access To Security Functions
		AC-16 (2)	**Security Attributes** Attribute Value Changes By Authorized Individuals
		AC-16 (4)	**Security Attributes** Association of Attributes By Authorized Individuals
		AC-16 (10)	**Security Attributes** Attribute Configuration By Authorized Individuals

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
FMT_MSA.2	**Management of Security Attributes** Secure Security Attributes	AC-16	**Security Attributes**
		CM-6	**Configuration Settings**
		SI-10	**Information Input Validation**
FMT_MSA.3	**Management of Security Attributes** Static Attribute Initialization	No Mapping.	
FMT_MSA.4	**Management of Security Attributes** Security Attribute Value Inheritance	No Mapping.	
FMT_MTD.1	**Management of TSF Data** Management of TSF Data	AC-3 (7)	**Access Enforcement** Role-Based Access Control
		AC-6	**Least Privilege**
		AC-6 (1)	**Least Privilege** Authorize Access To Security Functions
		AU-6 (7)	**Audit Review, Analysis, and Reporting** Permitted Actions
		AU-9 (4)	**Protection of Audit Information** Access By Subset of Privileged Users
FMT_MTD.2	**Management of TSF Data** Management of Limits on TSF Data	AC-3 (7)	**Access Enforcement** Role-based Access Control
		AC-6	**Least Privilege**
		AC-6 (1)	**Least Privilege** Authorize Access To Security Functions
FMT_MTD.3	**Management of TSF Data** Secure TSF Data	SI-10	**Information Input Validation**
FMT_REV.1	**Revocation** Revocation	AC-3 (7)	**Access Enforcement** Rose-based Access Control
		AC-3 (8)	**Access Enforcement** Revocation Of Access Authorizations
		AC-6	**Least Privilege**
		AC-6 (1)	**Least Privilege** Authorize Access To Security Functions
FMT_SAE.1	**Security Attribute Expiration** Time-Limited Authorization	AC-3 (7)	**Access Enforcement** Role-based Access Control
		AC-6	**Least Privilege**
		AC-6 (1)	**Least Privilege** Authorize Access To Security Functions
FMT_SMF.1	**Specification of Management Functions** Specification of Management Functions	No Mapping.	
FMT_SMR.1	**Security Management Roles** Security Roles	AC-2 (7)	**Account Management** Role-based schemes
		AC-3 (7)	**Access Enforcement** Role-Based Access Control
		AC-5	**Separation of Duties**
		AC-6	**Least Privilege**
FMT_SMR.2	**Security Management Roles** Restrictions on Security Roles	AC-2 (7)	**Account Management** Role-based schemes
		AC-3 (7)	**Access Enforcement** Role-Based Access Control
		AC-5	**Separation of Duties**

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
		AC-6	**Least Privilege**
FMT_SMR.3	**Security Management Roles** Assuming Roles	AC-6 (1)	**Least Privilege** Authorized Access to Security Functions
		AC-6 (2)	**Least Privilege** Non-Privileged Access For Nonsecurity Functions
FPR_ANO.1	**Anonymity** Anonymity	No Mapping.	
FPR_ANO.2	**Anonymity** Anonymity Without Soliciting Information	No Mapping.	
FPR_PSE.1	**Pseudonymity** Pseudonymity	No Mapping.	
FPR_PSE.2	**Pseudonymity** Reversible Pseudonymity	No Mapping.	
FPR_PSE.3	**Pseudonymity** Alias Pseudonymity	No Mapping.	
FPR_UNL.1	**Unlinkability** Unlinkability	No Mapping.	
FPR_UNO.1	**Unobservability** Unobservability	No Mapping.	
FPR_UNO.2	**Unobservability** Allocation of Information Impacting Unobservability	No Mapping.	
FPR_UNO.3	**Unobservability** Unobservability Without Soliciting Information	No Mapping.	
FPR_UNO.4	**Unobservability** Authorized User Observability	No Mapping.	
FPT_FLS.1	**Fail Secure** Failure with Preservation of Secure State	SC-7 (18)	**Boundary Protection** Fail Secure
		SC-24	**Fail in Known State**
FPT_ITA.1	**Availability of Exported TSF Data** Inter-TSF Availability within a Defined Availability Metric	CP-10	**Information System Recovery And Reconstitution** Restore Within Time Period
		SC-5	**Denial of Service Protection**
		SC-5 (2)	**Denial of Service Protection** Excess Capacity/Bandwidth/Redundancy
		SC-5 (3)	**Denial of Service Protection** Detection/Monitoring
FPT_ITC.1	**Confidentiality of Exported TSF Data** Inter-TSF Confidentiality During Transmission	SC-8	**Transmission Confidentiality and Integrity**
		SC-8 (1)	**Transmission Confidentiality and Integrity** Cryptographic Or Alternate Physical Protection
FPT_ITI.1	**Integrity of Exported TSF Data** Inter-TSF Detection of Modification	SC-8	**Transmission Confidentiality and Integrity**
		SC-8 (1)	**Transmission Confidentiality and Integrity** Cryptographic Or Alternate Physical Protection
		SI-7	**Software, Firmware, and Information Integrity**
		SI-7 (1)	**Software, Firmware, and Information Integrity** Integrity Scans

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
		SI-7 (5)	**Software, Firmware, and Information Integrity** Automated Response to Integrity Violations
		SI-7 (6)	**Software, Firmware, and Information Integrity** Cryptographic Protection
FPT_ITI.2	**Integrity of Exported TSF Data** Inter-TSF Detection and Correction of Modification	SC-8	**Transmission Confidentiality and Integrity**
		SC-8 (1)	**Transmission Confidentiality and Integrity** Cryptographic Or Alternate Physical Protection
		SI-7	**Software, Firmware, and Information Integrity**
		SI-7 (1)	**Software, Firmware, and Information Integrity** Integrity Scans
		SI-7 (5)	**Software, Firmware, and Information Integrity** Automated Response to Integrity Violations
		SI-7 (6)	**Software, Firmware, and Information Integrity** Cryptographic Protection
FPT_ITT.1	**Internal TOE TSF Data Transfer** Basic Internal TSF Data Transfer Protection	SC-8	**Transmission Confidentiality and Integrity**
		SC-8 (1)	**Transmission Confidentiality and Integrity** Cryptographic Or Alternate Physical Protection
FPT_ITT.2	**Internal TOE TSF Data Transfer** TSF Data Transfer Separation	AC-4 (21)	**Information Flow Enforcement** Physical / Logical Separation Of Information Flows
		SC-8	**Transmission Confidentiality and Integrity**
		SC-8 (1)	**Transmission Confidentiality and Integrity** Cryptographic Or Alternate Physical Protection
FPT_ITT.3	**Internal TOE TSF Data Transfer** TSF Data Integrity Monitoring	SI-7	**Software, Firmware, and Information Integrity**
		SI-7 (1)	**Software, Firmware, and Information Integrity** Integrity Scans
		SI-7 (5)	**Software, Firmware, and Information Integrity** Automated Response to Integrity Violations
		SI-7 (6)	**Software, Firmware, and Information Integrity** Cryptographic Protection
FPT_PHP.1	**TSF Physical Protection** Passive Detection of Physical Attack	PE-3 (5)	**Physical Access Control** Tamper Protection
		PE-6 (2)	**Monitoring Physical Access** Automated Intrusion Recognition / Responses
		SA-18	**Tamper Resistance and Detection**
FPT_PHP.2	**TSF Physical Protection** Notification of Physical Attack	PE-3 (5)	**Physical Access Control** Tamper Protection
		PE-6 (2)	**Monitoring Physical Access** Automated Intrusion Recognition / Responses
		SA-18	**Tamper Resistance and Detection**
FPT_PHP.3	**TSF Physical Protection** Resistance to Physical Attack	PE-3 (5)	**Physical Access Control** Tamper Protection

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
		SA-18	**Tamper Resistance and Detection**
FPT_RCV.1	**Trusted Recovery** Manual Recovery	CP-10	**Information System Recovery and Reconstitution**
		CP-12	**Safe Mode**
FPT_RCV.2	**Trusted Recovery** Automated Recovery	CP-10	**Information System Recovery and Reconstitution**
		CP-12	**Safe Mode**
FPT_RCV.3	**Trusted Recovery** Automated Recovery Without Undue Loss	CP-10	**Information System Recovery and Reconstitution**
		CP-12	**Safe Mode**
FPT_RCV.4	**Trusted Recovery** Function Recovery	SI-6	**Security Function Verification**
		SI-10 (3)	**Information Input Validation** Predictable Behavior
		SC-24	**Fail in Known State**
FPT_RPL.1	**Replay Detection** Replay Detection	IA-2 (8)	**Identification and Authentication (Organizational Users)** Network Access To Privileged Accounts - Replay Resistant
		IA-2 (9)	**Identification and Authentication (Organizational Users)** Network Access To Non-Privileged Accounts - Replay Resistant
		SC-23	**Session Authenticity**
		SI-3 (9)	**Malicious Code Protection** Authenticate Remote Commands
FPT_SSP.1	**State Synchrony Protocol** Simple Trusted Acknowledgement	No Mapping.	
FPT_SSP.2	**State Synchrony Protocol** Mutual Trusted Acknowledgement	No Mapping.	
FPT_STM.1	**Time Stamps** Reliable Time Stamps	AU-8	**Time Stamps**
FPT_TDC.1	**Inter-TSF TSF Data Consistency** Inter-TSF Basic Data Consistency	AC-16 (7)	**Security Attributes** | Consistent Attribute Interpretation
		AC-16 (8)	**Security Attributes** Association Techniques/Technologies
FPT_TEE.1	**Testing of External Entities** Testing of External Entities	SI-6	**Security Functionality Verification**
FPT_TRC.1	**Internal TOE TSF Data Replication Consistency** Internal TSF Consistency	SI-7	**Software, Firmware, and Information Integrity**
FPT_TST.1	**TSF Self Test** TSF Testing	SI-6	**Security Functionality Verification**
		SI-7	**Software, Firmware, and Information Integrity**
FRU_FLT.1	**Fault Tolerance** Degraded Fault Tolerance	AU-15	**Alternate Audit Capability**
		CP-11	**Alternate Communications Protocols**
		SC-24	**Fail in Known State**
		SI-13	**Predictable Failure Prevention**
		SI-13 (1)	**Predictable Failure Prevention** Transferring Component Responsibilities

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
		SI-13 (2)	**Predictable Failure Prevention** Time Limit on Process Execution Without Supervision
		SI-13 (3)	**Predictable Failure Prevention** Manual Transfer Between Components
		SI-13 (4)	**Predictable Failure Prevention** Standby Component Installation/Notification
		SI-13 (5)	**Predictable Failure Prevention** Failover Capability
FRU_FLT.2	**Fault Tolerance** Limited Fault Tolerance	AU-15	**Alternate Audit Capability**
		CP-11	**Alternate Communications Protocols**
		SC-24	**Fail in Known State**
		SI-13	**Predictable Failure Prevention**
		SI-13 (1)	**Predictable Failure Prevention** Transferring Component Responsibilities
		SI-13 (2)	**Predictable Failure Prevention** Time Limit on Process Execution Without Supervision
		SI-13 (3)	**Predictable Failure Prevention** Manual Transfer Between Components
		SI-13 (4)	**Predictable Failure Prevention** Standby Component Installation/Notification
		SI-13 (5)	**Predictable Failure Prevention** Failover Capability
FRU_PRS.1	**Priority of Service** Limited Priority of Service	SC-6	**Resource Availability**
FRU_PRS.2	**Priority of Service** Full Priority of Service	SC-6	**Resource Availability**
FRU_RSA.1	**Resource Allocation** Maximum Quotas	SC-6	**Resource Availability**
FRU_RSA.2	**Resource Allocation** Minimum and Maximum Quotas	SC-6	**Resource Availability**
FTA_LSA.1	**Limitation on Scope of Selectable Attributes** Limitation on Scope of Selectable Attributes	AC-2 (6)	**Account Management** Dynamic Privilege Management
		AC-2 (11)	**Account Management** Usage Conditions
FTA_MCS.1	**Limitation on Multiple Concurrent Sessions** Basic Limitation on Multiple Concurrent Sessions	AC-10	**Concurrent Session Control**
FTA_MCS.2	**Limitation on Multiple Concurrent Sessions** Per-User Limitation on Multiple Concurrent Sessions	AC-10	**Concurrent Session Control**
FTA_SSL.1	**Session Locking and Termination** TSF-Initiated Session Locking	AC-11	**Session Lock**
		AC-11 (1)	**Session Lock** Pattern-Hiding Displays
FTA_SSL.2	**Session Locking and Termination** User-Initiated Locking	AC-11	**Session Lock**
		AC-11 (1)	**Session Lock** Pattern-Hiding Displays

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
FTA_SSL.3	**Session Locking and Termination** TSF-Initiated Termination	AC-12	**Session Termination**
		SC-10	**Network Disconnect**
FTA_SSL.4	**Session Locking and Termination** User-Initiated Termination	AC-12 (1)	**Session Termination** User-Initiated Logouts / Message Displays
FTA_TAB.1	**TOE Access Banners** Default TOE Access Banners	AC-8	**System Use Notification**
FTA_TAH.1	**TOE Access History** TOE Access History	AC-9	**Previous Login (Access) Notification**
		AC-9 (1)	**Previous Login (Access) Notification** Unsuccessful Logons
FTA_TSE.1	**TOE Session Establishment** TOE Session Establishment	AC-2 (11)	**Account Management** Usage Conditions
FTP_ITC.1	**Inter-TSF Trusted Channel** Inter-TSF Trusted Channel	IA-3 (1)	**Device Identification and Authentication** Cryptographic Bidirectional Authentication
		SC-8	**Transmission Confidentiality and Integrity**
		SC-8 (1)	**Transmission Confidentiality and Integrity** Cryptographic or Alternate Physical Protection
FTP_TRP.1	**Trusted Path** Trusted Path	SC-11	**Trusted Path**
Assurance Requirements			
ASE_INT.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**ST Introduction** ST Introduction	SA-4	**Acquisition Process**
ASE_CCL.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Conformance Claims** Conformance Claims	PL-2	**System Security Plan**
		SA-4 (7)	**Acquisition Process** NIAP-Approved Protection Profiles
ASE_SPD.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Security Problem Definition** Security Problem Definition	PL-2	**System Security Plan**
		SA-4	**Acquisition Process**
ASE_OBJ.1 EAL1	**Security Objectives** Security Objectives for the Operational Environment	PL-2	**System Security Plan**
		SA-4	**Acquisition Process**
ASE_OBJ.2 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Security Objectives** Security Objectives	PL-2	**System Security Plan**
		SA-4	**Acquisition Process**

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
ASE_ECD.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Extended Components Definition** Extended Components Definition	No Mapping.	
ASE_REQ.1 EAL1	**Security Requirements** Stated Security Requirements	PL-2	**System Security Plan**
		SA-4	**Acquisition Process**
ASE_REQ.2 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Security Requirements** Derived Security Requirements	PL-2	**System Security Plan**
		SA-4	**Acquisition Process**
ASE_TSS.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**TOE Summary Specification** TOE Summary Specification	PL-2	**System Security Plan**
		SA-4 (1)	**Acquisition Process** Functional Properties of Security Controls
ASE_TSS.2	**TOE Summary Specification** TOE Summary Specification with Architectural Design Summary	PL-2	**System Security Plan**
		SA-4 (1)	**Acquisition Process** Functional Properties of Security Controls
		SA-4 (2)	**Acquisition Process** Design / Implementation Information For Security Controls
		SA-17	**Developer Security Architecture and Design**
ADV_ARC.1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Security Architecture** Security Architecture Description	AC-25	**Reference Monitor**
		SA-17	**Developer Security Architecture and Design**
		SA-18	**Tamper Resistance and Detection**
		SC-3	**Security Function Isolation**
		SC-3 (1)	**Security Function Isolation** Hardware Separation
		SC-3 (2)	**Security Function Isolation** Minimize Nonsecurity Functionality
		SC-41	**Process Isolation**
ADV_FSP.1 EAL1	**Functional Specification** Basic Functional Specification	SA-4 (1)	**Acquisition Process** Functional Properties of Security Controls
		SA-4 (2)	**Acquisition Process** Design / Implementation Information for Security Controls
ADV_FSP.2 EAL2	**Functional Specification** Security-Enforcing Functional Specification	SA-4 (1)	**Acquisition Process** Functional Properties of Security Controls
		SA-4 (2)	**Acquisition Process** Design / Implementation Information for Security Controls

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
		SA-17 (4)	**Developer Security Architecture and Design** Informal Correspondence
ADV_FSP.3 EAL3	**Functional Specification** Functional Specification With Complete Summary	SA-4 (1)	**Acquisition Process** Functional Properties of Security Controls
		SA-4 (2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17 (4)	**Developer Security Architecture and Design** Informal Correspondence
ADV_FSP.4 EAL4	**Functional Specification** Complete Functional Specification	SA-4 (1)	**Acquisition Process** Functional Properties of Security Controls
		SA-4 (2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17 (4)	**Developer Security Architecture and Design** Informal Correspondence
ADV_FSP.5 EAL5 EAL6	**Functional Specification** Complete Semi-Formal Functional Specification with Additional Error Information	SA-4 (1)	**Acquisition Process** Functional Properties of Security Controls
		SA-4 (2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17 (4)	**Developer Security Architecture and Design** Informal Correspondence
ADV_FSP.6 EAL7	**Functional Specification** Complete Semi-Formal Functional Specification with Additional Formal Specification	SA-4 (1)	**Acquisition Process** Functional Properties of Security Controls
		SA-4 (2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17 (3)	**Developer Security Architecture and Design** Formal Correspondence
		SA-17 (4)	**Developer Security Architecture and Design** Informal Correspondence
ADV_IMP.1 EAL4 EAL5	**Implementation Representation** Implementation Representation of the TSF	SA-4 (2)	**Acquisition Process** Design / Implementation Information for Security Controls
ADV_IMP.2 EAL6 EAL7	**Implementation Representation** Complete Mapping of the Implementation Representation of the TSF	SA-4 (2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17 (3)	**Developer Security Architecture and Design** Formal Correspondence
ADV_INT.1	**TSF Internals** Well-Structured Subset of TSF Internals	SA-8	**Security Engineering Principles**
		SC-3 (3)	**Security Function Isolation** Minimize Nonsecurity Functionality
		SC-3 (4)	**Security Function Isolation** Module Coupling and Cohesiveness
		SC-3 (5)	**Security Function Isolation** Layered Structures

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
ADV_INT.2 EAL5	**TSF Internals** Well-Structured Internals	SA-8	**Security Engineering Principles**
		SC-3 (3)	**Security Function Isolation** Minimize Nonsecurity Functionality
		SC-3 (4)	**Security Function Isolation** Module Coupling and Cohesiveness
		SC-3 (5)	**Security Function Isolation** Layered Structures
ADV_INT.3 EAL6 EAL7	**TSF Internals** Minimally Complex Internals	SA-8	**Security Engineering Principles**
		SA-17 (5)	**Developer Security Architecture and Design** Conceptually Simple Design
		SC-3 (3)	**Security Function Isolation** Minimize Nonsecurity Functionality
		SC-3 (4)	**Security Function Isolation** Module Coupling and Cohesiveness
		SC-3 (5)	**Security Function Isolation** Layered Structures
		AC-25	**Reference Monitor**
ADV_SPM.1 EAL6 EAL7	**Security Policy Modeling** Formal TOE Security Policy Model	SA-17 (1)	**Developer Security Architecture and Design** Formal Policy Model
		SA-17 (3)	**Developer Security Architecture and Design** Formal Correspondence
ADV_TDS.1 EAL2	**TOE Design** Basic Design	SA-4 (2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17	**Developer Security Architecture and Design**
ADV_TDS.2 EAL3	**TOE Design** Architectural Design	SA-4 (2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17	**Developer Security Architecture and Design**
ADV_TDS.3 EAL4	**TOE Design** Basic Modular Design	SA-4 (2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17	**Developer Security Architecture and Design**
ADV_TDS.4 EAL5	**TOE Design** Semiformal Modular Design	SA-4 (2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17	**Developer Security Architecture and Design**
		SA-17 (2)	**Developer Security Architecture and Design** Security Relevant Components
		SA-17 (4)	**Developer Security Architecture and Design** Informal Correspondence

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
ADV_TDS.5 EAL6	**TOE Design** Complete Semiformal Modular Design	SA-4 (2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17	**Developer Security Architecture and Design**
		SA-17 (2)	**Developer Security Architecture and Design** Security Relevant Components
		SA-17 (4)	**Developer Security Architecture and Design** Informal Correspondence
ADV_TDS.6 EAL7	**TOE Design** Complete Semiformal Modular Design with Formal High-Level Design Presentation	SA-4 (2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17	**Developer Security Architecture and Design**
		SA-17 (2)	**Developer Security Architecture and Design** Security Relevant Components
		SA-17 (3)	**Developer Security Architecture and Design** Formal Correspondence
		SA-17 (4)	**Developer Security Architecture and Design** Informal Correspondence
AGD_OPE.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Operational User Guidance** Operational User Guidance	SA-5	**Information System Documentation**
AGD_PRE.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Preparative Procedures** Preparative Procedures	SA-5	**Information System Documentation**
ALC_CMC.1 EAL1	**CM Capabilities** Labeling of the TOE	CM-9	**Configuration Management Plan**
		SA-10	**Developer Configuration Management**
ALC_CMC.2 EAL2	**CM Capabilities** Use of a CM System	CM-9	**Configuration Management Plan**
		SA-10	**Developer Configuration Management**
ALC_CMC.3 EAL3	**CM Capabilities** Authorization Controls	CM-3	**Configuration Change Control**
		CM-9	**Configuration Management Plan**
		SA-10	**Developer Configuration Management**
ALC_CMC.4 EAL4 EAL5	**CM Capabilities** Production Support, Acceptance Procedures, and Automation	CM-3	**Configuration Change Control**
		CM-3 (1)	**Configuration Change Control** Automated Document / Notification / Prohibition of Changes
		CM-3 (3)	**Configuration Change Control** Automated Change Implementation
		CM-9	**Configuration Management Plan**

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
		SA-10	**Developer Configuration Management**
ALC_CMC.5 EAL6 EAL7	**CM Capabilities** Advanced Support	CM-3	**Configuration Change Control**
		CM-3 (1)	**Configuration Change Control** Automated Document / Notification / Prohibition of Changes
		CM-3 (2)	**Configuration Change Control** Test / Validate / Document Changes
		CM-3 (3)	**Configuration Change Control** Automated mechanisms to field and deploy
		CM-9	**Configuration Management Plan**
		SA-10	**Developer Configuration Management**
ALC_CMS.1 EAL1	**CM Scope** TOE CM Coverage	CM-9	**Configuration Management Plan**
		SA-10	**Developer Configuration Management**
ALC_CMS.2 EAL2	**CM Scope** Parts of the TOE CM Coverage	CM-9	**Configuration Management Plan**
		SA-10	**Developer Configuration Management**
ALC_CMS.3 EAL3	**CM Scope** Implementation Representation CM Coverage	CM-9	**Configuration Management Plan**
		SA-10	**Developer Configuration Management**
ALC_CMS.4 EAL4	**CM Scope** Problem Tracking CM Coverage	CM-9	**Configuration Management Plan**
		SA-10	**Developer Configuration Management**
ALC_CMS.5 EAL5 EAL6 EAL7	**CM Scope** Development Tools CM Coverage	CM-9	**Configuration Management Plan**
		SA-10	**Developer Configuration Management**
ALC_DEL.1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Delivery** Delivery Procedures	MP-5	**Media Transport**
		SA-10 (1)	**Developer Configuration Management** Software / Firmware Integrity Verification
		SA-10 (6)	**Developer Configuration Management** Trusted Distribution
		SA-18	**Tamper Resistance and Detection**
		SA-19	**Component Authenticity**
ALC_DVS.1 EAL3 EAL4 EAL5	**Development Security** Identification of Security Measures	SA-1	**System and Services Acquisition Policy and Procedures**
		SA-3	**System Development Lifecycle**
		SA-12	**Supply Chain Protection**
ALC_DVS.2 EAL6 EAL7	**Development Security** Sufficiency of Security Measures	CM-5	**Access Restrictions for Change**
		SA-3	**System Development Lifecycle**
		SA-12	**Supply Chain Protection**
ALC_FLR.1	**Flaw Remediation** Basic Flaw Remediation	SA-10	**Developer Configuration Management**
		SA-11	**Developer Security Testing / Evaluation**
		SI-2	**Flaw Remediation**
ALC_FLR.2	**Flaw Remediation** Flaw Reporting Procedures	SA-10	**Developer Configuration Management**
		SA-11	**Developer Security Testing / Evaluation**
		SI-2	**Flaw Remediation**
ALC_FLR.3	**Flaw Remediation** Systematic Flaw Remediation	SA-10	**Developer Configuration Management**
		SA-11	**Developer Security Testing / Evaluation**
		SI-2	**Flaw Remediation**

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
ALC_LCD.1 EAL3 EAL4 EAL5 EAL6	**Life-Cycle Definition** Developer Defined Life-Cycle Model	SA-3	**System Development Life Cycle**
		SA-15	**Development Process, Standards, and Tools**
ALC_LCD.2 EAL7	**Life-Cycle Definition** Measurable Life-Cycle Model	SA-3	**System Development Life Cycle**
		SA-15	**Development Process, Standards, and Tools**
ALC_TAT.1 EAL4	**Tools and Techniques** Well-Defined Development Tools	SA-15	**Development Process, Standards, and Tools**
ALC_TAT.2 EAL5	**Tools and Techniques** Compliance with Implementation Standards	SA-15	**Development Process, Standards, and Tools**
ALC_TAT.3 EAL6 EAL7	**Tools and Techniques** Compliance with Implementation Standards – All Parts	SA-15	**Development Process, Standards, and Tools**
ATE_COV.1 EAL2	**Coverage** Evidence of Coverage	SA-11	**Developer Security Testing and Evaluation**
		SA-11 (7)	**Developer Security Testing and Evaluation** *Verify Scope of Testing / Evaluation*
ATE_COV.2 EAL3 EAL4 EAL5	**Coverage** Analysis of Coverage	SA-11	**Developer Security Testing and Evaluation**
		SA-11 (7)	**Developer Security Testing and Evaluation** *Verify Scope of Testing / Evaluation*
ATE_COV.3 EAL6 EAL7	**Coverage** Rigorous Analysis of Coverage	SA-11	**Developer Security Testing and Evaluation**
		SA-11 (7)	**Developer Security Testing and Evaluation** *Verify Scope of Testing / Evaluation*
ATE_DPT.1 EAL3	**Depth** Testing: Basic Design	SA-11	**Developer Security Testing and Evaluation**
		SA-11 (7)	**Developer Security Testing and Evaluation** *Verify Scope of Testing / Evaluation*
ATE_DPT.2 EAL4	**Depth** Testing: Security Enforcing Modules	SA-11	**Developer Security Testing and Evaluation**
		SA-11 (7)	**Developer Security Testing and Evaluation** *Verify Scope of Testing / Evaluation*
ATE_DPT.3 EAL5 EAL6	**Depth** Testing: Modular Design	SA-11	**Developer Security Testing and Evaluation**
		SA-11 (7)	**Developer Security Testing and Evaluation** *Verify Scope of Testing / Evaluation*
ATE_DPT.4 EAL7	**Depth** Testing: Implementation Representation	SA-11	**Developer Security Testing and Evaluation**
		SA-11 (7)	**Developer Security Testing and Evaluation** *Verify Scope of Testing / Evaluation*
ATE_FUN.1 EAL2 EAL3 EAL4 EAL5	**Functional Tests** Functional Testing	SA-11	**Developer Security Testing and Evaluation**
ATE_FUN.2 EAL6 EAL7	**Functional Tests** Ordered Functional Testing	SA-11	**Developer Security Testing and Evaluation**
ATE_IND.1 EAL1	**Independent Testing** Independent Testing – Conformance	CA-2	**Security Assessments**
		CA-2 (1)	**Security Assessments** *Independent Assessors*
		SA-11 (3)	**Developer Security Testing and Evaluation** *Independent Verification of Assessment Plans / Evidence*

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
ATE_IND.2 EAL2 EAL3 EAL4 EAL5 EAL6	**Independent Testing** Independent Testing – Sample	CA-2	**Security Assessments**
		CA-2 (1)	**Security Assessments** *Independent Assessors*
		SA-11 (3)	**Developer Security Testing and Evaluation** *Independent Verification of Assessment Plans / Evidence*
ATE_IND.3 EAL7	**Independent Testing** Independent Testing – Complete	CA-2	**Security Assessments**
		CA-2 (1)	**Security Assessments** *Independent Assessors*
		SA-11 (3)	**Developer Security Testing and Evaluation** *Independent Verification of Assessment Plans / Evidence*
AVA_VAN.1 EAL1	**Vulnerability Analysis** Vulnerability Survey	CA-2 (2)	**Security Assessments** *Specialized Assessments*
		CA-8	**Penetration Testing**
		RA-3	**Risk Assessment**
		SA-11 (2)	**Developer Security Testing and Evaluation** *Threat And Vulnerability Analyses / Flaw Remediation*
		SA-11 (5)	**Developer Security Testing and Evaluation** *Penetration Testing*
AVA_VAN.2 EAL2 EAL3	**Vulnerability Analysis** Vulnerability Analysis	CA-2 (2)	**Security Assessments** *Specialized Assessments*
		CA-8	**Penetration Testing**
		RA-3	**Risk Assessment**
		SA-11 (2)	**Developer Security Testing and Evaluation** *Threat And Vulnerability Analyses / Flaw Remediation*
		SA-11 (5)	**Developer Security Testing and Evaluation** *Penetration Testing*
AVA_VAN.3 EAL4	**Vulnerability Analysis** Focused Vulnerability Analysis	CA-2 (2)	**Security Assessments** *Specialized Assessments*
		CA-8	**Penetration Testing**
		RA-3	**Risk Assessment**
		SA-11 (2)	**Developer Security Testing and Evaluation** *Threat And Vulnerability Analyses / Flaw Remediation*
		SA-11 (5)	**Developer Security Testing and Evaluation** *Penetration Testing*
AVA_VAN.4 EAL5	**Vulnerability Analysis** Methodical Vulnerability Analysis	CA-2 (2)	**Security Assessments** *Types of Assessments*
		CA-8	**Penetration Testing**
		RA-3	**Risk Assessment**
		SA-11 (2)	**Developer Security Testing and Evaluation** *Threat And Vulnerability Analyses / Flaw Remediation*
		SA-11 (5)	**Developer Security Testing and Evaluation** *Penetration Testing*
AVA_VAN.5 EAL6 EAL7	**Vulnerability Analysis** Advanced Methodical Vulnerability Analysis	CA-2 (2)	**Security Assessments** *Types of Assessments*
		CA-8	**Penetration Testing**
		RA-3	**Risk Assessment**

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
		SA-11 (2)	**Developer Security Testing and Evaluation** *Threat And Vulnerability Analyses / Flaw Remediation*
		SA-11 (5)	**Developer Security Testing and Evaluation** *Penetration Testing*
ACO_COR.1	**Composition Rationale** Composition Rationale	SA-17	**Developer Security Architecture and Design**
ACO_DEV.1	**Development Evidence** Functional Description	SA-17	**Developer Security Architecture and Design**
ACO_DEV.2	**Development Evidence** Basic Evidence of Design	SA-17	**Developer Security Architecture and Design**
ACO_DEV.3	**Development Evidence** Detailed Evidence of Design	SA-17	**Developer Security Architecture and Design**
ACO_REL.1	**Reliance on Dependent Component** Basic Reliance Information	SA-17	**Developer Security Architecture and Design**
ACO_REL.2	**Reliance on Dependent Component** Reliance Information	SA-17	**Developer Security Architecture and Design**
ACO_CTT.1	**Composed TOE Testing** Interface Testing	SA-11	**Developer Security Testing and Evaluation**
ACO_CTT.2	**Composed TOE Testing** Rigorous Interface Testing	SA-11	**Developer Security Testing and Evaluation**
ACO_VUL.1	**Composition Vulnerability Analysis** Composition Vulnerability Review	CA-2	**Security Assessments**
		CA-8	**Penetration Testing**
		RA-3	**Risk Assessment**
		SA-11	**Developer Security Testing and Evaluation**
ACO_VUL.2	**Composition Vulnerability Analysis** Composition Vulnerability Analysis	CA-2	**Security Assessments**
		CA-8	**Penetration Testing**
		RA-3	**Risk Assessment**
		SA-11	**Developer Security Testing and Evaluation**
ACO_VUL.3	**Composition Vulnerability Analysis** Enhanced-Basic Composition Vulnerability Review	CA-2	**Security Assessments**
		CA-8	**Penetration Testing**
		RA-3	**Risk Assessment**
		SA-11	**Developer Security Testing and Evaluation**

APPENDIX I

OVERLAY TEMPLATE

APPLYING TAILORING GUIDANCE FOR SPECIAL CONDITIONS OR COMMUNITY-WIDE USE[116]

Organizations may use the following template when developing tailored baselines using the concept of overlays.[117] The template is provided as an example only—organizations may choose to use other formats or modify the format in this appendix based on organizational needs and the type of overlay being developed. The level of detail included in the overlay is at the discretion of the organization initiating the overlay but should be of sufficient breadth and depth to provide an appropriate rationale and justification for the resulting tailored baseline developed, including any risk-based decisions made during the overlay development process. Security control baseline tailoring using the concept of overlays results in security plans that are subject to approval by authorizing officials. The example template consists of eight sections:

- Identification;
- Overlay Characteristics;
- Applicability;
- Overlay Summary;
- Detailed Overlay Control Specifications;
- Tailoring Considerations;
- Definitions; and
- Additional Information or Instructions.

How Overlays Can Be Used

Within the Risk Management Framework (RMF), overlays are implemented as part of the tailoring process after the completion of an initial security categorization process described in Section 3.1 and any organization-specific guidance. The security categorization process results in the determination of an *impact level* of the information system, and is subsequently used to select an initial set of security controls from one of the security control baselines in Appendix D.[118] After the initial set of security controls is identified, organizations initiate the tailoring process to modify and align the controls more closely with the specific conditions within the organizations. Overlays provide tailoring guidance from a community-wide perspective to address specialized requirements, missions/business functions, technologies, or environments of operation. Overlays provide uniformity and efficiency of security control selection by presenting tailoring options

[116] Tailored baselines produced using the concept of *overlays* can be published independently in a variety of venues and publications including, for example, OMB policies, CNSS Instructions, NIST Special Publications, industry standards, and sector-specific guidance. As part of the overlay initiative, the previous guidance in Appendix I regarding industrial and process control system security will be transferred to NIST Special Publication 800-82.

[117] While organizations are encouraged to use the overlay concept to tailor security control baselines, generating widely divergent overlays on the same topic may prove to be counterproductive. The overlay concept is most effective when communities of interest work together to create consensus-based overlays that are not duplicative.

[118] CNSS Instruction 1253 provides security categorization guidance and security control baselines for national security systems.

developed by security experts and other subject matter experts to information system owners responsible for implementing and maintaining such systems.

There is a considerable range of options that can be used to construct overlays, depending on the specificity desired by the overlay developers. Some overlays may be very specific with respect to the hardware, firmware, and software that form the key components the information system and the environment in which the system operates. Other overlays may be more abstract in order to be applicable to a large class of information systems that may be deployed in different environments. The example template described below can be used for any level of specificity on this continuum of potential options for overlays.

Overlays that provide *greater specificity* are typically developed by organizations with authority over the information system owners and environments of operation. Organizations decide on the appropriate tailoring actions for the selected baseline security controls as described in Section 3.2. Many of the variables and conditions that qualify the overlay for use on a specific information system are made explicit to ensure consistency when applying the overlay. Overlays that provide *less specificity* can also be developed by security and subject matter experts for application to large classes of information systems or in situations where there is less than full knowledge about the specific implementation details related to the system. Less specific overlays may require additional tailoring to customize the set of security controls for the specific information system. These overlays leave many of the assignment and selection statements in the security controls (i.e., the variable portion of the controls) to be completed by the organization that owns and operates the information system. The eight sections comprising the overlay are described below.

Identification

Organizations identify the overlay by providing: (i) a unique name for the overlay; (ii) a version number and date; (iii) the version of NIST Special Publication 800-53 used to create the overlay; (iv) other documentation used to create the overlay; (v) author or authoring group and point of contact; and (vi) type of organizational approval received. Organizations define how long the overlay is to be in effect and any events that may trigger an update to the overlay other than changes to NIST Special Publication 800-53 or organization-specific security guidance. If there are no unique events that can trigger an update for the overlay, this section provides that notation.

Overlay Characteristics

Organizations describe the characteristics that define the intended use of the overlay in order to help potential users select the most appropriate overlay for their missions/business functions. This may include, for example, a description of: (i) the environment in which the information system will be used (e.g., inside a guarded building within the continental United States, in an unmanned space vehicle, while traveling for business to a foreign country that is known for attempting to gain access to sensitive or classified information, or in a mobile vehicle that is in close proximity to hostile entities); (ii) the type of information that will be processed, stored, or transmitted (e.g., personal identity and authentication information, financial management information, facilities, fleet, and equipment management information, defense and national security information, system development information); (iii) the functionality within the information system or the type of system (e.g., standalone system, industrial/process control system, or cross-domain system); and (iv) other characteristics related to the overlay that help protect organizational missions/business functions, information systems, information, or individuals from a specific set of threats that may not be addressed by the assumptions described in Chapter Three.

Applicability

Organizations provide criteria to assist potential users of the overlay in determining whether or not the overlay applies to a particular information system or environment of operation. Typical formats include, for example, a list of questions or a decision tree based on the description of the characteristics of the information system (including associated applications) and its environment of operation at the level of specificity appropriate to the overlay.

Overlay Summary

Organizations provide a brief summary of the salient characteristics of the overlay. This summary may include, for example: (i) the security controls and control enhancements that are affected by the overlay; (ii) an indication of which controls/enhancements are selected or not selected based on the characteristics and assumptions in the overlay, the tailoring guidance provided in Section 3.2, or any organization-specific guidance; (iii) the selected controls/enhancements including an overview of new supplemental guidance and parameter values; and (iv) references to applicable laws, Executive Orders, directives, instructions, regulations, policies, or standards.

Detailed Overlay Control Specifications

Organizations provide a comprehensive expression of the security controls/control enhancements in the overlay as part of the tailoring process. This may include, for example: (i) justification for selecting or not selecting a specific security control/control enhancement; (ii) modifications to the supplemental guidance or the addition of new supplemental guidance for the security controls and control enhancements to address the characteristics of the overlay and the environments in which the overlay is intended to operate; (iii) unique parameter values for security control selection or assignment statements; (iv) specific statutory and/or regulatory requirements (above and beyond FISMA) that are met by a security control or control enhancement; (v) recommendations for compensating controls, as appropriate; and (vi) guidance that extends the basic capability of the control/enhancement by specifying additional functionality, altering the strength of mechanism, or adding or limiting implementation options.

Tailoring Considerations

Organizations provide information to information system owners and authorizing officials to consider during the tailoring process when determining the set of security controls applicable to their specific information systems. This is especially important for overlays that are used in an environment of operation different from the one assumed by the security control baselines (as defined in Section 3.1). In addition, organizations can provide guidance on the use of multiple overlays applied to a security control baseline and address any potential conflicts that may arise between overlay specifications and baseline controls.

Definitions

Organizations provide any terms and associated definitions that are unique and relevant to the overlay. The terms and definitions are listed in alphabetical order. If there are no unique terms or definitions for the overlay, this is stated in this section.

Additional Information or Instructions

Organizations provide any additional information or instructions relevant to the overlay not covered in the previous sections.

APPENDIX J

PRIVACY CONTROL CATALOG

PRIVACY CONTROLS, ENHANCEMENTS, AND SUPPLEMENTAL GUIDANCE

The need to protect an individual's privacy is as important today as it was in 1974 when the Privacy Act first sought to balance the government's need to collect information from an individual with a citizen's right to be notified as to how that information was being used, collected, maintained, and disposed of after the requisite period of use. These concerns are also shared in the private sector, where healthcare, financial, and other services continue to be delivered via the web with increasingly higher levels of personalization. The proliferation of social media, Smart Grid, mobile, and cloud computing, as well as the transition from structured to unstructured data and metadata environments, have added significant complexities and challenges for federal organizations in safeguarding privacy. These challenges extend well beyond the traditional information technology security view of protecting privacy which focused primarily on ensuring confidentiality. Now there are greater implications with respect to controlling the integrity of an individual's information, and with ensuring that an individual's information is available on demand. The challenging landscape requires federal organizations to expand their view of privacy, in order to meet citizen expectations of privacy that go beyond information security.

Privacy, with respect to personally identifiable information (PII),[119] is a core value that can be obtained only with appropriate legislation, policies, procedures, and associated controls to ensure compliance with requirements. Protecting the privacy of individuals and their PII that is collected, used, maintained, shared, and disposed of by programs and information systems, is a fundamental responsibility of federal organizations. Privacy also involves each individual's right to decide when and whether to share personal information, how much information to share, and the particular circumstances under which that information can be shared. In today's digital world, effective privacy for individuals depends on the safeguards employed within the information systems that are processing, storing, and transmitting PII and the environments in which those systems operate. Organizations cannot have effective privacy without a basic foundation of information security. Privacy is more than security, however, and includes, for example, the principles of transparency, notice, and choice.

This appendix provides a structured set of controls for protecting privacy and serves as a roadmap for organizations to use in identifying and implementing privacy controls concerning the entire life cycle of PII, whether in paper or electronic form. The controls focus on information privacy as a value distinct from, but highly interrelated with, information security. Privacy controls are

[119] OMB Memorandum 07-16 defines PII as information which can be used to distinguish or trace an individual's identity such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. OMB Memorandum 10-22 further states that "the definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified by examining the context of use and combination of data elements. In performing this assessment, it is important for agencies to recognize that non-PII can become PII, whenever additional information is made publicly available, in any medium and from any source that, when combined with other available information, could be used to identify an individual." NIST Special Publication 800-122 also includes a definition of PII that differs from this appendix because it was focused on the security objective of confidentiality and not privacy in the broad sense. Organizational definitions of PII may vary based on the consideration of additional regulatory requirements. The privacy controls in this appendix apply regardless of the definition of PII by organizations.

the administrative, technical, and physical safeguards employed within organizations to protect and ensure the proper handling of PII.[120] Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.

The privacy controls in this appendix are based on the Fair Information Practice Principles (FIPPs)[121] embodied in the Privacy Act of 1974, Section 208 of the E-Government Act of 2002, and Office of Management and Budget (OMB) policies. The FIPPs are designed to build public trust in the privacy practices of organizations and to help organizations avoid tangible costs and intangible damages from privacy incidents. There are eight privacy control families, each aligning with one of the FIPPs. The privacy families can be implemented at the organization, department, agency, component, office, program, or information system level, under the leadership and oversight of the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO)[122] and in coordination with the Chief Information Security Officer, Chief Information Officer, program officials, legal counsel, and others as appropriate. Table J-1 provides a summary of the privacy controls by family in the privacy control catalog.

TABLE J-1: SUMMARY OF PRIVACY CONTROLS BY FAMILY

ID	PRIVACY CONTROLS
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-6	Privacy Reporting
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal

[120] In 2010, the Federal CIO Council Privacy Committee issued a framework for designing and implementing a privacy program entitled *Best Practices: Elements of a Federal Privacy Program (Elements White Paper)*. The privacy controls in this appendix mirror a number of the elements included in the paper. Organizations can use the privacy controls and the guidance in the paper to develop an organization-wide privacy program or enhance an already existing program.

[121] The FIPPs are widely accepted in the United States and internationally as a general framework for privacy and are reflected in other federal and international laws and policies. In a number of organizations, FIPPs serve as the basis for analyzing privacy risks and determining appropriate mitigation strategies. The Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) also provided information and materials in development of the privacy controls.

[122] All federal agencies and departments designate an SAOP/CPO as the senior organizational official with the overall organization-wide responsibility for information privacy issues. OMB Memorandum 05-08 provides guidance for the designation of SAOPs/CPOs. The term SAOP/CPO as used in this appendix means an organization's senior privacy leader, whose job title may vary from organization to organization.

ID	PRIVACY CONTROLS
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

There is a strong similarity between the structure of the privacy controls in this appendix and the structure of the security controls in Appendices F and G. For example, the control AR-1 (Governance and Privacy Program) requires organizations to develop privacy plans that can be implemented at the organizational or program level. These plans can also be used in conjunction with security plans to provide an opportunity for organizations to select the appropriate set of security and privacy controls in accordance with organizational mission/business requirements and the environments in which the organizations operate. Incorporating the fundamental concepts associated with managing information security risk helps to ensure that the employment of privacy controls is carried out in a cost-effective and risk-based manner while simultaneously meeting compliance requirements. Standardized privacy controls and assessment procedures (developed to evaluate the effectiveness of the controls) will provide a more disciplined and structured approach for satisfying federal privacy requirements and demonstrating compliance with those requirements.

In summary, the Privacy Appendix achieves several important objectives. The appendix:

- Provides a structured set of privacy controls, based on best practices, that helps organizations comply with applicable federal laws, Executive Orders, directives, instructions, regulations, policies, standards, guidance, and organization-specific issuances;
- Establishes a linkage and relationship between privacy and security controls for purposes of enforcing respective privacy and security requirements that may overlap in concept and in implementation within federal information systems, programs, and organizations;
- Demonstrates the applicability of the NIST Risk Management Framework in the selection, implementation, assessment, and ongoing monitoring of privacy controls deployed in federal information systems, programs, and organizations; and
- Promotes closer cooperation between privacy and security officials within the federal government to help achieve the objectives of senior leaders/executives in enforcing the requirements in federal privacy legislation, policies, regulations, directives, standards, and guidance.

HOW TO USE THIS APPENDIX

The privacy controls outlined in this publication are primarily for use by an organization's Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) when working with program managers, mission/business owners, information owners/stewards, Chief Information Officers, Chief Information Security Officers, information system developers/integrators, and risk executives to determine how best to incorporate effective privacy protections and practices (i.e., privacy controls) within organizational programs and information systems and the environments in which they operate. The privacy controls facilitate the organization's efforts to comply with privacy requirements affecting those organizational programs and/or systems that collect, use, maintain, share, or dispose of personally identifiable information (PII) or other activities that raise privacy risks. While the security controls in Appendix F are allocated to the low, moderate, and high baselines in Appendix D, the privacy controls are selected and implemented based on the privacy requirements of organizations and the need to protect the PII of individuals collected and maintained by organizational information systems and programs, in accordance with federal privacy legislation, policies, directives, regulations, guidelines, and best practices.

Organizations analyze and apply each privacy control with respect to their distinct mission/business and operational needs based on their legal authorities and obligations. Implementation of the privacy controls may vary based upon this analysis (e.g., organizations that are defined as *covered entities* pursuant to the Health Insurance Portability and Accountability Act [HIPAA] may have additional requirements that are not specifically enumerated in this publication). This enables organizations to determine the information practices that are compliant with law and policy and those that may need review. It also enables organizations to tailor the privacy controls to meet their defined and specific needs at the organization level, mission/business process level, and information system level. Organizations with national security or law enforcement authorities take those authorities as well as privacy interests into account in determining how to apply the privacy controls in their operational environments. Similarly, organizations subject to the Confidential Information Protection and Statistical Efficiency Act (CIPSEA), implement the privacy controls consistent with that Act. All organizations implement the privacy controls consistent with the Privacy Act of 1974, 5 U.S.C. § 552a, subject to any exceptions and/or exemptions.

Privacy control enhancements described in Appendix J reflect best practices which organizations should strive to achieve, but are not mandatory. Organizations should decide when to apply control enhancements to support their particular missions/business functions. Specific *overlays* for privacy, developed in accordance with the guidance in Section 3.2 and Appendix I, can also be considered to facilitate the tailoring of the security control baselines in Appendix D with the requisite privacy controls to ensure that both security and privacy requirements can be satisfied by organizations. Many of the security controls in Appendix F provide the fundamental information protection for confidentiality, integrity, and availability within organizational information systems and the environments in which those systems operate—protection that is essential for strong and effective privacy.

Organizations document the agreed upon privacy controls to be implemented in organizational programs and information systems and the environments in which they operate. At the discretion of the implementing organization, privacy controls may be documented in a distinct privacy plan or incorporated into other risk management documents (e.g., system security plans). Organizations also establish appropriate assessment methodologies to determine the extent to which the privacy controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting designated privacy requirements. Organizational assessments of privacy controls can be conducted either by the SAOP/CPO alone or jointly with the other organizational risk management offices including the information security office.

Implementation Tip

- Select and implement privacy controls based on the privacy requirements of organizations and the need to protect the personally identifiable information (PII) of individuals collected and maintained by systems and programs.
- Coordinate privacy control selection and implementation with the organizational Risk Executive Function, mission/business owners, enterprise architects, Chief Information Officer, SAOP/CPO, and Chief Information Security Officer.
- View the privacy controls in Appendix J from the same perspective as the Program Management controls in Appendix G—that is, the controls are implemented for each organizational information system irrespective of the FIPS 199 categorization for that system.
- Select and implement the optional privacy control enhancements when there is a demonstrated need for additional privacy protection for individuals and PII.
- Apply the privacy controls consistent with any specific exceptions and exemptions included in legislation, Executive Orders, directives, policies, and regulations (e.g., law enforcement or national security considerations).

FAMILY: AUTHORITY AND PURPOSE

This family ensures that organizations: (i) identify the legal bases that authorize a particular personally identifiable information (PII) collection or activity that impacts privacy; and (ii) specify in their notices the purpose(s) for which PII is collected.

AP-1 AUTHORITY TO COLLECT

Control: The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need.

Supplemental Guidance: Before collecting PII, the organization determines whether the contemplated collection of PII is legally authorized. Program officials consult with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and legal counsel regarding the authority of any program or activity to collect PII. The authority to collect PII is documented in the System of Records Notice (SORN) and/or Privacy Impact Assessment (PIA) or other applicable documentation such as Privacy Act Statements or Computer Matching Agreements. Related controls: AR-2, DM-1, TR-1, TR-2.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (e); Section 208(c), E-Government Act of 2002 (P.L. 107-347); OMB Circular A-130, Appendix I.

AP-2 PURPOSE SPECIFICATION

Control: The organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.

Supplemental Guidance: Often, statutory language expressly authorizes specific collections and uses of PII. When statutory language is written broadly and thus subject to interpretation, organizations ensure, in consultation with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and legal counsel, that there is a close nexus between the general authorization and any specific collection of PII. Once the specific purposes have been identified, the purposes are clearly described in the related privacy compliance documentation, including but not limited to Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), and Privacy Act Statements provided at the time of collection (e.g., on forms organizations use to collect PII). Further, in order to avoid unauthorized collections or uses of PII, personnel who handle PII receive training on the organizational authorities for collecting PII, authorized uses of PII, and on the contents of the notice. Related controls: AR-2, AR-4, AR-5, DM-1, DM-2, TR-1, TR-2, UL-1, UL-2.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3)(A)-(B); Sections 208(b), (c), E-Government Act of 2002 (P.L. 107-347).

FAMILY: ACCOUNTABILITY, AUDIT, AND RISK MANAGEMENT

This family enhances public confidence through effective controls for governance, monitoring, risk management, and assessment to demonstrate that organizations are complying with applicable privacy protection requirements and minimizing overall privacy risk.

AR-1 GOVERNANCE AND PRIVACY PROGRAM

Control: The organization:

a. Appoints a Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and information systems;

b. Monitors federal privacy laws and policy for changes that affect the privacy program;

c. Allocates [*Assignment: organization-defined allocation of budget and staffing*] sufficient resources to implement and operate the organization-wide privacy program;

d. Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures;

e. Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and

f. Updates privacy plan, policies, and procedures [*Assignment: organization-defined frequency, at least biennially*].

Supplemental Guidance: The development and implementation of a comprehensive governance and privacy program demonstrates organizational accountability for and commitment to the protection of individual privacy. Accountability begins with the appointment of an SAOP/CPO with the authority, mission, resources, and responsibility to develop and implement a multifaceted privacy program. The SAOP/CPO, in consultation with legal counsel, information security officials, and others as appropriate: (i) ensures the development, implementation, and enforcement of privacy policies and procedures; (ii) defines roles and responsibilities for protecting PII; (iii) determines the level of information sensitivity with regard to PII holdings; (iv) identifies the laws, regulations, and internal policies that apply to the PII; (v) monitors privacy best practices; and (vi) monitors/audits compliance with identified privacy controls.

To further accountability, the SAOP/CPO develops privacy plans to document the privacy requirements of organizations and the privacy and security controls in place or planned for meeting those requirements. The plan serves as evidence of organizational privacy operations and supports resource requests by the SAOP/CPO. A single plan or multiple plans may be necessary depending upon the organizational structures, requirements, and resources, and the plan(s) may vary in comprehensiveness. For example, a one-page privacy plan may cover privacy policies, documentation, and controls already in place, such as Privacy Impact Assessments (PIA) and System of Records Notices (SORN). A comprehensive plan may include a baseline of privacy controls selected from this appendix and include: (i) processes for conducting privacy risk assessments; (ii) templates and guidance for completing PIAs and SORNs; (iii) privacy training and awareness requirements; (iv) requirements for contractors processing PII; (v) plans for eliminating unnecessary PII holdings; and (vi) a framework for measuring annual performance goals and objectives for implementing identified privacy controls.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a; E-Government Act of 2002 (P.L. 107-347); Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; OMB Memoranda 03-22, 05-08, 07-16; OMB Circular A-130; Federal Enterprise Architecture Security and Privacy Profile.

AR-2 PRIVACY IMPACT AND RISK ASSESSMENT

Control: The organization:

a. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and

b. Conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.

Supplemental Guidance: Organizational privacy risk management processes operate across the life cycles of all mission/business processes that collect, use, maintain, share, or dispose of PII. The tools and processes for managing risk are specific to organizational missions and resources. They include, but are not limited to, the conduct of PIAs. The PIA is both a process and the document that is the outcome of that process. OMB Memorandum 03-22 provides guidance to organizations for implementing the privacy provisions of the E-Government Act of 2002, including guidance on when PIAs are required for information systems. Some organizations may be required by law or policy to extend the PIA requirement to other activities involving PII or otherwise impacting privacy (e.g., programs, projects, or regulations). PIAs are conducted to identify privacy risks and identify methods to mitigate those risks. PIAs are also conducted to ensure that programs or information systems comply with legal, regulatory, and policy requirements. PIAs also serve as notice to the public of privacy practices. PIAs are performed before developing or procuring information systems, or initiating programs or projects, that collect, use, maintain, or share PII and are updated when changes create new privacy risks.

Control Enhancements: None.

References: Section 208, E-Government Act of 2002 (P.L. 107-347); Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; OMB Memoranda 03-22, 05-08, 10-23.

AR-3 PRIVACY REQUIREMENTS FOR CONTRACTORS AND SERVICE PROVIDERS

Control: The organization:

a. Establishes privacy roles, responsibilities, and access requirements for contractors and service providers; and

b. Includes privacy requirements in contracts and other acquisition-related documents.

Supplemental Guidance: Contractors and service providers include, but are not limited to, information providers, information processors, and other organizations providing information system development, information technology services, and other outsourced applications. Organizations consult with legal counsel, the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO), and contracting officers about applicable laws, directives, policies, or regulations that may impact implementation of this control. Related control: AR-1, AR-5, SA-4.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a(m); Federal Acquisition Regulation, 48 C.F.R. Part 24; OMB Circular A-130.

AR-4 PRIVACY MONITORING AND AUDITING

Control: The organization monitors and audits privacy controls and internal privacy policy [*Assignment: organization-defined frequency*] to ensure effective implementation.

Supplemental Guidance: To promote accountability, organizations identify and address gaps in privacy compliance, management, operational, and technical controls by conducting regular assessments (e.g., internal risk assessments). These assessments can be self-assessments or third-party audits that result in reports on compliance gaps identified in programs, projects, and information systems. In addition to auditing for effective implementation of all privacy controls identified in this appendix, organizations assess whether they: (i) implement a process to embed privacy considerations into the life cycle of personally identifiable information (PII), programs, information systems, mission/business processes, and technology; (ii) monitor for changes to applicable privacy laws, regulations, and policies; (iii) track programs, information systems, and applications that collect and maintain PII to ensure compliance; (iv) ensure that access to PII is only on a *need-to-know* basis; and (v) ensure that PII is being maintained and used only for the legally authorized purposes identified in the public notice(s).

Organizations also: (i) implement technology to audit for the security, appropriate use, and loss of PII; (ii) perform reviews to ensure physical security of documents containing PII; (iii) assess contractor compliance with privacy requirements; and (iv) ensure that corrective actions identified as part of the assessment process are tracked and monitored until audit findings are corrected. The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) coordinates monitoring and auditing efforts with information security officials and ensures that the results are provided to senior managers and oversight officials. Related controls: AR-6, AR-7, AU-1, AU-2, AU-3, AU-6, AU-12, CA-7, TR-1, UL-2.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a; Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; Section 208, E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 05-08, 06-16, 07-16; OMB Circular A-130.

AR-5 PRIVACY AWARENESS AND TRAINING

Control: The organization:

a. Develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures;

b. Administers basic privacy training [*Assignment: organization-defined frequency, at least annually*] and targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII [*Assignment: organization-defined frequency, at least annually*]; and

c. Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements [*Assignment: organization-defined frequency, at least annually*].

Supplemental Guidance: Through implementation of a privacy training and awareness strategy, the organization promotes a culture of privacy. Privacy training and awareness programs typically focus on broad topics, such as responsibilities under the Privacy Act of 1974 and E-Government Act of 2002 and the consequences of failing to carry out those responsibilities, how to identify new privacy risks, how to mitigate privacy risks, and how and when to report privacy incidents. Privacy training may also target data collection and use requirements identified in public notices, such as Privacy Impact Assessments (PIAs) or System of Records Notices (SORNs) for a program or information system. Specific training methods may include: (i) mandatory annual privacy awareness training; (ii) targeted, role-based training; (iii) internal privacy program websites; (iv) manuals, guides, and handbooks; (v) slide presentations; (vi) events (e.g., privacy awareness week, privacy clean-up day); (vii) posters and brochures; and (viii) email messages to all employees and contractors. Organizations update training based on changing statutory, regulatory, mission,

program, business process, and information system requirements, or on the results of compliance monitoring and auditing. Where appropriate, organizations may provide privacy training as part of existing information security training. Related controls: AR-3, AT-2, AT-3, TR-1.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a(e); Section 208, E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 07-16.

AR-6 PRIVACY REPORTING

Control: The organization develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

Supplemental Guidance: Through internal and external privacy reporting, organizations promote accountability and transparency in organizational privacy operations. Reporting also helps organizations to determine progress in meeting privacy compliance requirements and privacy controls, compare performance across the federal government, identify vulnerabilities and gaps in policy and implementation, and identify success models. Types of privacy reports include: (i) annual Senior Agency Official for Privacy (SAOP) reports to OMB; (ii) reports to Congress required by the *Implementing Regulations of the 9/11 Commission Act*; and (iii) other public reports required by specific statutory mandates or internal policies of organizations. The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) consults with legal counsel, where appropriate, to ensure that organizations meet all applicable privacy reporting requirements.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a; Section 208, E-Government Act of 2002 (P.L. 107-347); Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; Section 803, 9/11 Commission Act, 42 U.S.C. § 2000ee-1; Section 804, 9/11 Commission Act, 42 U.S.C. § 2000ee-3; Section 522, Consolidated Appropriations Act of 2005 (P.L. 108-447); OMB Memoranda 03-22; OMB Circular A-130.

AR-7 PRIVACY-ENHANCED SYSTEM DESIGN AND DEVELOPMENT

Control: The organization designs information systems to support privacy by automating privacy controls.

Supplemental Guidance: To the extent feasible, when designing organizational information systems, organizations employ technologies and system capabilities that automate privacy controls on the collection, use, retention, and disclosure of personally identifiable information (PII). By building privacy controls into system design and development, organizations mitigate privacy risks to PII, thereby reducing the likelihood of information system breaches and other privacy-related incidents. Organizations also conduct periodic reviews of systems to determine the need for updates to maintain compliance with the Privacy Act and the organization's privacy policy. Regardless of whether automated privacy controls are employed, organizations regularly monitor information system use and sharing of PII to ensure that the use/sharing is consistent with the authorized purposes identified in the Privacy Act and/or in the public notice of organizations, or in a manner compatible with those purposes. Related controls: AC-6, AR-4, AR-5, DM-2, TR-1.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a(e)(10); Sections 208(b) and(c), E-Government Act of 2002 (P.L. 107-347); OMB Memorandum 03-22.

AR-8 ACCOUNTING OF DISCLOSURES

Control: The organization:

a. Keeps an accurate accounting of disclosures of information held in each system of records under its control, including:

   (1) Date, nature, and purpose of each disclosure of a record; and

   (2) Name and address of the person or agency to which the disclosure was made;

b. Retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and

c. Makes the accounting of disclosures available to the person named in the record upon request.

Supplemental Guidance: The Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) periodically consults with managers of organization systems of record to ensure that the required accountings of disclosures of records are being properly maintained and provided to persons named in those records consistent with the dictates of the Privacy Act. Organizations are not required to keep an accounting of disclosures when the disclosures are made to individuals with a need to know, are made pursuant to the Freedom of Information Act, or are made to a law enforcement agency pursuant to 5 U.S.C. § 552a(c)(3). Heads of agencies can promulgate rules to exempt certain systems of records from the requirement to provide the accounting of disclosures to individuals. Related control: IP-2.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (c)(1), (c)(3), (j), (k).

FAMILY: DATA QUALITY AND INTEGRITY

This family enhances public confidence that any personally identifiable information (PII) collected and maintained by organizations is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in public notices.

DI-1 DATA QUALITY

Control: The organization:

a. Confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information;

b. Collects PII directly from the individual to the greatest extent practicable;

c. Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems [*Assignment: organization-defined frequency*]; and

d. Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

Supplemental Guidance: Organizations take reasonable steps to confirm the accuracy and relevance of PII. Such steps may include, for example, editing and validating addresses as they are collected or entered into information systems using automated address verification look-up application programming interfaces (API). The types of measures taken to protect data quality are based on the nature and context of the PII, how it is to be used, and how it was obtained. Measures taken to validate the accuracy of PII that is used to make determinations about the rights, benefits, or privileges of individuals under federal programs may be more comprehensive than those used to validate less sensitive PII. Additional steps may be necessary to validate PII that is obtained from sources other than individuals or the authorized representatives of individuals.

When PII is of a sufficiently sensitive nature (e.g., when it is used for annual reconfirmation of a taxpayer's income for a recurring benefit), organizations incorporate mechanisms into information systems and develop corresponding procedures for how frequently, and by what method, the information is to be updated. Related controls: AP-2, DI-2, DM-1, IP-3, SI-10.

Control Enhancements:

(1) *DATA QUALITY | VALIDATE PII*

The organization requests that the individual or individual's authorized representative validate PII during the collection process.

(2) *DATA QUALITY | RE-VALIDATE PII*

The organization requests that the individual or individual's authorized representative revalidate that PII collected is still accurate [*Assignment: organization-defined frequency*].

References: The Privacy Act of 1974, 5 U.S.C. § 552a (c) and (e); Treasury and General Government Appropriations Act for Fiscal Year 2001 (P.L. 106-554), app C § 515, 114 Stat. 2763A-153-4; Paperwork Reduction Act, 44 U.S.C. § 3501; OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies (October 2001); OMB Memorandum 07-16**.**

DI-2 DATA INTEGRITY AND DATA INTEGRITY BOARD

Control: The organization:

a. Documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls; and

b. Establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements[123] and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.

Supplemental Guidance: Organizations conducting or participating in Computer Matching Agreements with other organizations regarding applicants for and recipients of financial assistance or payments under federal benefit programs or regarding certain computerized comparisons involving federal personnel or payroll records establish a Data Integrity Board to oversee and coordinate their implementation of such matching agreements. In many organizations, the Data Integrity Board is led by the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO). The Data Integrity Board ensures that controls are in place to maintain both the quality and the integrity of data shared under Computer Matching Agreements. Related controls: AC-1, AC-3, AC-4, AC-6, AC-17, AC-22, AU-2, AU-3, AU-6, AU-10, AU-11, DI-1, SC-8, SC-28, UL-2.

Control Enhancements:

(1) *DATA INTEGRITY AND DATA INTEGRITY BOARD | PUBLISH AGREEMENTS ON WEBSITE*

The organization publishes Computer Matching Agreements on its public website.

References: The Privacy Act of 1974, 5 U.S.C. §§ 552a (a)(8)(A), (o), (p), (u); OMB Circular A-130, Appendix I.

[123] Organizations enter into Computer Matching Agreements in connection with computer matching programs to which they are a party. With certain exceptions, a computer matching program is any computerized comparison of two or more automated systems of records or a system of records with nonfederal records for the purpose of establishing or verifying the eligibility of, or continuing compliance with, statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to cash or in-kind assistance or payments under federal benefit programs or computerized comparisons of two or more automated federal personnel or payroll systems of records or a system of federal personnel or payroll records with nonfederal records. See Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a (a)(8)(A).

FAMILY: DATA MINIMIZATION AND RETENTION

This family helps organizations implement the data minimization and retention requirements to collect, use, and retain only personally identifiable information (PII) that is relevant and necessary for the purpose for which it was originally collected. Organizations retain PII for only as long as necessary to fulfill the purpose(s) specified in public notices and in accordance with a National Archives and Records Administration (NARA)-approved record retention schedule.

DM-1 MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION

Control: The organization:

a. Identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection;

b. Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and

c. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings [*Assignment: organization-defined frequency, at least annually*] to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

Supplemental Guidance: Organizations take appropriate steps to ensure that the collection of PII is consistent with a purpose authorized by law or regulation. The minimum set of PII elements required to support a specific organization business process may be a subset of the PII the organization is authorized to collect. Program officials consult with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and legal counsel to identify the minimum PII elements required by the information system or activity to accomplish the legally authorized purpose.

Organizations can further reduce their privacy and security risks by also reducing their inventory of PII, where appropriate. OMB Memorandum 07-16 requires organizations to conduct both an initial review and subsequent reviews of their holdings of all PII and ensure, to the maximum extent practicable, that such holdings are accurate, relevant, timely, and complete. Organizations are also directed by OMB to reduce their holdings to the minimum necessary for the proper performance of a documented organizational business purpose. OMB Memorandum 07-16 requires organizations to develop and publicize, either through a notice in the Federal Register or on their websites, a schedule for periodic reviews of their holdings to supplement the initial review. Organizations coordinate with their federal records officers to ensure that reductions in organizational holdings of PII are consistent with NARA retention schedules.

By performing periodic evaluations, organizations reduce risk, ensure that they are collecting only the data specified in the notice, and ensure that the data collected is still relevant and necessary for the purpose(s) specified in the notice. Related controls: AP-1, AP-2, AR-4, IP-1, SE-1, SI-12, TR-1.

Control Enhancements:

(1) *MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION | LOCATE / REMOVE / REDACT / ANONYMIZE PII*

The organization, where feasible and within the limits of technology, locates and removes/redacts specified PII and/or uses anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure.

Supplemental Guidance: NIST Special Publication 800-122 provides guidance on anonymization.

References: The Privacy Act of 1974, 5 U.S.C. §552a (e); Section 208(b), E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 07-16.

DM-2 DATA RETENTION AND DISPOSAL

Control: The organization:

a. Retains each collection of personally identifiable information (PII) for [*Assignment: organization-defined time period*] to fulfill the purpose(s) identified in the notice or as required by law;

b. Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and

c. Uses [*Assignment: organization-defined techniques or methods*] to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

Supplemental Guidance: NARA provides retention schedules that govern the disposition of federal records. Program officials coordinate with records officers and with NARA to identify appropriate retention periods and disposal methods. NARA may require organizations to retain PII longer than is operationally needed. In those situations, organizations describe such requirements in the notice. Methods of storage include, for example, electronic, optical media, or paper.

Examples of ways organizations may reduce holdings include reducing the types of PII held (e.g., delete Social Security numbers if their use is no longer needed) or shortening the retention period for PII that is maintained if it is no longer necessary to keep PII for long periods of time (this effort is undertaken in consultation with an organization's records officer to receive NARA approval). In both examples, organizations provide notice (e.g., an updated System of Records Notice) to inform the public of any changes in holdings of PII.

Certain read-only archiving techniques, such as DVDs, CDs, microfilm, or microfiche, may not permit the removal of individual records without the destruction of the entire database contained on such media. Related controls: AR-4, AU-11, DM-1, MP-1, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SI-12, TR-1.

Control Enhancements:

(1) *DATA RETENTION AND DISPOSAL | SYSTEM CONFIGURATION*

The organization, where feasible, configures its information systems to record the date PII is collected, created, or updated and when PII is to be deleted or archived under an approved record retention schedule.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (e)(1), (c)(2); Section 208 (e), E-Government Act of 2002 (P.L. 107-347); 44 U.S.C. Chapters 29, 31, 33; OMB Memorandum 07-16; OMB Circular A-130; NIST Special Publication 800-88.

DM-3 MINIMIZATION OF PII USED IN TESTING, TRAINING, AND RESEARCH

Control: The organization:

a. Develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research; and

b. Implements controls to protect PII used for testing, training, and research.

Supplemental Guidance: Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. The use of PII in testing, research, and training increases risk of unauthorized disclosure or misuse of the information. If PII must be used, organizations take measures to minimize any associated risks and to authorize the use of and limit the amount of PII for these purposes. Organizations consult with the SAOP/CPO and legal counsel to ensure that the use of PII in testing, training, and research is compatible with the original purpose for which it was collected.

Control Enhancements:

(1) *MINIMIZATION OF PII USED IN TESTING, TRAINING, AND RESEARCH | RISK MINIMIZATION TECHNIQUES*

The organization, where feasible, uses techniques to minimize the risk to privacy of using PII for research, testing, or training.

Supplemental Guidance: Organizations can minimize risk to privacy of PII by using techniques such as de-identification.

References: NIST Special Publication 800-122.

FAMILY: INDIVIDUAL PARTICIPATION AND REDRESS

This family addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their personally identifiable information (PII). By providing individuals with access to PII and the ability to have their PII corrected or amended, as appropriate, the controls in this family enhance public confidence in organizational decisions made based on the PII.

IP-1 CONSENT

Control: The organization:

a. Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection;

b. Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII;

c. Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and

d. Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

Supplemental Guidance: Consent is fundamental to the participation of individuals in the decision-making process regarding the collection and use of their PII and the use of technologies that may increase risk to personal privacy. To obtain consent, organizations provide individuals appropriate notice of the purposes of the PII collection or technology use and a means for individuals to consent to the activity. Organizations tailor the public notice and consent mechanisms to meet operational needs. Organizations achieve awareness and consent, for example, through updated public notices.

Organizations may obtain consent through opt-in, opt-out, or implied consent. Opt-in consent is the preferred method, but it is not always feasible. Opt-in requires that individuals take affirmative action to *allow* organizations to collect or use PII. For example, opt-in consent may require an individual to click a radio button on a website, or sign a document providing consent. In contrast, opt-out requires individuals to take action to *prevent* the new or continued collection or use of such PII. For example, the Federal Trade Commission's Do-Not-Call Registry allows individuals to opt-out of receiving unsolicited telemarketing calls by requesting to be added to a list. Implied consent is the least preferred method and should be used in limited circumstances. Implied consent occurs where individuals' behavior or failure to object indicates agreement with the collection or use of PII (e.g., by entering and remaining in a building where notice has been posted that security cameras are in use, the individual implies consent to the video recording). Depending upon the nature of the program or information system, it may be appropriate to allow individuals to limit the types of PII they provide and subsequent uses of that PII. Organizational consent mechanisms include a discussion of the consequences to individuals of failure to provide PII. Consequences can vary from organization to organization. Related controls: AC-2, AP-1, TR-1, TR-2.

Control Enhancements:

(1) *CONSENT | MECHANISMS SUPPORTING ITEMIZED OR TIERED CONSENT*

The organization implements mechanisms to support itemized or tiered consent for specific uses of data.

Supplemental Guidance: Organizations can provide, for example, individuals' itemized choices as to whether they wish to be contacted for any of a variety of purposes. In this situation, organizations construct consent mechanisms to ensure that organizational operations comply with individual choices.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (b), (e)(3); Section 208(c), E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 10-22.

IP-2 INDIVIDUAL ACCESS

Control: The organization:

a. Provides individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records;

b. Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records;

c. Publishes access procedures in System of Records Notices (SORNs); and

d. Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

Supplemental Guidance: Access affords individuals the ability to review PII about them held within organizational systems of records. Access includes timely, simplified, and inexpensive access to data. Organizational processes for allowing access to records may differ based on resources, legal requirements, or other factors. The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) is responsible for the content of Privacy Act regulations and record request processing, in consultation with legal counsel. Access to certain types of records may not be appropriate, however, and heads of agencies may promulgate rules exempting particular systems from the access provision of the Privacy Act. In addition, individuals are not entitled to access to information compiled in reasonable anticipation of a civil action or proceeding. Related controls: AR-8, IP-3, TR-1, TR-2.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. §§ 552a (c)(3), (d)(5), (e) (4); (j), (k), (t); OMB Circular A-130.

IP-3 REDRESS

Control: The organization:

a. Provides a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate; and

b. Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.

Supplemental Guidance: Redress supports the ability of individuals to ensure the accuracy of PII held by organizations. Effective redress processes demonstrate organizational commitment to data quality especially in those business functions where inaccurate data may result in inappropriate decisions or denial of benefits and services to individuals. Organizations use discretion in determining if records are to be corrected or amended, based on the scope of redress requests, the changes sought, and the impact of the changes. Individuals may appeal an adverse decision and have incorrect information amended, where appropriate.

To provide effective redress, organizations: (i) provide effective notice of the existence of a PII collection; (ii) provide plain language explanations of the processes and mechanisms for requesting access to records; (iii) establish criteria for submitting requests for correction or amendment; (iv) implement resources to analyze and adjudicate requests; (v) implement means of correcting or amending data collections; and (vi) review any decisions that may have been the result of inaccurate information.

Organizational redress processes provide responses to individuals of decisions to deny requests for correction or amendment, including the reasons for those decisions, a means to record individual objections to the organizational decisions, and a means of requesting organizational reviews of the initial determinations. Where PII is corrected or amended, organizations take steps to ensure that all authorized recipients of that PII are informed of the corrected or amended information. In instances where redress involves information obtained from other organizations, redress processes include coordination with organizations that originally collected the information. Related controls: IP-2, TR-1, TR-2, UL-2.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (d), (c)(4); OMB Circular A-130.

IP-4 COMPLAINT MANAGEMENT

Control: The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.

Supplemental Guidance: Complaints, concerns, and questions from individuals can serve as a valuable source of external input that ultimately improves operational models, uses of technology, data collection practices, and privacy and security safeguards. Organizations provide complaint mechanisms that are readily accessible by the public, include all information necessary for successfully filing complaints (including contact information for the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) or other official designated to receive complaints), and are easy to use. Organizational complaint management processes include tracking mechanisms to ensure that all complaints received are reviewed and appropriately addressed in a timely manner. Related controls: AR-6, IP-3.

Control Enhancements:

(1) *COMPLAINT MANAGEMENT | RESPONSE TIMES*

The organization responds to complaints, concerns, or questions from individuals within [*Assignment: organization-defined time period*].

References: OMB Circular A-130; OMB Memoranda 07-16, 08-09.

FAMILY: SECURITY

This family supplements the security controls in Appendix F to ensure that technical, physical, and administrative safeguards are in place to protect personally identifiable information (PII) collected or maintained by organizations against loss, unauthorized access, or disclosure, and to ensure that planning and responses to privacy incidents comply with OMB policies and guidance. The controls in this family are implemented in coordination with information security personnel and in accordance with the existing NIST Risk Management Framework.

SE-1 INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION

Control: The organization:

a. Establishes, maintains, and updates [*Assignment: organization-defined frequency*] an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII); and

b. Provides each update of the PII inventory to the CIO or information security official [*Assignment: organization-defined frequency*] to support the establishment of information security requirements for all new or modified information systems containing PII.

Supplemental Guidance: The PII inventory enables organizations to implement effective administrative, technical, and physical security policies and procedures to protect PII consistent with Appendix F, and to mitigate risks of PII exposure. As one method of gathering information for their PII inventories, organizations may extract the following information elements from Privacy Impact Assessments (PIA) for information systems containing PII: (i) the name and acronym for each system identified; (ii) the types of PII contained in that system; (iii) classification of level of sensitivity of all types of PII, as combined in that information system; and (iv) classification of level of potential risk of substantial harm, embarrassment, inconvenience, or unfairness to affected individuals, as well as the financial or reputational risks to organizations, if PII is exposed. Organizations take due care in updating the inventories by identifying linkable data that could create PII. Related controls: AR-1, AR-4, AR-5, AT-1, DM-1, PM-5, UL-3.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (e) (10); Section 208(b)(2), E-Government Act of 2002 (P.L. 107-347); OMB Memorandum 03-22; OMB Circular A-130, Appendix I; FIPS Publication 199; NIST Special Publications 800-37, 800-122.

SE-2 PRIVACY INCIDENT RESPONSE

Control: The organization:

a. Develops and implements a Privacy Incident Response Plan; and

b. Provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.

Supplemental Guidance: In contrast to the Incident Response (IR) family in Appendix F, which concerns a broader range of incidents affecting information security, this control uses the term Privacy Incident to describe only those incidents that relate to personally identifiable information (PII). The organization Privacy Incident Response Plan is developed under the leadership of the SAOP/CPO. The plan includes: (i) the establishment of a cross-functional Privacy Incident Response Team that reviews, approves, and participates in the execution of the Privacy Incident Response Plan; (ii) a process to determine whether notice to oversight organizations or affected individuals is appropriate and to provide that notice accordingly; (iii) a privacy risk assessment process to determine the extent of harm, embarrassment, inconvenience, or unfairness to affected individuals and, where appropriate, to take steps to mitigate any such risks; (iv) internal

procedures to ensure prompt reporting by employees and contractors of any privacy incident to information security officials and the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO), consistent with organizational incident management structures; and (v) internal procedures for reporting noncompliance with organizational privacy policy by employees or contractors to appropriate management or oversight officials. Some organizations may be required by law or policy to provide notice to oversight organizations in the event of a breach. Organizations may also choose to integrate Privacy Incident Response Plans with Security Incident Response Plans, or keep the plans separate. Related controls: AR-1, AR-4, AR-5, AR-6, AU-1 through 14, IR-1 through IR-8, RA-1.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (e), (i)(1), and (m); Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; OMB Memoranda 06-19, 07-16; NIST Special Publication 800-37.

FAMILY: TRANSPARENCY

This family ensures that organizations provide public notice of their information practices and the privacy impact of their programs and activities.

TR-1 PRIVACY NOTICE

Control: The organization:

a. Provides effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary;

b. Describes: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected; and

c. Revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.

Supplemental Guidance: Effective notice, by virtue of its clarity, readability, and comprehensiveness, enables individuals to understand how an organization uses PII generally and, where appropriate, to make an informed decision prior to providing PII to an organization. Effective notice also demonstrates the privacy considerations that the organization has addressed in implementing its information practices. The organization may provide general public notice through a variety of means, as required by law or policy, including System of Records Notices (SORNs), Privacy Impact Assessments (PIAs), or in a website privacy policy. As required by the Privacy Act, the organization also provides direct notice to individuals via Privacy Act Statements on the paper and electronic forms it uses to collect PII, or on separate forms that can be retained by the individuals.

The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) is responsible for the content of the organization's public notices, in consultation with legal counsel and relevant program managers. The public notice requirement in this control is satisfied by an organization's compliance with the public notice provisions of the Privacy Act, the E-Government Act's PIA requirement, with OMB guidance related to federal agency privacy notices, and, where applicable, with policy pertaining to participation in the Information Sharing Environment (ISE).[124] Changing PII practice or policy without prior notice is disfavored and should only be undertaken in consultation with the SAOP/CPO and counsel. Related controls: AP-1, AP-2, AR-1, AR-2, IP-1, IP-2, IP-3, UL-1, UL-2.

Control Enhancements:

(1) *PRIVACY NOTICE | REAL-TIME OR LAYERED NOTICE*

The organization provides real-time and/or layered notice when it collects PII.

Supplemental Guidance: Real-time notice is defined as notice at the point of collection. A layered notice approach involves providing individuals with a summary of key points in the organization's privacy policy. A second notice provides more detailed/specific information.

[124] The Information Sharing Environment is an approach that facilitates the sharing of terrorism and homeland security information. The ISE was established by the Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458, 118 Stat. 3638. See the ISE website at: http://www.ise.gov.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3), (e)(4); Section 208(b), E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 07-16, 10-22, 10-23; ISE Privacy Guidelines.

TR-2 SYSTEM OF RECORDS NOTICES AND PRIVACY ACT STATEMENTS

Control: The organization:

a. Publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information (PII);

b. Keeps SORNs current; and

c. Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.

Supplemental Guidance: Organizations issue SORNs to provide the public notice regarding PII collected in a system of records, which the Privacy Act defines as "a group of any records under the control of any agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifier." SORNs explain how the information is used, retained, and may be corrected, and whether certain portions of the system are subject to Privacy Act exemptions for law enforcement or national security reasons. Privacy Act Statements provide notice of: (i) the authority of organizations to collect PII; (ii) whether providing PII is mandatory or optional; (iii) the principal purpose(s) for which the PII is to be used; (iv) the intended disclosures (routine uses) of the information; and (v) the consequences of not providing all or some portion of the information requested. When information is collected verbally, organizations read a Privacy Act Statement prior to initiating the collection of PII (for example, when conducting telephone interviews or surveys). Related control: DI-2.

Control Enhancements:

(1) *SYSTEM OF RECORDS NOTICES AND PRIVACY ACT STATEMENTS | PUBLIC WEBSITE PUBLICATION*
The organization publishes SORNs on its public website.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3); OMB Circular A-130.

TR-3 DISSEMINATION OF PRIVACY PROGRAM INFORMATION

Control: The organization:

a. Ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO); and

b. Ensures that its privacy practices are publicly available through organizational websites or otherwise.

Supplemental Guidance: Organizations employ different mechanisms for informing the public about their privacy practices including, but not limited to, Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), privacy reports, publicly available web pages, email distributions, blogs, and periodic publications (e.g., quarterly newsletters). Organizations also employ publicly facing email addresses and/or phone lines that enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices. Related control: AR-6.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a; Section 208, E-Government Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 10-23.

FAMILY: USE LIMITATION

This family ensures that organizations only use personally identifiable information (PII) either as specified in their public notices, in a manner compatible with those specified purposes, or as otherwise permitted by law. Implementation of the controls in this family will ensure that the scope of PII use is limited accordingly.

UL-1 INTERNAL USE

Control: The organization uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.

Supplemental Guidance: Organizations take steps to ensure that they use PII only for legally authorized purposes and in a manner compatible with uses identified in the Privacy Act and/or in public notices. These steps include monitoring and auditing organizational use of PII and training organizational personnel on the authorized uses of PII. With guidance from the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and where appropriate, legal counsel, organizations document processes and procedures for evaluating any proposed new uses of PII to assess whether they fall within the scope of the organizational authorities. Where appropriate, organizations obtain consent from individuals for the new use(s) of PII. Related controls: AP-2, AR-2, AR-3, AR-4, AR-5, IP-1, TR-1, TR-2.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (b)(1).

UL-2 INFORMATION SHARING WITH THIRD PARTIES

Control: The organization:

a. Shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes;

b. Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used;

c. Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and

d. Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

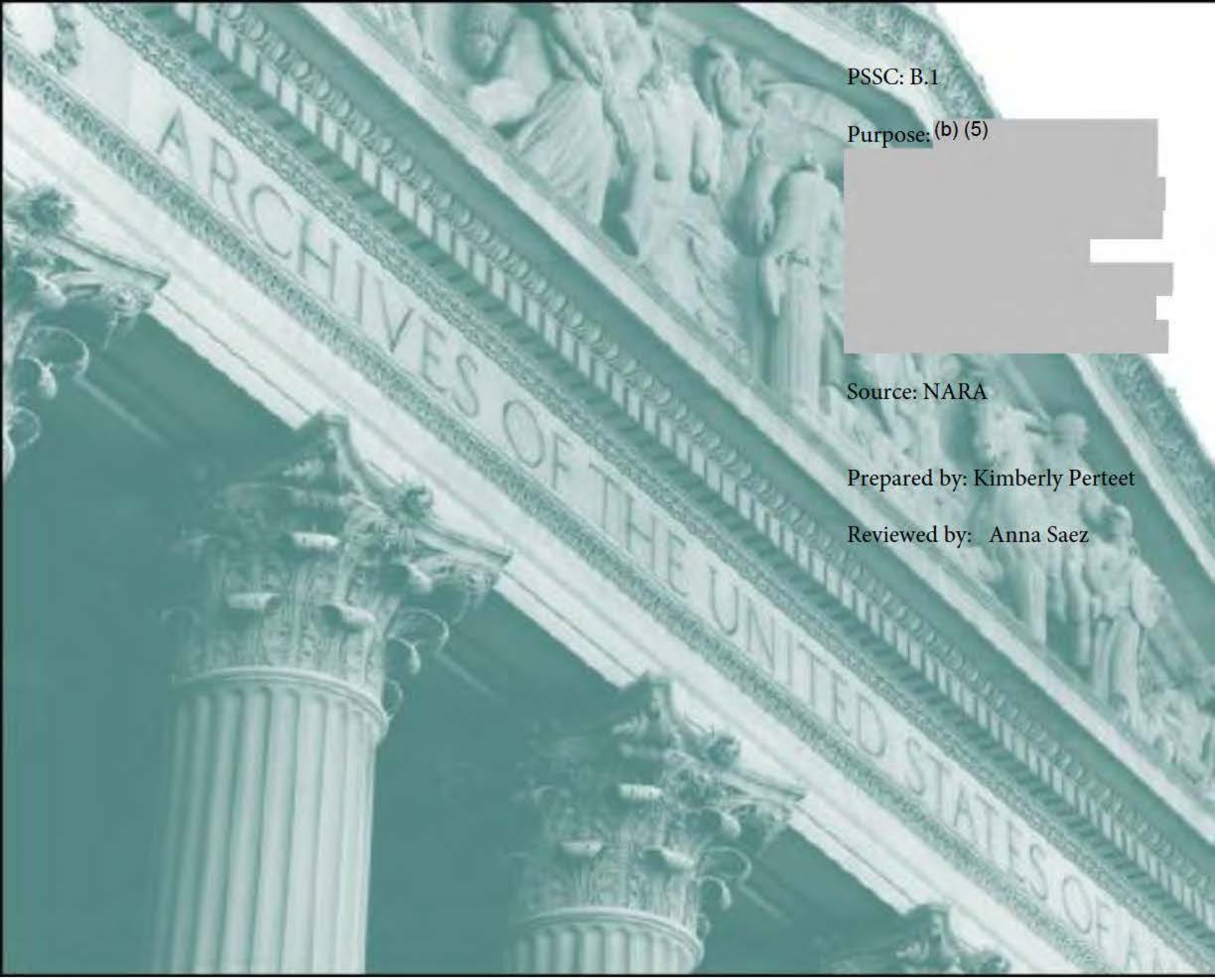
Supplemental Guidance: The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and, where appropriate, legal counsel review and approve any proposed external sharing of PII, including with other public, international, or private sector entities, for consistency with uses described in the existing organizational public notice(s). When a proposed new instance of external sharing of PII is not currently authorized by the Privacy Act and/or specified in a notice, organizations evaluate whether the proposed external sharing is compatible with the purpose(s) specified in the notice. If the proposed sharing is compatible, organizations review, update, and republish their Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), website privacy policies, and other public notices, if any, to include specific descriptions of the new uses(s) and obtain consent where appropriate and feasible. Information-sharing agreements also include security protections consistent with the sensitivity of the information being shared. Related controls: AR-3, AR-4, AR-5, AR-8, AP-2, DI-1, DI-2, IP-1, TR-1.

Control Enhancements: None.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (a)(7), (b), (c), (e)(3)(C), (o); ISE Privacy Guidelines.

Acknowledgements

This appendix was developed by the National Institute of Standards and Technology and the Privacy Committee of the Federal Chief Information Officer (CIO) Council. In particular, we wish to thank the members of the Privacy Committee's Best Practices Subcommittee and its Privacy Controls Appendix Working Group—Claire Barrett, Chris Brannigan, Pamela Carcirieri, Debra Diener, Deborah Kendall, Martha Landesberg, Steven Lott, Lewis Oleinick, and Roanne Shaddox—for their valuable insights, subject matter expertise, and overall contributions in helping to develop the content for this appendix to Special Publication 800-53. We also wish to recognize and thank Erika McCallister, Toby Levin, James McKenzie, Julie McEwen, and Richard Graubart for their significant contributions to this project. A special note of thanks goes to Peggy Himes and Elizabeth Lennon for their superb administrative support. The authors also gratefully acknowledge and appreciate the significant contributions from individuals, groups, and organizations in the public and private sectors, whose thoughtful and constructive comments improved the overall quality, thoroughness, and usefulness of this publication.



PSSC: B.1

Purpose: (b) (5)

Source: NARA

Prepared by: Kimberly Perteet

Reviewed by: Anna Saez

Federal Equal Opportunity Recruitment Program Plan Fiscal Year 2012

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

Table of Contents

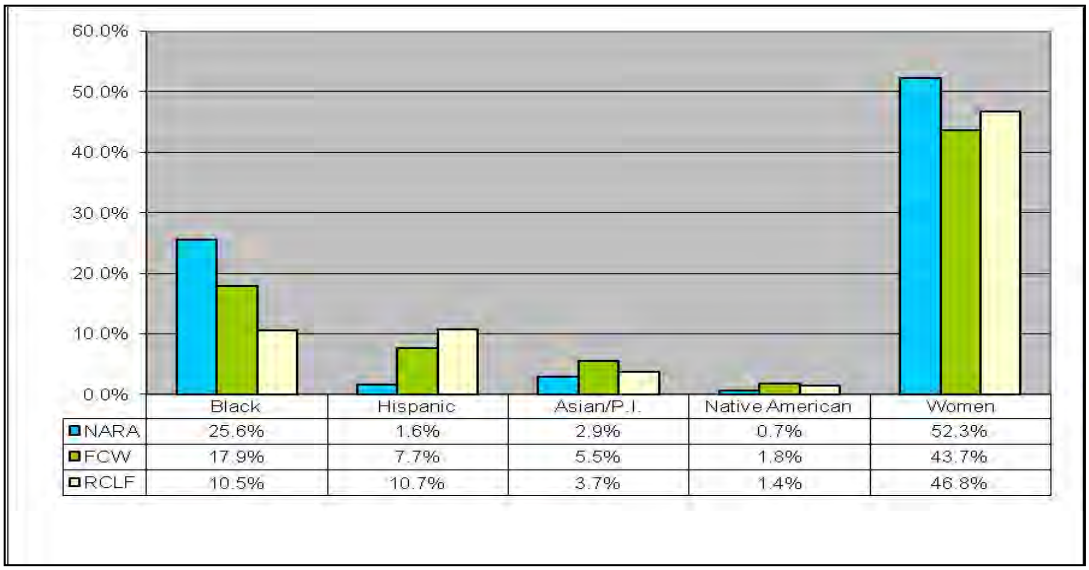
Executive Summary

Moreover, we recognize diversity as a catalyst for new ideas and innovation, helping us to solve not only the problems of today but also the challenges of tomorrow. R1

This Federal Equal Opportunity Recruitment Program (FEORP) Plan is our roadmap for how to recruit and retain a highly qualified diverse workforce. It outlines the basic policy, legal authority, and responsibility for NARA's FEORP Plan; provides data on our workforce and how it compares to both the Federal Civilian Workforce (FCW) and the Relevant Civilian Labor Force (RCLF); and identifies specific actions that NARA will undertake in the coming years to address areas where underrepresentation of women and minorities exist in our workforce.

As shown in Figure 1 below, representation for some groups – specifically, women and Blacks - compare favorably to both the FCW and the RCLF. However, with the exception of these two groups, all others are underrepresented at NARA when compared to the FCW. In particular, Hispanics are significantly underrepresented in NARA, comprising just 1.6 percent of the workforce as compared to the 7.7 percent of the FCW and 10.7 percent of the RCLF. Representation rates for Asian/Pacific Islanders and Native Americans are also below those in both the RCLF and the FCW.

Figure 1
NARA vs. Federal and Relevant Civilian Labor Workforce[1]



	Black	Hispanic	Asian/P.I.	Native American	Women
NARA	25.6%	1.6%	2.9%	0.7%	52.3%
FCW	17.9%	7.7%	5.5%	1.8%	43.7%
RCLF	10.5%	10.7%	3.7%	1.4%	46.8%

[1] NARA data provided by NARA's Performance Measurement and Reporting System (PMRS); covers full-time permanent employees as of October 27, 2011
Federal Civilian Workforce (FCW.); covers full and part-time permanent employees, data sourced from Fedscope, June 2011, Nationwide
Relevant Civilian Labor Workforce (RCLF); covers full and part-time permanent employees, data sourced from Census EEO Tool, Nationwide

supervisory workforce, they comprise only 45 percent of supervisory positions and 23 percent of executive positions.

To address these challenges, NARA has identified three multi-year strategic goals that together form the foundation of our FEORP. These goals are:

- Ensure that FEORP goals are aligned with NARA's Strategic Plan and Strategic Human Capital Plan and integrated with workforce planning efforts;
- Expand the pipeline of women and minorities available for employment with NARA; and
- Enhance staff development opportunities that prepare staff for upper level positions.

In support of these goals, we have identified 14 specific strategies that NARA will undertake in Fiscal Year 2012 to enhance the representation of women and minorities at all levels. Our strategies focus on expanding partnerships with minority-serving universities, education associations, and professional organizations; attending and networking at minority conferences and job fairs; encouraging the use of developmental assignments that provide on-the-job training opportunities for women and minorities; and ensuring that our FEORP goals and strategies are fully aligned with NARA's Strategic Human Capital Plan and, by extension, NARA's Strategic Plan.

Progress against these goals and strategies will be assessed each year as part of our human capital accountability efforts and the U.S. Office of Personnel Management's (OPM) annual FEORP and Federal Hispanic Employment Plan (HEP) reporting requirements. In addition, this plan will be revised each year to reflect NARA's latest workforce demographics and updated strategies for addressing underrepresentation at NARA.

Introduction

I agency created by statute in 1934, NARA safeguards the records of all three branches of the Federal Government.

Our job is to ensure continuing access to essential documentation and, in doing so, we serve a broad spectrum of American society. Genealogists and family historians; veterans and their authorized representatives; academics, scholars, historians, business and occupational researchers; publication and broadcast journalists; Congress, the Courts, the White House, and other public officials; Federal Government agencies and the individuals they serve; state and local government personnel; professional organizations and their members; students and teachers; and the general public – all seek answers from the records we preserve.

Mission

The National Archives and Records Administration serves American democracy by safeguarding and preserving the records of our Government, ensuring that the people can discover, use, and learn from this documentary heritage. We ensure continuing access to the essential documentation of the rights of American citizens and the actions of their government. We support democracy, promote civic education, and facilitate historical understanding of our national experience.

Vision

As the nation's record keeper, it is our vision that all Americans will understand the vital role records play in a democracy, and their own personal stake in the National Archives. Our holdings and diverse programs will be available to more people than ever before through modern technology and dynamic partnerships. The stories of our nation and our people are told in the records and artifacts cared for in NARA facilities around the country. We want all Americans to be inspired to explore the records of their country.

We carry out our mission through a national network of archives and records services facilities stretching

response to hundreds of thousands of requests, the records on which the entitlements of citizens, the credibility of Government, and the accuracy of history depend.

In order to accomplish our mission and effectively represent the many customers we serve, NARA recognizes the need to recruit, retain, reward, and promote a highly qualified diverse workforce. Demographic research suggests that the future workforce talent pool will be much more diverse, including individuals of different genders, ages, races, ethnicities, and lifestyles. By effectively leveraging this human capital, we can increase the variety of available skills and knowledge in our workforce, thereby achieving greater mission success. Specifically, diversity recruitment initiatives can help NARA reduce turnover, improve retention and employee morale, and increase innovation.

NARA's commitment to diversity is reflected in our 2006 – 2016 Strategic Plan ("*Preserving the Past to Protect the Future"*). The Strategic Plan incorporates two goals, specifically 6.1 and 6.2, aimed at enhancing the competencies and diversity of our workforce:

Strategic Goal 6

We will equip NARA to meet the changing needs of our customers.

- **6.1 By 2016, 95 percent of employees possess the core competencies that were identified for their jobs.**
- **6.2 By 2016, the percentage of NARA employees in underrepresented groups match their respective availability levels in the Civilian Labor Force (CLF).**

This Federal Equal Opportunity Recruitment Program Plan further emphasizes our commitment to diversity. It identifies specific objectives and strategies for eliminating underrepresentation of women and minorities in NARA, and it provides a framework for aligning our strategic diversity recruitment and human capital goals with the vision and mission articulated in our Strategic Plan.

women exist.

The U.S. Office of Personnel Management (OPM) sets policy and provides guidance to Federal agencies on the development and administration of FEORP. OPM requires that agency FEORP plans cover the following underrepresented groups: White females, Black males and females, Hispanic males and females[2], Asian/Pacific Islander males and females, and Native American males and females.

The FEORP applies to all positions in all pay plans, unless specifically exempt by statute.

This plan is reviewed and updated on an annual basis.

LEGAL AUTHORITY

As outlined in 5 U.S.C. 7201(b), "It is the policy of the United States to insure equal employment opportunities for employees without discrimination because of race, color, religion, sex, or national origin."

Further, as outlined in Executive Order 13171, "The head of each executive department and agency (agency) shall establish and maintain a program for the recruitment and career development of Hispanics/Latinos in Federal government."

OPM's implementing regulations for these provisions are contained at 5 CFR 720, Subpart B – Federal Equal Opportunity Recruitment Program. Specifically, 5 CFR 720.205 requires each agency to "have an up-to-date equal opportunity recruitment program plan covering recruitment of positions at various organizational levels and geographic locations within the agency."

Pursuant to this policy, 5 U.S.C. 7201(c) requires: "That each Executive agency conduct a continuing program for the recruitment of members of minorities for positions in the agency to carry out the [anti-discrimination] policy set forth in subsection (b) in a manner designed to eliminate underrepresentation of minorities in the various categories of civil service employment within the Federal service, with special efforts directed at recruiting in minority communities, in educational institutions, and from other sources from which minorities can be recruited…."

[2] Until 2010, agencies were also required to submit a separate Hispanic Employment Plan to OPM. However, in September 2010, OPM released a memo, "Subject: Tenth Annual Report to the President on Hispanic Employment" which requests that Hispanic Employment information be submitted with the FEORP report in an effort to consolidate like reports. Complying with this request, NARA has integrated the analysis, goals and strategies Hispanic employment into our FEORP plan.

DEFINITIONS

It is the policy of the National Archives and Records Administration to prohibit discrimination and to ensure equal employment opportunity for all applicants and employees without regard to race, color, religion, sex, sexual orientation and genetics, national origin, age or disability.

DESIGNATION OF RESPONSIBILITY

A. The Chief Human Capital Officer (CHCO), is responsible for:
    1. Overseeing the planning and implementation of this plan;
    2. Communicating the FEORP plan to NARA's managers and employees;
    3. Certifying that the FEORP plan exists and is current; and
    4. Submitting the annual FEORP report to OPM.

B. The Talent Management Division (HT) within the Office of Human Capital is responsible for:
    1. Annually developing and updating the FEORP plan;
    2. Implementing the recruitment strategies and programs identified within the plan; and
    3. Preparing FEORP reports and responding to inquiries about program activities.

C. The Staffing and Recruitment Branch (HTS) within The Office of Human Capital is responsible for:
    1. Conducting recruitment and hiring practices that align with the FEORP plan and promote the advancement of women and minorities; and
    2. Providing advice and assistance to selecting officials when vacancies occur in underrepresented occupations.

D. The Office of Diversity and Inclusion (HD) recommends changes to programs and procedures to eliminate practices that act as barriers to the hiring and advancement of women and minorities.

E. The Learning and Development Division (HL) is responsible for providing developmental opportunities that will support the advancement of women and minorities.

F. Hiring officials are responsible for conducting recruitment and hiring practices that align with this plan and promote the advancement of women and minorities.

Underrepresentation Analysis

national origin (RNO) and gender of our workforce as of October 7, 2011.

When evaluating the composition of our workforce to determine if underrepresentation exists, NARA measures itself against two groups: the Federal Civilian Workforce and the Relevant Civilian Labor Force. The Federal Civilian Workforce is defined by the OPM as full and part-time permanent non-military employees working in non-Postal Executive Branch agencies of the U.S. Government. Measuring ourselves against the FCW enables us to see how our workforce compares to other Federal agencies.

Relevant Civilian Labor Force is defined as those occupations in the Civilian Labor Force (non-institutionalized individuals 16 years of age or older, employed or unemployed, U.S. citizens and non-U.S. citizens) that are directly comparable or relevant to occupations at NARA. Appendix B contains a list of the 54 occupational groups that comprise NARA's RCLF, cross-walked to their corresponding OPM occupational series. Measuring ourselves against the RCLF enables us to compare ourselves against like occupations in the national labor market.

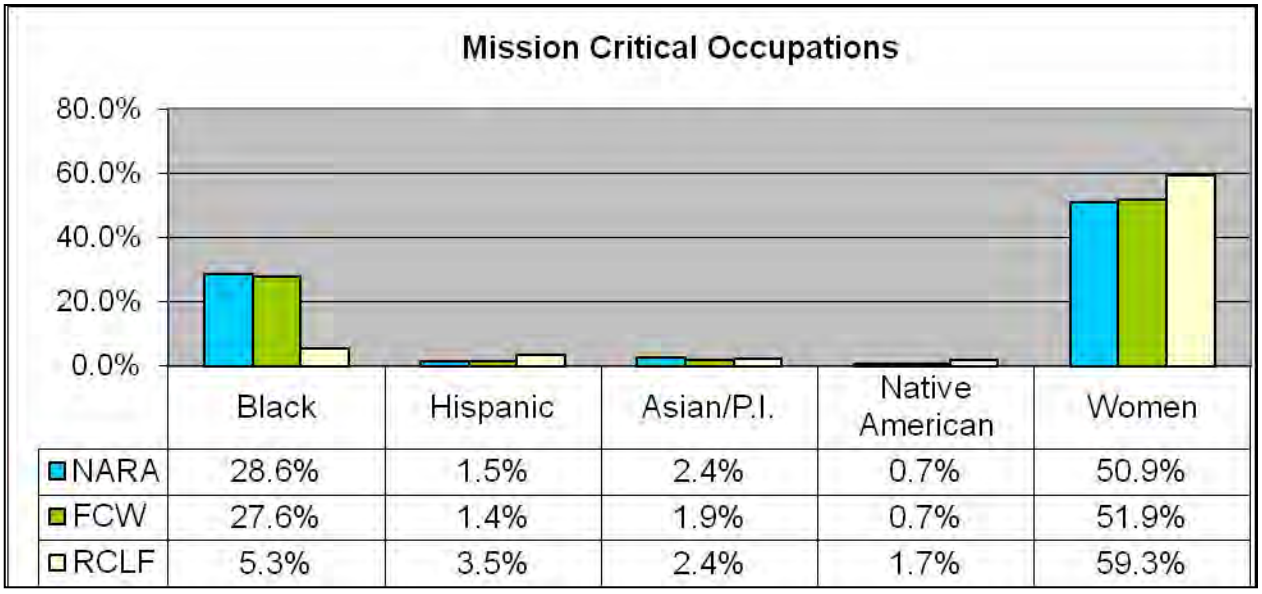
Table 1
Representation of Minorities and Women at NARA

RNO AND GENDER	AGENCY WORKFORCE	
	#	percent
Overall total (includes White non-Hispanics)	**2,723**	**100**
Men	1,301	47.8
Women	1,422	52.2
Total Blacks	**697**	**25.6**
Men	262	37.5
Women	435	62.4
Total Hispanics	**43**	**1.6**
Men	22	51.2
Women	21	48.8
Total Asian/Pacific Islanders	**77**	**2.9**
Men	39	50.6
Women	38	49.3
Total Native Americans	**18**	**0.7**
Men	11	61.0
Women	7	39.0

[3] Total employment includes full-time permanent staff onboard as of October 7, 2011.

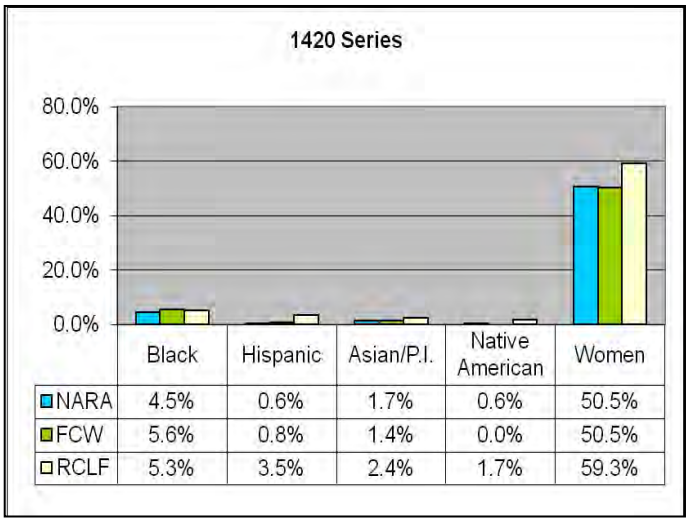
Table 2 compares NARA's workforce to the Relevant Civilian Labor Force. Groups that are underrepresented by comparison to the RCLF (the legal standard of comparison required by 5 CFR 720)

RNO AND GENDER	NARA percent	RCLF percent
Overall total (includes White non-Hispanics)	**100**	**100**
Men	47.8	53.2
Women	52.2	46.8
Total Blacks	**25.6**	**10.5**
Men	9.6	4.8
Women	16.0	5.7
Total Hispanics	**1.6**	**10.7**
Men	.80	6.2
Women	.80	4.5
Total Asian/Pacific Islanders	**2.9**	**3.7**
Men	1.4	1.9
Women	1.5	1.7
Total Native Americans	**0.7**	**1.4**
Men	.40	.70
Women	.30	.70



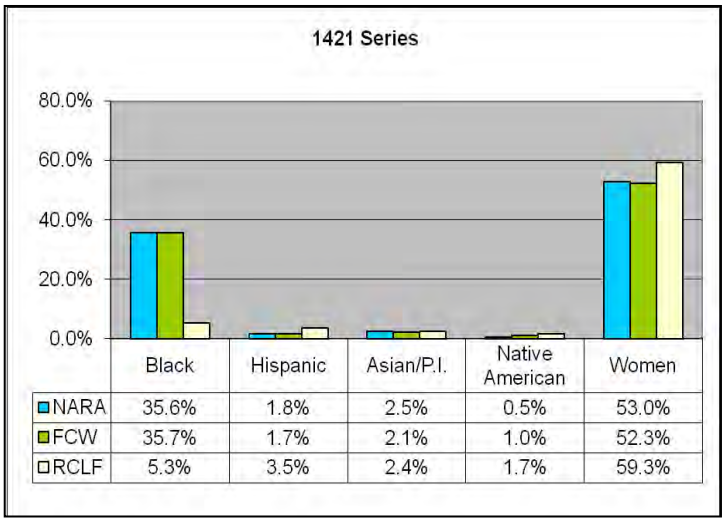
	Black	Hispanic	Asian/P.I.	Native American	Women
NARA	28.6%	1.5%	2.4%	0.7%	50.9%
FCW	27.6%	1.4%	1.9%	0.7%	51.9%
RCLF	5.3%	3.5%	2.4%	1.7%	59.3%

Figure 3



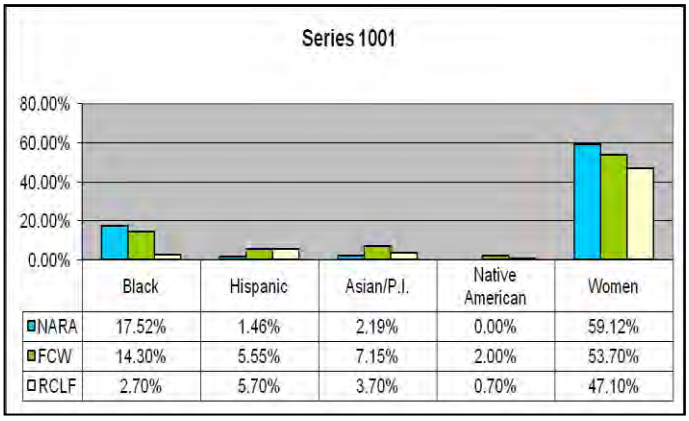
	Black	Hispanic	Asian/P.I.	Native American	Women
NARA	4.5%	0.6%	1.7%	0.6%	50.5%
FCW	5.6%	0.8%	1.4%	0.0%	50.5%
RCLF	5.3%	3.5%	2.4%	1.7%	59.3%

Figure 4

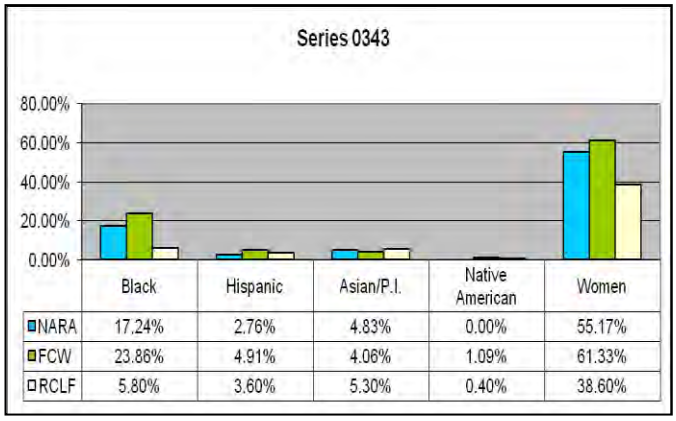


	Black	Hispanic	Asian/P.I.	Native American	Women
NARA	35.6%	1.8%	2.5%	0.5%	53.0%
FCW	35.7%	1.7%	2.1%	1.0%	52.3%
RCLF	5.3%	3.5%	2.4%	1.7%	59.3%

To provide a larger perspective on the composition of NARA's workforce, Figures 5, 6 and 7 show the RNO and gender of the next three largest occupational series within the agency: the GS-1001 General

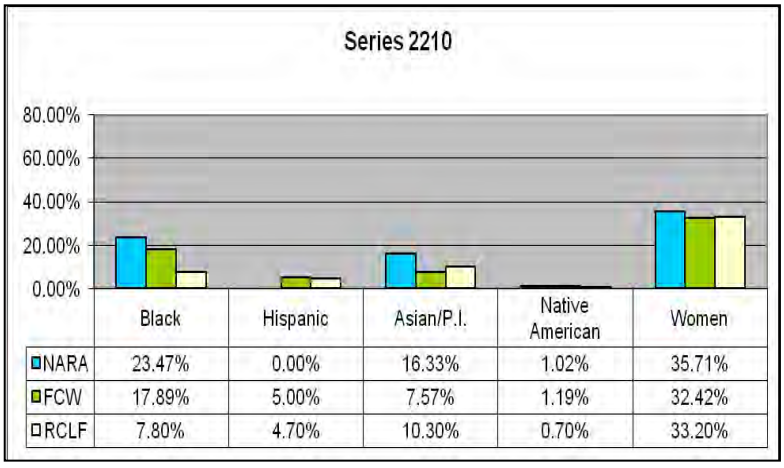


	Black	Hispanic	Asian/P.I.	Native American	Women
NARA	17.52%	1.46%	2.19%	0.00%	59.12%
FCW	14.30%	5.55%	7.15%	2.00%	53.70%
RCLF	2.70%	5.70%	3.70%	0.70%	47.10%



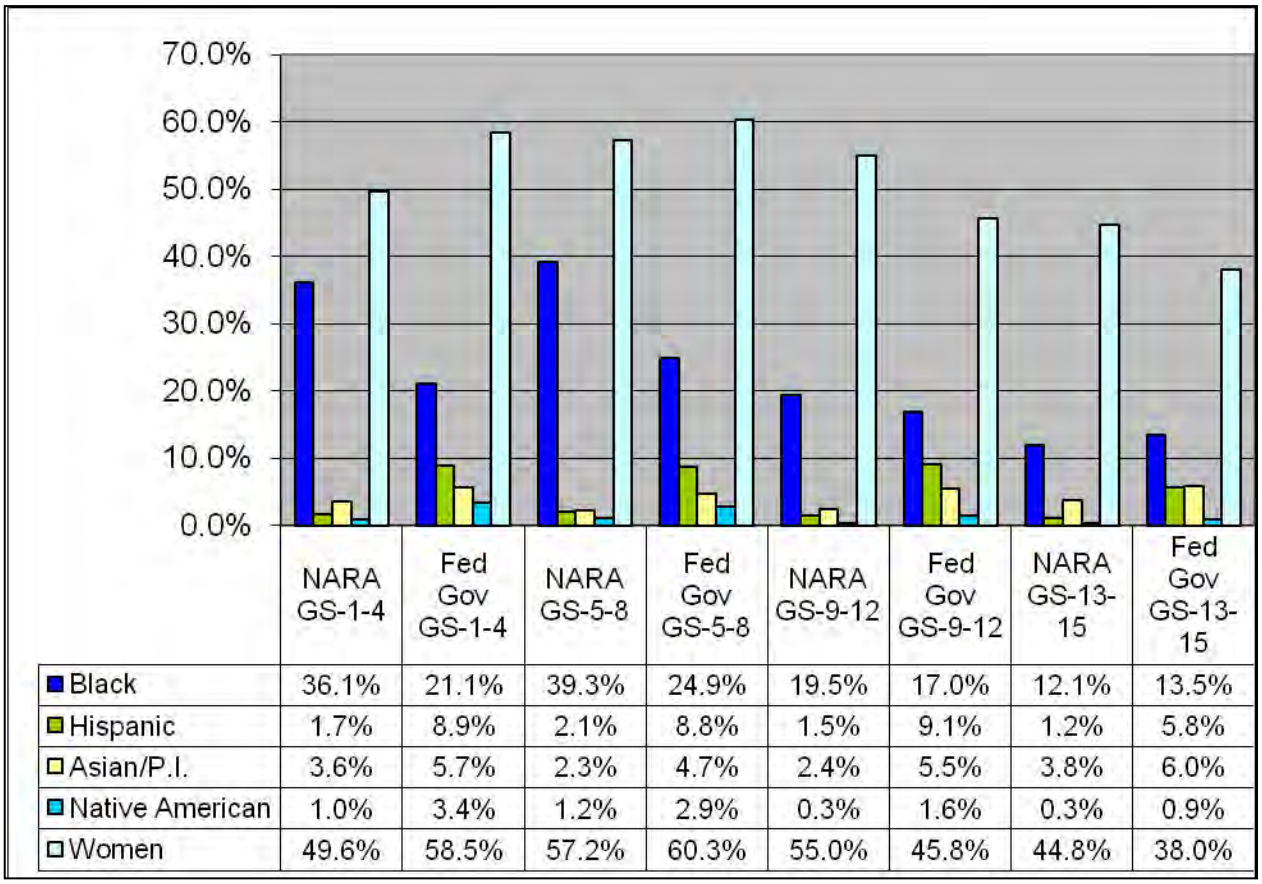
	Black	Hispanic	Asian/P.I.	Native American	Women
NARA	17.24%	2.76%	4.83%	0.00%	55.17%
FCW	23.86%	4.91%	4.06%	1.09%	61.33%
RCLF	5.80%	3.60%	5.30%	0.40%	38.60%

Figure 7



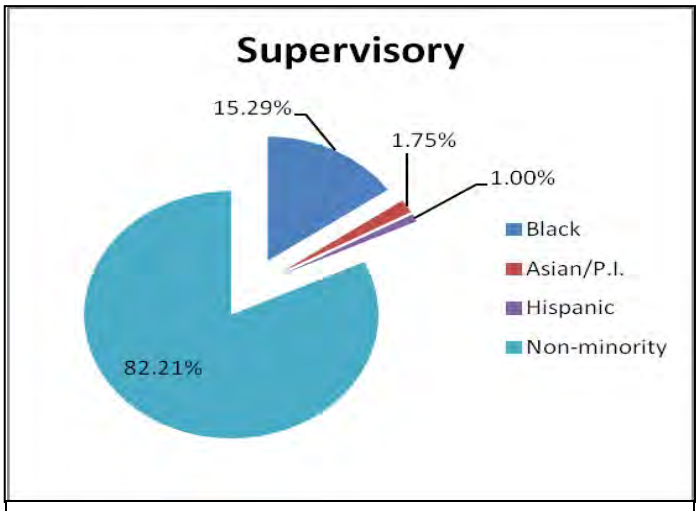
	Black	Hispanic	Asian/P.I.	Native American	Women
NARA	23.47%	0.00%	16.33%	1.02%	35.71%
FCW	17.89%	5.00%	7.57%	1.19%	32.42%
RCLF	7.80%	4.70%	10.30%	0.70%	33.20%

Grade Cluster Information

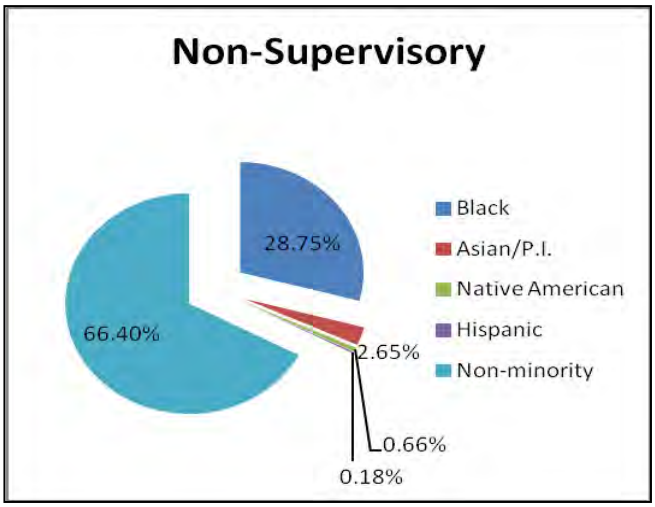


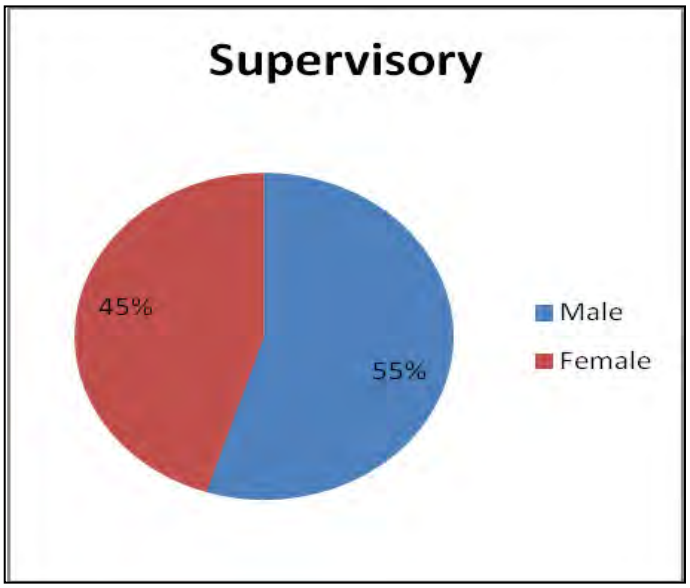
	NARA GS-1-4	Fed Gov GS-1-4	NARA GS-5-8	Fed Gov GS-5-8	NARA GS-9-12	Fed Gov GS-9-12	NARA GS-13-15	Fed Gov GS-13-15
Black	36.1%	21.1%	39.3%	24.9%	19.5%	17.0%	12.1%	13.5%
Hispanic	1.7%	8.9%	2.1%	8.8%	1.5%	9.1%	1.2%	5.8%
Asian/P.I.	3.6%	5.7%	2.3%	4.7%	2.4%	5.5%	3.8%	6.0%
Native American	1.0%	3.4%	1.2%	2.9%	0.3%	1.6%	0.3%	0.9%
Women	49.6%	58.5%	57.2%	60.3%	55.0%	45.8%	44.8%	38.0%

Figure 9
Supervisory vs. Non-supervisory Workforce



*Note Native American not shown (0% representation)





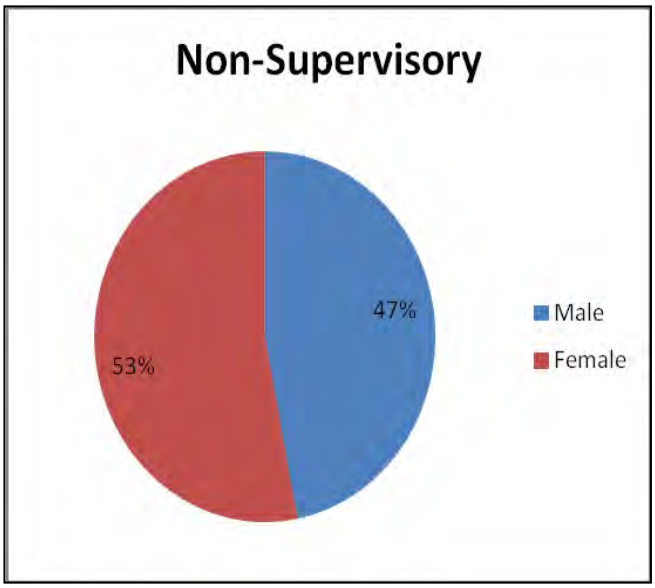
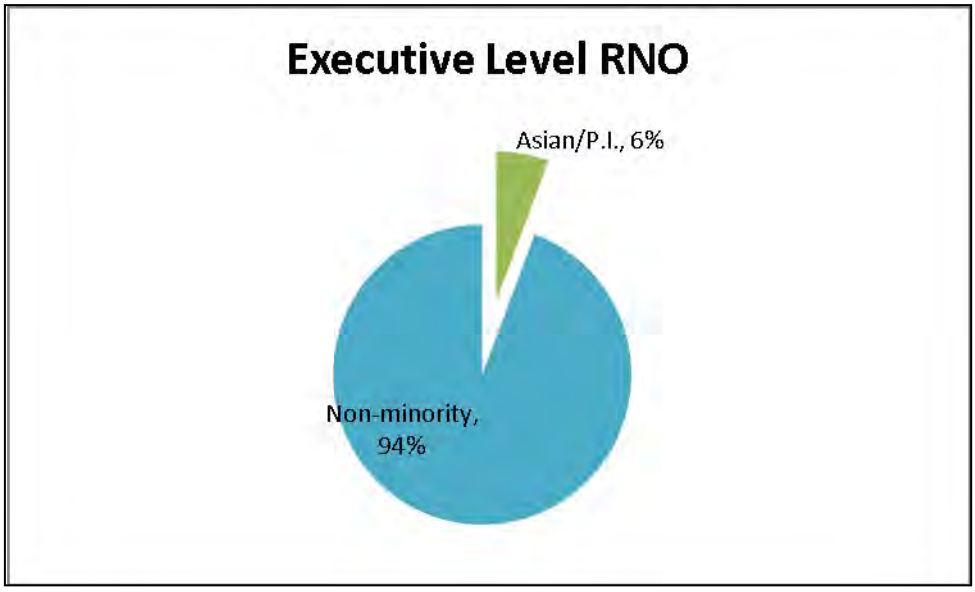
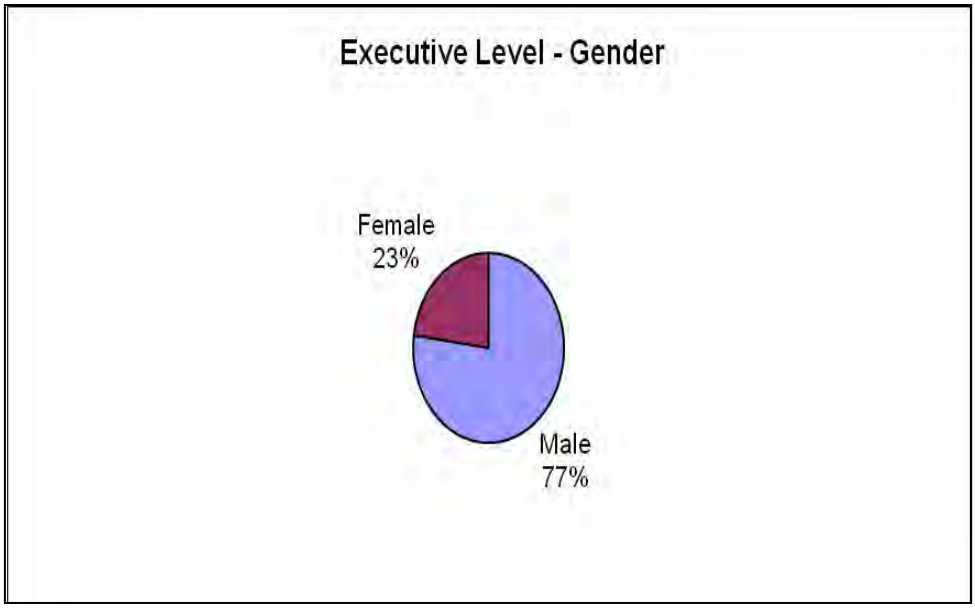


Figure 10
Executive Level RNO and Gender





Findings

Hispanics, who comprise only 1.6 percent of NARA's workforce. Native Americans are likewise underrepresented at all grade levels and across four of NARA's five largest occupational series. Representation rates for Asian/Pacific Islanders vary. For example, Asian/Pacific Islanders comprise six percent of NARA's executive level positions; however, they are consistently underrepresented at all other grade levels.

Our analysis also shows that minorities and women are better represented in the non-supervisory workforce than in the supervisory workforce. Minorities comprise 32 percent of our non-supervisory workforce, and only 18 percent of our supervisory ranks; likewise, women comprise 53 percent of our non-supervisory workforce and 45 percent of supervisory positions.

Progress is needed in increasing the representation of women and minorities at the most senior levels of NARA. As illustrated in Figure 10, minorities comprise just 6 percent of NARA's executive level positions, and women comprise 23 percent of NARA's executive level positions.

Specific findings for each group are outlined below:

BLACKS

Blacks comprise 25.6 percent of NARA's total workforce, exceeding their representation in the FCW and RCLF by 7.7 percent and 15.1 percent respectively. Representation rates for Blacks exceed the FCW across all grade levels, except at the GS 13-15 levels where representation rates are somewhat lower than the FCW. Representation rates for Blacks declined in FY11 in three of NARA's five largest occupational series; GS-1421 (Archives Technician), GS-1001 (General Arts and Information) and the GS-2210 (Information Technology Management) series.

NARA's greatest challenges regarding the representation of Blacks are at the supervisory and executive levels. Blacks comprise 28.7 percent of NARA's non-supervisory workforce, but only 15.2 percent of supervisory positions. Moreover, Blacks are not represented at all among NARA's executive level positions. It is encouraging to note, however, that there was a 1.2 percent increase in representation (14 to 15.2 percent) of Blacks at the supervisory level from last year.

HISPANICS

underrepresentation occurring at the GS 9-12 levels with a difference of 4.8 percent when compared to the FCW.

Hispanics are underrepresented across NARA's five largest occupational series when compared to the RCLF. However, when compared to FCW, Hispanics fare slightly better in the GS-1421 occupational series – exceeding the FCW by .1 percent.

Hispanics comprise .18 percent of NARA's non-supervisory workforce and are represented at a rate of 1 percent within NARA's supervisory positions. Hispanics are not represented at all among NARA's executive level positions.

NARA's greatest challenge in recruiting Hispanics continues to be the exceedingly small number of Hispanics studying in the fields of archives, history, library and information science, and social science – the areas of study from which the majority (58.9 percent) of NARA's workforce is based. Of the approximate 200,000 undergraduate and graduate degrees conferred in the areas of library and information science, social science or history in 2008 - 2009, only 0.86 percent was conferred to Hispanics[4].

ASIAN/PACIFIC ISLANDERS

Asian/Pacific Islanders represent 2.5 percent of NARA's workforce, as compared to 5.5 percent of the Federal workforce and 3.7 percent of the RCLF. In comparison to FY10, representation of this group has increased by .4 percent. Representation rates vary across NARA's five largest occupational series. Within the GS-1421 occupational series, Asian/Pacific Islanders slightly exceed both the FCW and RECLF. Within the GS-1001 series, Asian/Pacific Islanders are only slightly underrepresented when compared to the RCLF, but significantly more underrepresented when compared to the FCW. Within the GS-0343 series, Asian/Pacific Islanders exceed the FCW representation by .77 percent but are underrepresented by .47 percent when compared to the RCLF. This however, is an improvement over FY10 when Asian/Pacific Islanders were not represented all within this occupational series. Asian/Pacific Islanders also continue to exceed both the FCW and the RCLF within the GS-2210 series.

Although Asian/Pacific Islanders represent only 1.7 percent of supervisory positions at NARA, they are the only minority group represented within NARA's executive ranks – representing 6 percent of that workforce.

[4] National Center for Education Statistics, 2008-2009, Tables 297 and 300. 2008 – 2009 is the most recent year for which data is available.

NATIVE AMERICANS

where Native Americans comprise 4.8 percent of the workforce (an increase of 0.3 percent over FY10), exceeding the FCW by the same amount. Native Americans do not hold any supervisory or executive level positions at NARA.

As with Hispanics, one of the challenges NARA faces in recruiting Native Americans is the small number of Native Americans majoring in fields of study that are applicable to NARA's Mission Critical Occupations. Only .80 percent of all undergraduate and graduate degrees conferred in 2008 - 2009 were conferred to Native Americans majoring in library and information science, social science or history.[5]

WOMEN

Women represent 52.3 percent of NARA's workforce, exceeding their representation in the FCW and RCLF by 8.6 and 5.5 percent respectively.

Women comprise 50.9 percent of NARA's MCOs, an increase of 2.9 percent over FY10. However, women exceed the RCLF for NARA's three other largest occupational series – the GS-1001 series, GS-0343 series, and GS-2210 series, and the FCW in two of those series (GS-1001 and GS-2210).

NARA leads the FCW in female representation at the GS 9-12 and GS 13-15 levels. However, women are underrepresented at the GS 1-4 and GS 5-8 levels. This is an improvement over FY10 when the FCW led NARA in female representation at all but the GS 5-8 level. Women comprise 53 percent of the non-supervisory workforce and 45 percent of supervisory positions. Women comprise 23 percent of NARA's executive positions, a decrease of 3 percent when compared to FY10.

[5] National Center for Education Statistics, 2008-2009, Tables 297 and 300. 2008 – 2009 is the most recent year for which data is available.

Trend Analysis

and gender of our Mission Critical Occupations (MCOs), RNO and gender of NARA's next three largest occupational series (GS-1001 General Arts and Information series, GS-0343 Management and Program Analysts series, and GS-2210 Information Technology Management series), grade-cluster data, and the composition of our supervisory/non-supervisory workforce as well as our executive level positions.

These areas are discussed in detail below.

NARA's Workforce Composition

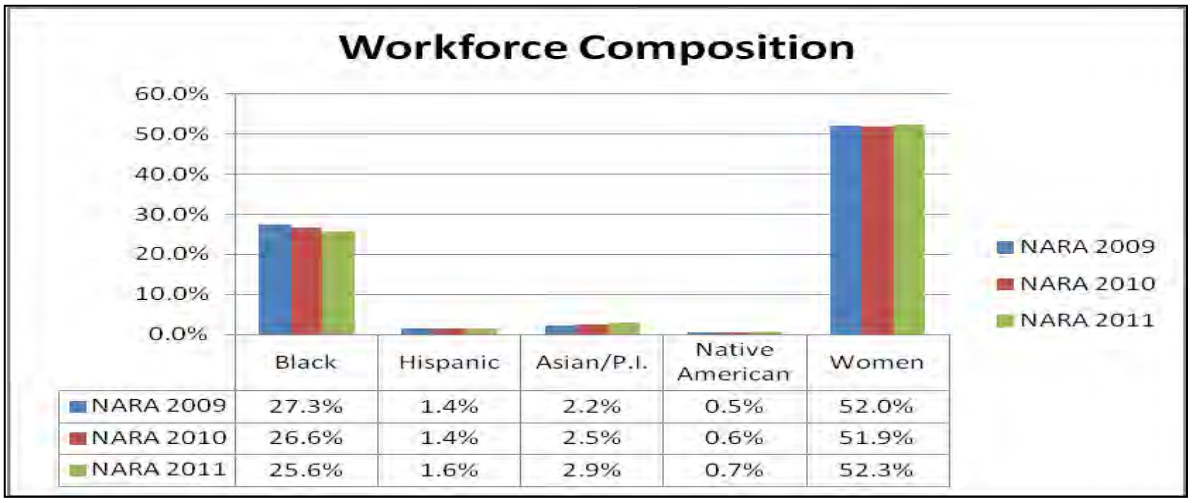
Overall minority representation has remained relatively stable over the three-year period, as shown in Figure 11 below.

Representation of Blacks within NARA's workforce has declined slightly each year - down 1.7 compared to FY2009 and 1.0 percent compared to FY2010. Despite this decrease, Blacks continue to exceed both the FCW and RCLF over the three-year analysis period.

Hispanic representation had remained consistent at 1.4 percent for FY2009 and FY2010. In FY11 there was slight increase (up .2 percent) to 1.6 percent in FY11. Representation of Asian/Pacific Islanders has shown the greatest improvement, with slight increases each year over the three-year period.

Native American representation has increased slightly each year, for a net increase of .2 percent over the three-year analysis period.

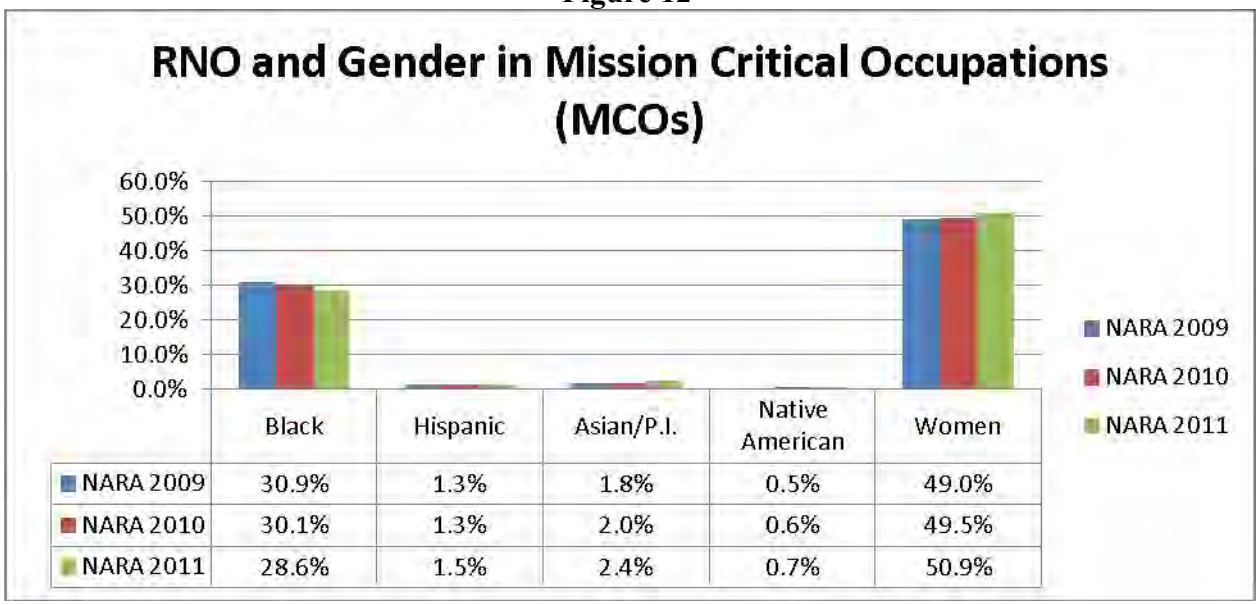
Figure 11



	Black	Hispanic	Asian/P.I.	Native American	Women
NARA 2009	27.3%	1.4%	2.2%	0.5%	52.0%
NARA 2010	26.6%	1.4%	2.5%	0.6%	51.9%
NARA 2011	25.6%	1.6%	2.9%	0.7%	52.3%

As shown in Figure 12 below, representation of Blacks declined from 30.9% in 2009 to 30.1% in 2010 and 28.6% in 2011, while all other races and women either stayed the same or slightly increased at the end of the analysis period. While we are cognizant of the decline in Black representation levels, we also recognize that we continue to considerably exceed the representation of Blacks in these occupations when compared to the RCLF – by an average of 24.5 percent over the three year period.

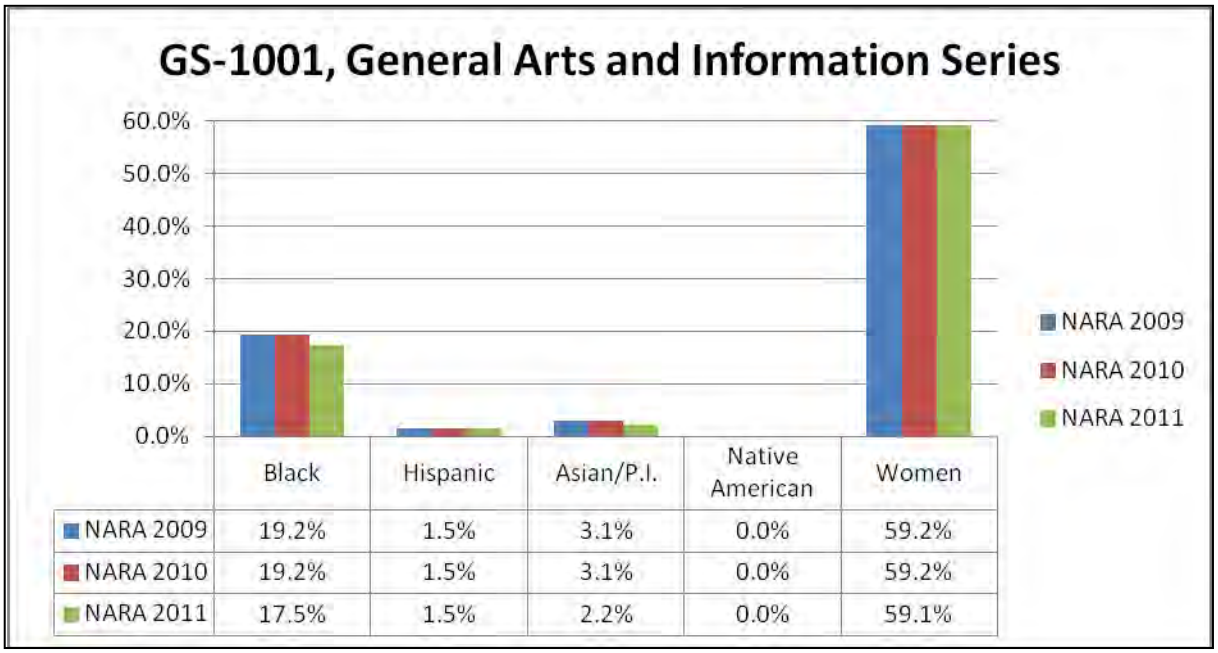
Figure 12



	Black	Hispanic	Asian/P.I.	Native American	Women
NARA 2009	30.9%	1.3%	1.8%	0.5%	49.0%
NARA 2010	30.1%	1.3%	2.0%	0.6%	49.5%
NARA 2011	28.6%	1.5%	2.4%	0.7%	50.9%

GS-1001, General Arts and Information Series – Representation of women, Hispanics, and Native Americans has not changed. Representation of Blacks and Asian /Pacific Islanders has declined slightly.

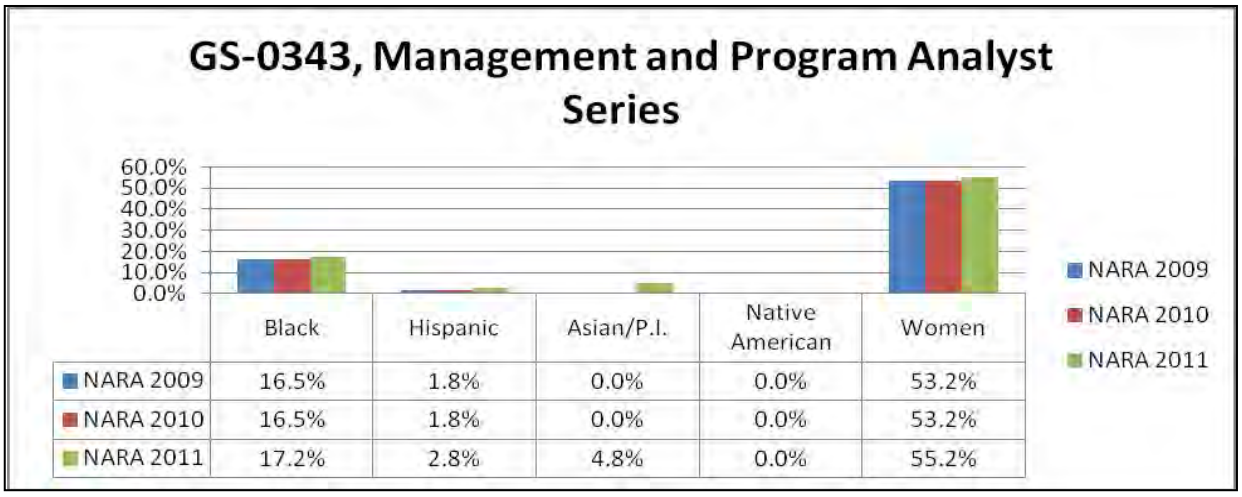
Figure 13



	Black	Hispanic	Asian/P.I.	Native American	Women
NARA 2009	19.2%	1.5%	3.1%	0.0%	59.2%
NARA 2010	19.2%	1.5%	3.1%	0.0%	59.2%
NARA 2011	17.5%	1.5%	2.2%	0.0%	59.1%

GS-0343, Management and Program Analyst Series - When comparing NARA's workforce in the

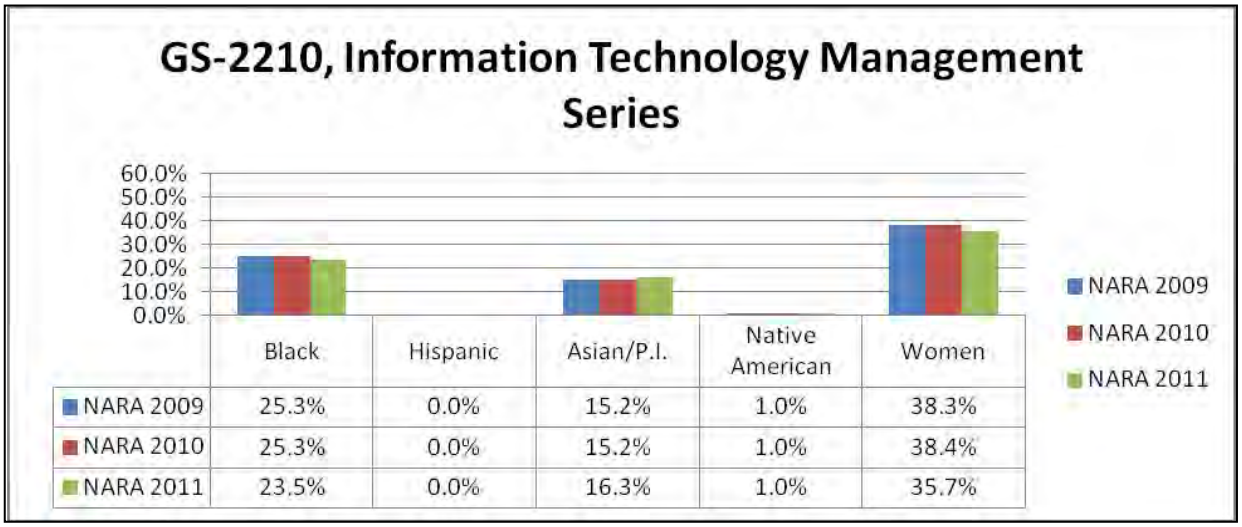
Figure 14



	Black	Hispanic	Asian/P.I.	Native American	Women
NARA 2009	16.5%	1.8%	0.0%	0.0%	53.2%
NARA 2010	16.5%	1.8%	0.0%	0.0%	53.2%
NARA 2011	17.2%	2.8%	4.8%	0.0%	55.2%

GS-2210, Information Technology Management Series - Over the course of the three-year analysis period, Hispanics have had no representation in this occupational series. There has been a slight decrease in representation amongst Blacks and Women. Representation of Asian/Pacific Islanders, on the other hand, maintained representation from FY09 to FY10 at 15.2% and increased by 1.1 percent in FY11.

Figure 15



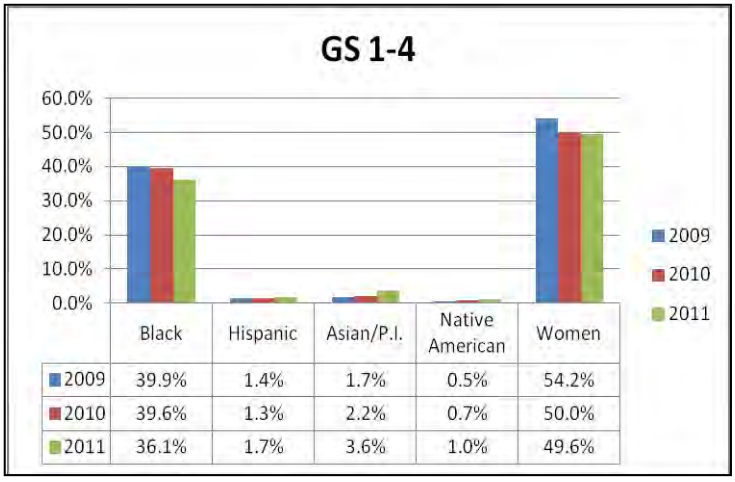
	Black	Hispanic	Asian/P.I.	Native American	Women
NARA 2009	25.3%	0.0%	15.2%	1.0%	38.3%
NARA 2010	25.3%	0.0%	15.2%	1.0%	38.4%
NARA 2011	23.5%	0.0%	16.3%	1.0%	35.7%

NARA's Grade-Cluster Data

The following figures (16-19) compare the grade cluster data over the course of the three-year analysis.

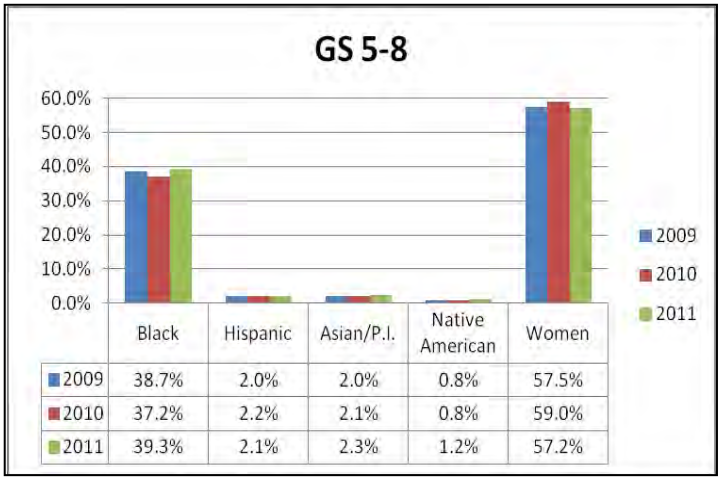
Figures 16-19 Grade Cluster Information

Figure 16



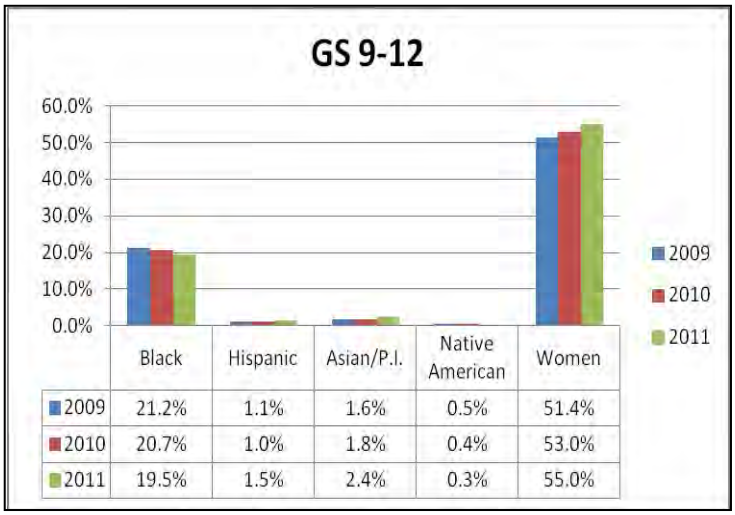
	Black	Hispanic	Asian/P.I.	Native American	Women
2009	39.9%	1.4%	1.7%	0.5%	54.2%
2010	39.6%	1.3%	2.2%	0.7%	50.0%
2011	36.1%	1.7%	3.6%	1.0%	49.6%

Figure 17



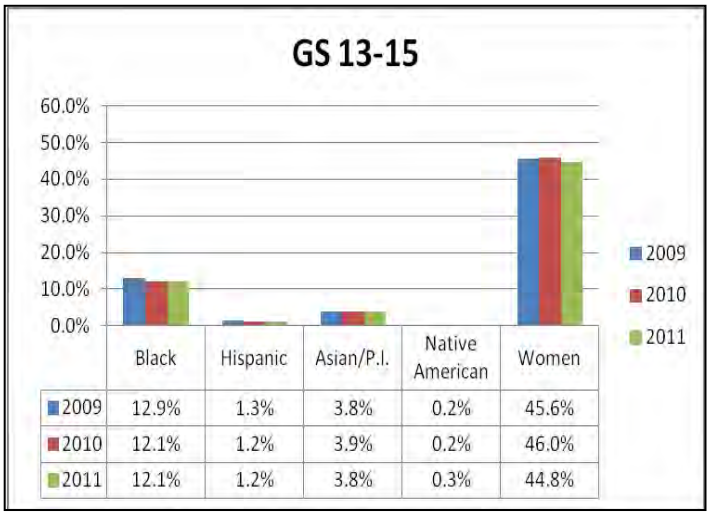
	Black	Hispanic	Asian/P.I.	Native American	Women
2009	38.7%	2.0%	2.0%	0.8%	57.5%
2010	37.2%	2.2%	2.1%	0.8%	59.0%
2011	39.3%	2.1%	2.3%	1.2%	57.2%

Figure 18



	Black	Hispanic	Asian/P.I.	Native American	Women
2009	21.2%	1.1%	1.6%	0.5%	51.4%
2010	20.7%	1.0%	1.8%	0.4%	53.0%
2011	19.5%	1.5%	2.4%	0.3%	55.0%

Figure 19

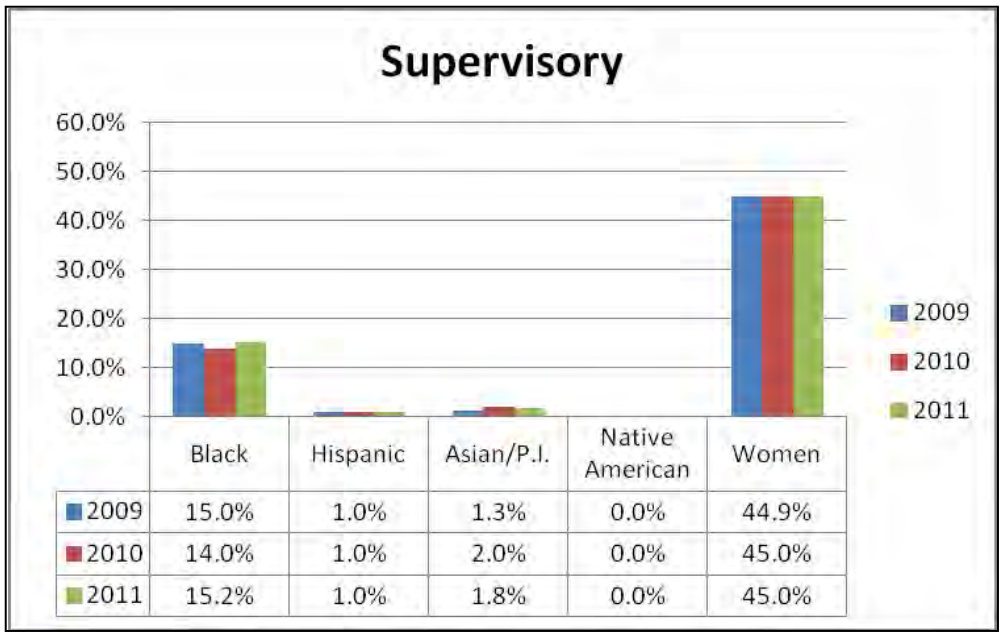


	Black	Hispanic	Asian/P.I.	Native American	Women
2009	12.9%	1.3%	3.8%	0.2%	45.6%
2010	12.1%	1.2%	3.9%	0.2%	46.0%
2011	12.1%	1.2%	3.8%	0.3%	44.8%

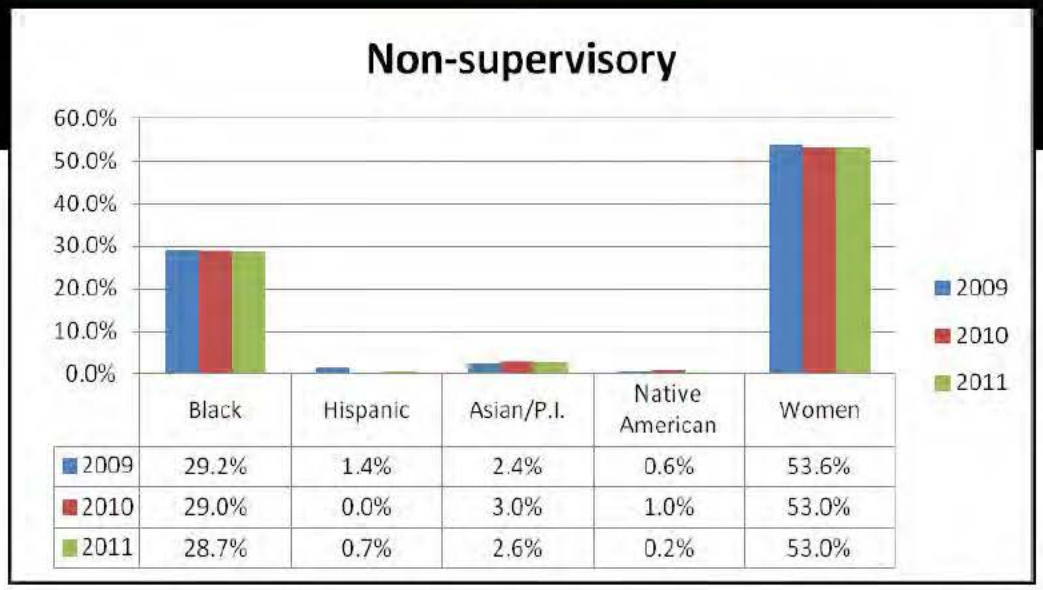
the executive level over the three-year analysis period. The representation of Asian/Pacific Islanders has remained stable. Representation of women has fluctuated from 24.2 percent in 2009 to 26 percent in 2010 and 23 percent in 2011. While these increases are hopeful, there is still room for improvement. As we move forward it will important to communicate these trends and findings and develop strategies to increase representation of minorities across the board at executive levels.

Figures 20 - 22
Supervisory/Non-supervisory and Executive Level Workforce

Figure 20

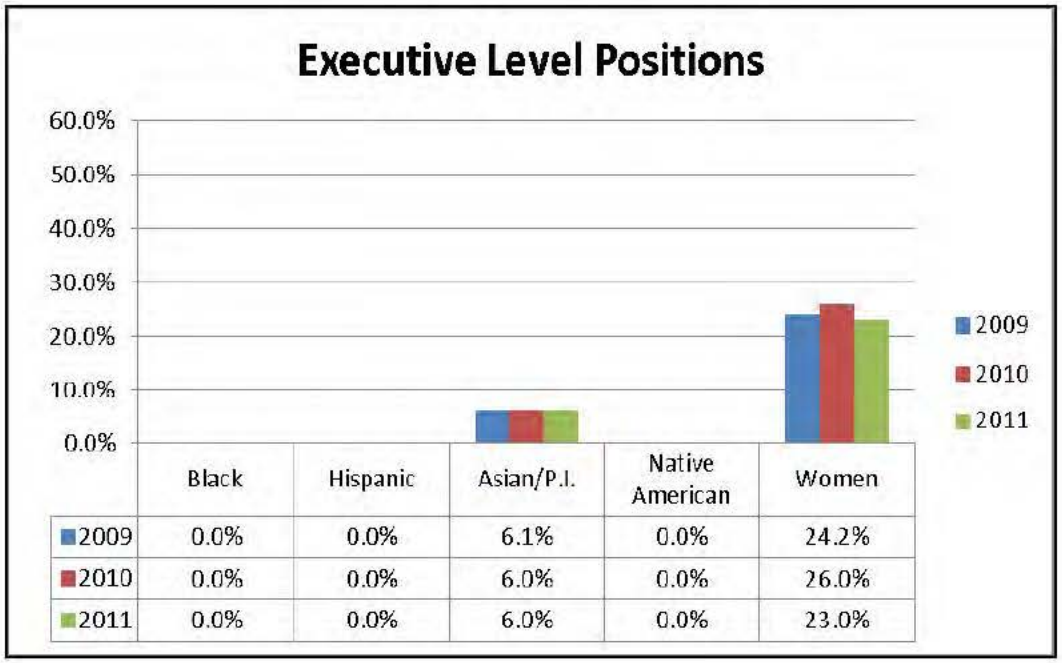


	Black	Hispanic	Asian/P.I.	Native American	Women
2009	15.0%	1.0%	1.3%	0.0%	44.9%
2010	14.0%	1.0%	2.0%	0.0%	45.0%
2011	15.2%	1.0%	1.8%	0.0%	45.0%



	Black	Hispanic	Asian/P.I.	Native American	Women
2009	29.2%	1.4%	2.4%	0.6%	53.6%
2010	29.0%	0.0%	3.0%	1.0%	53.0%
2011	28.7%	0.7%	2.6%	0.2%	53.0%

Figure 22



	Black	Hispanic	Asian/P.I.	Native American	Women
2009	0.0%	0.0%	6.1%	0.0%	24.2%
2010	0.0%	0.0%	6.0%	0.0%	26.0%
2011	0.0%	0.0%	6.0%	0.0%	23.0%

that we have had minimal variation in minority representation throughout the analysis period.

While our strategies appear to be effective in maintaining the representation of minorities and women, the data suggests that new and/or additional strategies, including an in-depth analysis of barriers, may be needed in order to yield significant changes going forward. In addition, the lack of minority candidates majoring in the fields of study applicable to the majority of NARA's workforce continues to be a challenge.

Goals & Strategies

that together form the foundation for improving our recruitment strategy for women and minorities:

- **Ensure that FEORP goals are aligned with NARA's Strategic Plan and Strategic Human Capital Plan and integrated with workforce planning efforts;**
- **Expand the pipeline of women and minorities available for employment with NARA; and**
- **Enhance staff development opportunities that prepare staff for upper level positions.**

In support of these goals, we have identified 14 specific strategies that NARA will undertake in Fiscal Year 2012 to enhance the representation of women and minorities at all levels. These strategies are discussed in detail on the following pages.

Several of these strategies are a continuation from previous years. However, as mentioned previously in this report, NARA recognizes the need to identify additional new strategies and further analyze barriers if we are to make significant improvements versus simply maintaining our current rates of minority representation.

Progress against our goals and strategies will be assessed each year as part of our human capital accountability efforts and OPM's annual FEORP reporting requirement. In addition, this plan will be revised each year to reflect our latest workforce demographics and the strategies will be updated as necessary to address any underrepresentation at NARA.

GOAL 1

Ensure that FEORP goals are aligned with NARA's Strategic Plan and Strategic Human Capital Plan and integrated with workforce planning efforts.

In FY2011 NARA began work on a workforce planning infrastructure that will enable managers to better understand the composition of their workforce, anticipate retirements and other attrition, and plan for projected vacancies.

The purpose of this goal is to ensure that the recruitment goals outlined in NARA's FEORP plan are fully aligned with the goals of NARA's Strategic Human Capital Plan and, by extension, NARA's Strategic Plan. This alignment is critical to ensuring that diversity recruitment goals are met. Appendix C documents the linkage between NARA's FEORP, Strategic Human Capital Plan, and Strategic Plan. The following strategies support NARA's overall strategic plan and will ensure that we have the infrastructure in place to plan for and prioritize human capital needs in Fiscal Year 2012.

Through our strategic diversity planning efforts, we intend to remain focused on creating solutions that support an inclusive work environment, develop continual improvement in workforce representation, strengthen employee talent through diversity recruiting, hiring and retention, ensuring a diverse leadership pipeline through employee development and promoting and holding management accountability for diversity at all levels.

STRATEGIES

1.1 Analyze and incorporate EEO data (e.g., workforce demographics, hiring statistics, and turnover statistics) as a formal component of NARA's workforce planning process.

1.2 Continue to work with program offices to identify the human capital required to meet organizational goals, analyze competency gaps in mission-critical occupations, develop strategies to address human capital needs and include the agency's diversity recruitment goals.

1.3 Develop and implement an agency-wide diversity strategic plan to provide a formulated approach to increasing minority, female and Veteran representation throughout NARA and in upper management positions and hold hiring managers, supervisors and upper management accountable for implementing strategies and reaching identified goals.

1.4 Continue to work with NARA's EEO office as they pursue assistance from the Equal Employment Opportunity Commission and USAStaffing to create a government-wide applicant flow data tool.

GOAL 2

Maintain a diverse high-performing workforce by effectively recruiting, hiring and retaining top talent.

NARA places a particular emphasis on recruiting for our Mission Critical Occupations – Archivists, Archives Specialists, and Archives Technicians – since these occupations comprise the largest percentage (58.9 percent) of our permanent workforce and thus, the most opportunities to enhance diversity.

NARA targets its recruitment outreach efforts to organizations that represent highly qualified diverse applicants in the fields of archives, library and information science, and history. We utilize a variety of outreach methods and tools in an attempt to reach the broadest cross-section of applicants. These include: attending career fairs and professional networking events; posting recruitment advertisements on diversity websites; and attending resume workshops and related career events in partnership with universities and minority-serving organizations and hosting interns through our Summer Diversity Internship program.

Through our Summer Diversity Internship Program, NARA reaches out to minority-serving organizations to fund internship opportunities for talented minorities. In FY 2011, we sponsored 12 highly qualified diverse candidates through the Hispanic Association of Colleges and Universities (HACU) National Internship Program and ten students through The Washington Center (TWC) internship program.

Beyond the recruitment efforts in place, NARA recognizes the need to hire and retain a diverse workforce. Therefore, strategies will be implemented in FY12 that will provide the necessary training to supervisors and managers in understanding the benefit of hiring and retaining a diverse workforce. Having a diverse applicant pool alone will not increase minority representation at NARA; we must actually hire some of these diverse candidates and work to retain new and current minorities.

STRATEGIES

2.1 Continue to utilize minority serving intern organizations in order to build a diverse talent pool.

2.2 Expand NARA's network of recruiters (referred to as Diversity Champions), including issuing guidance that emphasizes diversity as a recruitment factor.

2.3 Attend and network at the following minority conferences and career fairs in Fiscal Year 2012:

- American Legion Veterans Career Fair.

2.4 Strengthen relationships with Hispanic-Serving Institutions (HSIs), Historically Black Colleges and Universities (HBCUs), and Tribal Colleges and Universities (TCUs) through education of NARA's mission and promotion of internship and employment opportunities at NARA.

2.5 Continue to maximize the visibility of vacancy announcements by posting them on USAJobs.gov, NARA's career website and with universities/organizations with a high concentration of minorities and/or female students, alumni and/or members.

2.6 Conduct benchmarking efforts in order to better understand and implement strategies that have yielded other Federal agencies successes in the areas of minority recruitment, hiring and retention.

GOAL 3

Enhance staff development opportunities that prepare staff for upper level positions.

NARA depends on leaders who possess the knowledge, skills, and abilities to effectively lead our workforce in support of NARA's mission. We are committed to developing our leadership capacity and to ensuring continuity in leadership even as key players retire or move to new responsibilities. To do this, we recognize that we must have systems and processes in place to bring forth new, highly competent, diverse leaders.

As NARA moves forward with the development of our workforce planning infrastructure, we will be systematically identifying our current and future leadership needs and the leadership competencies and talent sources available to meet those needs. We will also be using the results of that analysis to design and implement development opportunities that prepare staff for upper level positions, paying close attention to the need for diversity among our supervisory and executive ranks.

STRATEGIES

3.1 Encourage supervisors/managers to consider the use of developmental assignments and/or detail opportunities as tools for resourcing special projects that, in turn, provide minority and/or female employees the opportunity to gain experience in higher graded occupations.

3.2 Increase awareness of the benefits of a diverse workforce at NARA's manager/supervisor training and encourage upward mobility of minorities and women.

3.3 Develop mentoring programs that will enable employees to broaden skill sets; exposing them to a wider scope of activities performed by NARA thereby expanding their visibility and personal networks throughout the agency.

3.4 Educate and promote awareness among employees about available opportunities to participate in a mentoring program, either as a mentor or mentee.

Appendix A – Definitions

Accountability: A data-driven results-oriented planning system.

performance and to organizational success.

Diversity or Workplace diversity: Covers gender, age, disability, language, ethnicity, cultural background, sexual preference, religious belief and family responsibilities. Diversity also refers to the other ways in which people are different, such as educational level, life experience, work experience, socio-economic background, personality, marital status and abilities/disabilities. Workplace diversity involves recognizing the value of individual differences and managing them in the workplace.

Federal Civilian Workforce (FCW): Covers full and part-time permanent employees in non-Postal Executive Branch Agencies participating in Central Personnel Data File (CPDF). CPDF coverage is limited to Federal civilian employees.

Federal Equal Opportunity Recruitment Program (FEORP): A recruiting initiative designed to eliminate underrepresentation of minorities and women in the Federal service.

Gaps: Amount by which workforce needs (future state) exceed current resources. These resources should be essential for NARA to carry out its mission and accomplish its strategic goals.

Minorities: All categories of current and potential employees identified as non-white.

Mission Critical Occupation: An occupation that is so critical to NARA's mission, that if it ceased to exist NARA could not accomplish its statutory mission and related statutes, the vision articulated in NARA's Strategic Plan, and the mission articulated in NARA's Strategic Plan.

Relevant Civilian Labor Force (RCLF): Occupational groups that are directly comparable or relevant to occupational groups at NARA.

Underrepresentation: A situation in which the number of women or members of a minority group within a category of civil service employment constitutes a lower percentage of the total number of employees within the employment category than the percentage that women or the minority group constitutes within the civilian labor force of the United States.

Appendix B – Relevant Civilian Labor Force Crosswalk

18	SAFETY & OCCUPATIONAL HEALTH MANAGEMENT	354	OTHER HEALTHCARE PRACTITIONERS & TECHNICAL OCCUPATIONS
80	SECURITY ADMINISTRATION	73	OTHER BUSINESS OPERATIONS SPECIALISTS
170	HISTORY	186	MISCELLANEOUS SOCIAL SCIENTISTS, INCLUDING SOCIOLOGISTS
201	HUMAN RESOURCES MANAGEMENT	62	HUMAN RESOURCES, TRAINING & LABOR RELATIONS SPECIALISTS
203	HUMAN RESOURCES CLERICAL & ASSISTANCE	536	TIMEKEEPING
260	EQUAL EMPLOYMENT OPPORTUNITY	56	COMPLIANCE OFFICERS
301	MISCELLANEOUS ADMINISTRATION & PROGRAM	73	OTHER BUSINESS OPERATIONS SPECIALISTS
303	MISCELLANEOUS CLERK & ASSISTANT	593	OFFICE & ADMINISTRATIVE SUPPORT WORKERS, ALL OTHER
305	MAIL & FILE	526	FILE CLERKS
318	SECRETARY	570	SECRETARIES & ADMINISTRATIVE ASSISTANTS
322	CLERK-TYPIST	582	WORD PROCESSORS & TYPISTS
326	OFFICE AUTOMATION CLERICAL AND ASSISTANCE	582	WORD PROCESSORS & TYPISTS
334	COMPUTER SPECIALIST	100	COMPUTER SCIENTISTS AND SYSTEMS ANALYST
335	COMPUTER CLERK & ASSISTANT	104	COMPUTER SUPPORT SPECIALISTS

340	PROGRAM MANAGEMENT	73	OTHER BUSINESS OPERATIONS SPECIALISTS
342	SUPPORT SERVICES ADMINISTRATION	10	ADMINISTRATIVE SERVICES MANAGERS
343	MANAGEMENT PROGRAM ANALYSIS	71	MANAGEMENT ANALYSTS
344	MANAGEMENT & PROGRAM CLERICAL & ASSISTANCE	593	OFFICE & ADMINISTRATIVE SUPPORT WORKERS, ALL OTHER
346	LOGISTICS MANAGEMENT	70	LOGISTICIANS
350	EQUIPMENT OPERATOR	511	BILLING & POSTING CLERKS & MACHINE OPERATORS
356	DATA TRANSCRIBER	581	DATA ENTRY KEYERS
361	EQUAL OPPORTUNITY ASSISTANCE	593	OFFICE & ADMINISTRATIVE SUPPORT WORKERS, ALL OTHER
390	TELECOMMUNICATIONS PROCESSING	503	COMMUNICATIONS EQUIPMENT OPERATORS, ALL OTHERS
391	TELECOMMUNICATIONS	290	BROADCAST & SOUND ENGINEERING TECHNICIANS
501	FINANCIAL ADMINISTRATION & PROGRAM	95	FINANCIAL SPECIALISTS, ALL OTHER
503	FINANCIAL CLERICAL & TECHNICIAN	512	BOOKKEEPING, ACCOUNTING & AUDITING CLERKS
505	FINANCIAL MANAGEMENT	95	FINANCIAL SPECIALISTS, ALL OTHER
510	ACCOUNTING	80	ACCOUNTANTS & AUDITORS
511	AUDITING	80	ACCOUNTANTS & AUDITORS
525	ACCOUNTING TECHNICIAN	512	BOOKKEEPING, ACCOUNTING, & AUDITING CLERKS
530	CASH PROCESSING	472	CASHIERS

560	BUDGET ANALYSIS	82	BUDGET ANALYSTS
			INCLUDING AGRICULTURAL & BIOMEDICAL
808	ARCHITECTURE	130	ARCHITECTS
854	COMPUTER ENGINEERING	140	COMPUTER HARDWARE ENGINEERS
855	ELECTRONICS ENGINEERING	141	ELECTRICAL & ELECTRONIC ENGINEERS
904	LAW CLERK	215	MISC. LEGAL SUPPORT WORKERS
905	GENERAL ATTORNEY	210	LAWYERS
0	PARALEGAL SPECIALIST	214	PARALEGALS & LEGAL ASSISTANTS
1001	GENERAL ARTS & INFORMATION	260	ARTISTS & RELATED WORKERS
1010	EXHIBITS SPECIALIST	263	DESIGNERS
1015	MUSEUM CURATOR	240	ARCHIVISTS, CURATORS & MUSEUM TECHNICIANS
1016	MUSEUM SPECIALIST & TECHNICIAN	240	ARCHIVISTS, CURATORS & MUSEUM TECHNICIANS
1035	PUBLIC AFFAIRS	282	PUBLIC RELATIONS SPECIALISTS
1060	PHOTOGRAPHY	291	PHOTOGRAPHERS
1071	AUDIOVISUAL PRODUCTION	271	PRODUCERS & DIRECTORS
1082	WRITING & EDITING	285	WRITERS & AUTHORS
1083	TECHNICAL WRITING & EDITING	284	TECHNICAL WRITERS
1084	VISUAL INFORMATION	263	DESIGNERS
1101	GENERAL BUSINESS & INDUSTRY	73	OTHER BUSINESS OPERATIONS SPECIALISTS

1102	CONTRACTING	53	PURCHASING AGENTS, EXCEPT WHOLESALE, RETAIL & FARM
1310	PHYSICS	170	ASTRONOMERS & PHYSICISTS
1320	CHEMISTRY	172	CHEMISTS & MATERIALS SCIENTISTS
1410	LIBRARIAN	243	LIBRARIANS
1411	LIBRARY TECHNICIAN	244	LIBRARY TECHNICIANS
1412	TECHNICIAN INFORMATION SERVICES	244	LIBRARY TECHNICIANS
1420	ARCHIVIST	240	ARCHIVISTS, CURATORS & MUSEUM TECHNICIANS
1421	ARCHIVES TECHNICIAN	240	ARCHIVISTS, CURATORS & MUSEUM TECHNICIANS
1499	LIBRARY & ARCHIVES STUDENT TRAINEE	255	OTHER EDUCATION, TRAINING & LIBRARY WORKERS
1550	COMPUTER SCIENCE	100	COMPUTER SCIENTISTS & SYSTEMS ANALYSTS
1601	EQUIPMENT, FACILITIES, & SERVICES	73	OTHER BUSINESS OPERATIONS SPECIALISTS
1640	FACILITY OPERATIONS	22	CONSTRUCTION MANAGERS
1654	PRINTING MANAGEMENT	10	ADMINISTRATIVE SERVICES MANAGERS
1701	GENERAL EDUCATION & TRAINING	234	OTHER TEACHERS & INSTRUCTORS
1702	EDUCATION & TRAINING TECHNICIAN	255	OTHER EDUCATION, TRAINING & LIBRARY WORKERS
1712	TRAINING INSTRUCTION	234	OTHER TEACHERS & INSTRUCTORS
1750	INSTRUCTIONAL SYSTEMS	255	OTHER EDUCATION, TRAINING & LIBRARY WORKERS

1811	CRIMINAL INVESTIGATING	382	DETECTIVES & CRIMINAL INVESTIGATORS
2001	GENERAL SUPPLY	73	OTHER BUSINESS OPERATIONS SPECIALISTS
2010	INVENTORY MANAGEMENT	70	LOGISTICIANS
2091	SALES STORE CLERICAL	476	RETAIL SALESPERSONS
2210	INFORMATION TECHNOLOGY MANAGEMENT	100	COMPUTER SCIENTISTS & SYSTEMS ANALYSTS
3306	OPTICAL INSTRUMENT REPAIRING	743	PRECISION INSTRUMENT & EQUIPMENT REPAIRERS
3502	LABORING	962	LABORERS & FREIGHT, STOCK, & MATERIAL MOVERS, HAND
5301	MISC. INDUSTRIAL EQUIP. MAINTENANCE	NA	NA
5703	MOTOR VEHICLE OPERATING	915	MISCELLANEOUS MOTOR VEHICLE OPERATORS
6907	MATERIALS HANDLER	975	MISCELLANEOUS MATERIAL MOVING WORKERS

Strategic Goals Crosswalk	Strategic Goal 6: NARA Strategic Goal 6: We will equip NARA to meet the changing needs of our customers	
	6.1: By 2016, 95 percent of employees possess the core competencies that were identified for their jobs	6.2: By 2016, the percentages of NARA employees underrepresented groups match their respective availability levels in the Civilian Labor Force (CLF)
NARA FEORP Goals		
	1.0 Ensure that FEORP goals are aligned with NARA's Strategic Plan and Strategic Human Capital Plan and integrated with workforce planning efforts.	**2.0** Expand the pipeline of women and minorities available for employment with NARA.	**3.0** Enhance staff development opportunities that prepare staff for upper level positions.
Strategic Human Capital Goals			
Strategic Alignment – Ensure that NARA's Strategic Human Capital Plan is aligned with the Agency's Strategic Plan and integrated into workforce planning efforts	✓		✓
Leadership and Knowledge Management – Ensure that NARA supports a culture of leadership and continuous learning		✓	✓
Results-Oriented Performance Culture – Sustain a productive workforce and achieve results by valuing and recognizing performance in an environment in which all employees are encouraged to contribute		✓	✓
Talent Management – Maximize employee talent through recruitment, outreach, hiring and retention efforts		✓	✓
Accountability – Monitor and evaluate results of NARA's human capital management policies, practices, and programs	✓		

NBER WORKING PAPER SERIES

HARD EVIDENCE ON SOFT SKILLS

James J. Heckman
Tim D. Kautz

Working Paper 18121
http://www.nber.org/papers/w18121

NATIONAL BUREAU OF ECONOMIC RESEARCH
1050 Massachusetts Avenue
Cambridge, MA 02138
June 2012

This paper was presented as the Adam Smith Lecture at the Annual Meeting of the European Association of Labour Economists held in Cyprus, September 2011. This research was supported in part by the University of Chicago, A New Science of Virtues: A Project of the University of Chicago, the American Bar Foundation, a conference series from the Spencer Foundation, the JB & MK Pritzker Family Foundation, Susan Thompson Buffett Foundation, the Geary Institute, University College Dublin, Ireland, NICHD R37 HD065072 and R01 HD054702. We acknowledge the support of a European Research Council grant hosted by University College Dublin, DEVHEALTH 269874, a grant from the Institute for New Economic Thinking (INET), and an anonymous funder. The views expressed in this paper are those of the authors and not necessarily those of the funders or commentators mentioned here, nor of the National Bureau of Economic Research.

Hard Evidence on Soft Skills
James J. Heckman and Tim D. Kautz
NBER Working Paper No. 18121
June 2012
JEL No. D01,I20

ABSTRACT

This paper summarizes recent evidence on what achievement tests measure; how achievement tests relate to other measures of "cognitive ability" like IQ and grades; the important skills that achievement tests miss or mismeasure, and how much these skills matter in life.

Achievement tests miss, or perhaps more accurately, do not adequately capture, soft skills—personality traits, goals, motivations, and preferences—that are valued in the labor market, in school, and in many other domains. The larger message of this paper is that soft skills predict success in life, that they causally produce that success, and that programs that enhance soft skills have an important place in an effective portfolio of public policies.

James J. Heckman
Department of Economics
The University of Chicago
1126 E. 59th Street
Chicago, IL 60637
and University College Dublin and IZA
and also NBER
jjh@uchicago.edu

Tim D. Kautz
University of Chicago
Department of Economics
1126 E. 59th Street
Chicago IL 60637
tkautz@uchicago.edu

Contents

1 Introduction

Contemporary society places great value on standardized achievement tests to sift and sort people, to evaluate schools, and to assess the performance of nations. Admissions committees use tests like the SAT, the ACT, and the GRE (Graduate Record Examinations) to screen applicants. In the United States, the No Child Left Behind (NCLB) Act stipulates that government-run schools must administer standardized achievement tests in order to be eligible for federal funding.[1] The Programme for International Student Assessment (PISA) evaluates student performance in math, science, and reading across countries. The results attract media attention and influence policy. The year 2000 PISA test results caused Germany to re-evaluate its educational system and introduce a variety of educational reforms (Grek, 2009).

Despite the widespread use of standardized achievement tests, the traits that they measure are not well-understood. This paper summarizes recent evidence on what achievement tests capture; how achievement tests relate to other measures of "cognitive ability" like IQ and grades; the important skills that achievement tests miss or mismeasure, and how much these other skills matter in life.

Achievement tests miss, or more accurately, do not adequately capture, *soft skills*—personality traits, goals, motivations, and preferences that are valued in the labor market, in school, and in many other domains. The larger message of this paper is that soft skills predict success in life, that they produce that success, and that programs that enhance soft skills have an important place in an effective portfolio of public policies.[2]

Measurement of cognition and educational attainment has been refined during the past century. Psychometricians have shown that cognitive ability has multiple facets.[3] This

[1] Sales of achievement tests have increased by nearly 400% between 1959 and 2005 (Digest of Education Statistics, various years; The Bowker Annual: Library and Book Trade Almanac, various years).

[2] This paper draws on and supplements Borghans et al. (2008a), Almlund et al. (2011), and Heckman et al. (2012a).

[3] See Carroll (1994) and Ackerman and Heggestad (1997) for a discussion.

progress is not widely appreciated. Many social scientists—even many psychologists—continue to use IQ tests, standardized achievement tests, and grades interchangeably to proxy "cognitive ability."[4] Even though scores on IQ tests, standardized achievement tests, and grades are positively correlated with each other, the recent literature shows that they measure different skills and depend on different facets of cognitive ability. Recent research also shows that all three measures are associated with personality, but to different degrees across various cognitive measures.

Standardized achievement tests were designed to capture "general knowledge" produced in schools and through life experiences. Such knowledge is thought to be relevant to success inside and outside of the classroom. However, achievement tests are often validated using other standardized achievement tests or other measures of cognitive ability—surely a circular practice.

A more relevant validity criterion is how well these tests predict meaningful outcomes, such as educational attainment, labor market success, crime, and health. No single measure of cognitive ability predicts much of the variance in these outcomes, and measurement error does not account for most of the remaining variance, leaving much room for other determinants of success.[5]

Success in life depends on personality traits that are not well captured by measures of cognition. Conscientiousness, perseverance, sociability, and curiosity matter. While economists have largely ignored these traits, personality psychologists have studied them over the last century.[6] They have constructed measures of them and provide evidence that these traits predict meaningful life outcomes.

Many scholars—inside and outside of psychology—have questioned the existence of stable personality traits, arguing that constraints and incentives in situations almost entirely

[4]Many call this "IQ", e.g., Flynn (2007), Nisbett (2009), and Nisbett et al. (2012).

[5]On the magnitudes of measurement error on a variety of economic measures, see Bound et al. (2001). These authors report that at most 15–30% of earnings variance is due to measurement error.

[6]Some early studies in economics are Bowles and Gintis (1976), and Bowles et al. (2001). An important study in sociology is Jencks (1979). Work in psychology going back to Terman et al. (1925) shows that personality traits matter (see Murray, 1938; Terman et al., 1947; and the discussion in Gensowski, 2012).

determine behavior. These scholars claim that people are like chameleons—they adapt to any situation.[7] A substantial body of evidence shows that stable traits exist. People tend to behave in the same fashion across a wide range of situations.[8] Evidence from genetics and neuroscience provides a biological basis for the existence of such traits, suggesting that something tied to the person, not the just the situation, affects behavior.[9]

Throughout this paper we use the term "personality traits" to describe the personal attributes not thought to be captured by measures of abstract reasoning power. These attributes go by many names in the literature, including soft skills, personality traits, noncognitive skills, noncognitive abilities, character, and socioemotional skills. These different names connote different properties. The term "traits" suggests a sense of permanence and possibly also of heritability. The terms "skills" and "character" suggest that they can be learned. In reality, the extent to which these personal attributes can change lies on a spectrum. Both cognitive and personality traits can change and be changed over the life cycle but through different mechanisms and to different degrees at different ages. To avoid confusion, throughout this paper we use the term "trait" to capture the set of personal attributes we study.[10]

Psychological traits are not directly observed. There is no ruler for perseverance, no caliper for intelligence. All cognitive and personality traits are measured using performance on "tasks," broadly defined. Different tasks require different traits in different combinations. Some distinguish between measurements of traits and measurements of outcomes, but this distinction is misleading. Both traits and outcomes are measured using performance on some task or set of tasks.

Psychologists sometimes claim to circumvent this measurement issue by creating taxonomies of traits and by applying intuitive names to responses on questionnaires. These

[7] See Mischel (1968). Some behavioral economists share this view. See, e.g., Thaler (2008).

[8] See Epstein (1979) for an early paper showing that personality traits are stable across multiple situations. See the special issue of Journal of Research in Personality (43),"*Personality and Assessment at Age 40*," for a more recent discussion.

[9] See Bouchard and Loehlin (2001) for estimates of the heritability of traits. See Canli (2006) and DeYoung et al. (2010) for evidence that regions of the brain are associated with different traits.

[10] Drawing on the literature in psychology, Borghans et al. (2008a) present one definition of cognitive traits.

questionnaires are not windows to the soul. They are still rooted in task performance or behavior. Responding to a questionnaire is itself a task. Additionally, many of the questionnaires inquire directly about behavior, e.g., a measure of Agreeableness used in the German Socioeconomic Panel asks the extent to which a respondent "is sometimes somewhat rude to others."[11] How else can one answer that question but reflect on one's behavior? IQ tests and standardized achievement tests also measure performance on different "cognitively loaded" tasks.

Performance on most tasks depends on effort, personality traits, cognitive ability, and incentives, although the importance of each differs by task. This dependence creates a fundamental problem in measuring traits. Most studies in psychology devise a set of measures to capture a trait but do not standardize for incentives in the situation in which the trait is being measured or for other traits. Measured cognitive ability and measured personality depend on a constellation of factors. The identification problem arising from the multiple determinants of performance on tasks is empirically important, even for measures of cognitive ability. Incentives can affect performance on IQ tests. Multiple traits affect performance on cognitive tasks. For example, personality traits affect achievement test scores and grades.[12] Caution is required in taking the measures developed by psychologists too literally.

Nonetheless, measures of personality traits predict meaningful life outcomes. Conscientiousness – the tendency to be organized, responsible, and hardworking—is the most widely predictive of the commonly used personality measures. It predicts educational attainment, health, and labor market outcomes as strongly as measures of cognitive ability.[13]

Most studies in psychology only report correlations between measured traits and outcomes without addressing whether the traits *cause* the outcomes and without controlling for the other traits and incentives that determine performance on the tasks used to measure the traits. While traits are relatively stable across situations, they are not set in stone. They

[11]Throughout this paper, we adopt the convention of capitalizing traits from the "Big Five" personality taxonomy. See Table 3 for a description of the Big Five.

[12]See Borghans et al. (2011a).

[13]See the evidence collected in Almlund et al. (2011), Borghans et al. (2008a), and Roberts et al. (2007).

change over the life cycle. On average, Agreeableness and Conscientiousness tend to grow with age. Different facets of cognitive ability peak at different ages. Interventions, education, and parenting can affect traits in lasting ways.

This paper summarizes recent evidence that personality causally affects life outcomes. We review some of the literature from psychology and economics and then focus on two particularly compelling examples.[14]

First, we show how an achievement test, the General Educational Development (GED) test, fails to capture important traits that affect success in life. High school dropouts can take the GED to certify to employers and post-secondary institutions that their skills are equivalent to those of high school graduates who do not attend college. After accounting for differences in pre-existing cognitive ability, GED recipients perform much worse in the labor market than high school graduates and much more like other high school dropouts. GED recipients lack important personality traits. (See Heckman et al., 2011a and Heckman et al., 2012a.)

Second, we show how an early childhood intervention, the Perry Preschool Program, improved the lives of disadvantaged children, even though the program did not permanently change the IQ of its participants. The program changed their personality traits in a lasting way (see Heckman et al., 2012b). Other interventions and observational studies provide supporting evidence that early-childhood investments improve outcomes through their effects on personality.[15]

[14]Borghans et al. (2008a) and Almlund et al. (2011) present extensive surveys of this literature.

[15]The "*Tools of the Mind*" intervention is designed to promote "executive functioning," which has both cognitive and personality components. Barnett et al. (2008, 2006); Bierman et al. (2010); Bodrova and Leong (2001, 2007); Dee and West (2011); Diamond et al. (2007); Durlak et al. (2011); Lillard and Else-Quest (2006) report success of this intervention. For a contrary view, see the study by Farran et al. (2011).

2 Defining and Measuring Personality Traits

2.1 History and Measurement of Cognitive Ability

Modern intelligence tests have been used for just over a century, beginning when a French minister of public instruction wished to identify retarded pupils in need of specialized education programs. In response, Alfred Binet created the first IQ test.[16] IQ scores were interpreted as measuring a stable trait. The standardized achievement test was created in the wake of the perceived success of IQ tests as an objective and cost-effective measure of acquired skills. In contrast to IQ tests, standardized achievement tests were designed to measure "general knowledge" that could be acquired in schools and through life experiences and was widely applicable beyond the classroom to workplace and social functioning.[17]

Achievement tests are typically validated on other achievement tests, IQ tests, and grades, rather than on tasks or outcomes in the labor market and in social functioning. Table 1 shows correlations among scores on standardized achievement tests, IQ tests, and grades. Standardized achievement tests are correlated with IQ tests, but the correlation depends on the subject area of the standardized achievement test. Hartlage and Steele (1977) find that the arithmetic portions of standardized achievement tests are the most highly correlated with IQ. Grades and scores on IQ tests and standardized achievement tests are far from perfectly correlated, suggesting that they measure different aspects of "cognitive functioning."[18]

Psychologists distinguish between fluid intelligence (the rate at which people learn) and crystalized intelligence (acquired knowledge).[19] Achievement tests are heavily weighted to-

[16] In 1904, *La Société Libre pour l'Etude Psychologique de l'Enfant* appointed a commission to create a mechanism for identifying these pupils in need of alternative education led by Binet. See Herrnstein and Murray (1994) for an overview of Binet's life and work.

[17] See Lindquist (1951).

[18] It is an irony of the testing literature that high school grades are more predictive of first year college performance than SAT scores (Bowen et al., 2009). The SAT and related tests are thought to be more objective measures of student quality than high school grades (Lemann, 1999).

[19] See, e.g., Nisbett et al. (2012).

Table 1: Cognitive Ability Validities

Test	**Validation Domain**	**Estimate(s)**	**Source(s)**
SAT (Achievement)	1st Year College GPA	0.35 - 0.53	Kobrin et al. (2008)
ACT (Achievement)	Early College GPA	0.42	ACT, Inc. (2007)
GED (Achievement)	HS Senior GPA	0.33 - 0.49	GED Testing Service (2009)
DAT (Achievement)	College GPA	0.13 - 0.62†	Omizo (1980)
AFQT (Achievement)	9th Grade GPA	0.54	Borghans et al. (2011a)
WAIS (IQ)	College GPA	0.38 - 0.43	Feingold (1982)
WAIS (IQ)	HS GPA	0.62	Feingold (1982)
Various IQ**	9th Grade GPA	0.42	Borghans et al. (2011a)
WISC (IQ)	WRAT (Achievement)	0.44 - 0.75‡	Hartlage and Steele (1977)
WISC-R (IQ)	WRAT (Achievement)	0.35 - 0.76‡	Hartlage and Steele (1977)
Various IQ**	AFQT (Achievement)	0.65	Borghans et al. (2011a)
Stanford Binet (IQ)	WISC-R (IQ)	0.77 - 0.87	Rothlisberg (1987), Greene et al. (1990)
Raven's (IQ)	WAIS-R (IQ)	0.74 - 0.84	O'Leary et al. (1991)
WIAT (Achievement)	CAT/2 (Achievement)	0.69 - 0.83*	Michalko and Saklofske (1996)

Definitions: WISC – Wechsler Intelligence Scale for Children, WISC-R – Wechsler Intelligence Scale for Children - Revised, WAIS - Wechsler Adult Intelligence Scale, Raven's IQ – Raven's Standard Progressive Matrices, GED – General Educational Development, DAT – Differential Aptitude Tests, WIAT – Wechsler Individual Achievement Test, CAT – California Achievement Test, WRAT – Wide Range Achievement Test, AFQT – Armed Forces Qualification Test
† Large range is due to varying validity of eight subtests of DAT
‡ Ranges are given because correlations vary by academic subject
∗ Ranges are given because correlations vary by grade level
∗∗ IQ test scores in the NLSY79 are pooled across several IQ tests using IQ percentiles

wards crystallized intelligence,[20] whereas IQ tests like Raven's progressive matrices (1962) are heavily weighted toward fluid intelligence.[21,22] Many psychologists do not recognize the differences among these measures and interchangeably use IQ, achievement tests, and grades to measure "cognitive ability" or "intelligence," and this practice is also widespread in economics.[23]

2.2 Defining and Measuring Psychological Traits

Validating one measure of cognitive ability using other measures of cognitive ability is circular. More relevant is how well these measures predict important life outcomes. Table 2 shows the extent to which IQ, standardized achievement tests, and grades explain the variance of outcomes at age 35 in the National Longitudinal Survey of Youth, 1979 (NLSY79) data. The three groups of columns under each category show results for different sub-samples based on the availability of the different cognitive measures. For each category, the first column shows the explained variance using only the designated measure of cognitive ability. Achievement tests and grades are more predictive than IQ. But none of these measures explains much of the variation of any outcome, leaving considerable room for other determinants. As noted in the introduction, it is unlikely that measurement error accounts for all of the remaining variance.

Personality is one missing ingredient. The second columns in each category preview our later discussion of the explanatory power of personality. They show the variance explained by measures of personality.[24] In many cases, the variance explained by personality measures rivals that explained by measures of cognitive ability. The relative importance of person-

[20] See Roberts et al. (2000).

[21] See Raven et al. (1988). The high correlation between intelligence and achievement tests is in part due to the fact that both require cognitive ability and knowledge. Common developmental factors may affect both of these traits. Fluid intelligence promotes the acquisition of crystallized intelligence.

[22] Carroll (1994) and Ackerman and Heggestad (1997) discuss more disaggregated facets of cognitive ability.

[23] See Flynn (2007) and Nisbett et al. (2012). For examples in economics, see Benjamin et al. (2006).

[24] They include measures of adolescent risky behavior, self-esteem and locus of control (the extent to which people feel they have control over their lives). For precise definitions of the measures used, see the notes to Table 2.

ality depends on the outcome. The third column for each sub-sample shows the variance explained when both the cognitive and personality measures are used as predictors. In many cases, including the measures of personality in a regression with cognitive measures explains additional variance. The correlations between the set of measures of personality and the measures of cognition are positive, but not especially strong (see the bottom row of each table). Each set of traits has an independent influence on the outcomes in the table.

Even though economists have largely ignored personality traits, the pioneers of the original IQ tests recognized their importance.[25] Alfred Binet the creator of the first IQ test (the Stanford-Binet test), noted that:

> *"[Success in school] ...admits of other things than intelligence; to succeed in his studies, one must have qualities which depend on attention, will, and character; for example a certain docility, a regularity of habits, and especially continuity of effort. A child, even if intelligent, will learn little in class if he never listens, if he spends his time in playing tricks, in giggling, in playing truant."*
>
> -(Binet and Simon, 1916, p. 254)

Since the middle of the 19th century, personality psychologists have studied these traits. One leading personality psychologist defines personality traits in the following way:

> *"Personality traits are the relatively enduring patterns of thoughts, feelings, and behaviors that reflect the tendency to respond in certain ways under certain circumstances."*
>
> -(Roberts, 2009, p. 140)

Personality traits are manifested through thoughts, feelings, and behaviors, and therefore, must be inferred from measures of performance on "*tasks*," broadly defined. Under this

[25]Lewis Terman, who created the Stanford-Binet test, even collected data on personality traits of a high-ability sample. In this sample, Conscientiousness is highly predictive of health and earnings (Savelyev, 2011; Gensowski, 2012).

Table 2: Predictive Validities in Outcomes that Matter (Adjusted R-Squared)

	IQ Sample			*AFQT Sample*			*GPA Sample*		
Males	IQ	Personality	Both	AFQT	Personality	Both	GPA	Personality	Both
Earnings at Age 35	0.07	0.05	0.09	0.17	0.07	0.18	0.09	0.06	0.12
Hourly Wage at Age 35	0.07	0.03	0.08	0.13	0.06	0.14	0.07	0.06	0.09
Hours Worked at Age 35	0.01	0.03	0.04	0.03	0.02	0.03	0.02	0.01	0.02
Jail by Age 35	0.03	0.02	0.04	0.06	0.06	0.09	0.03	0.03	0.04
Welfare at Age 35	0.01	0.00	0.01	0.03	0.01	0.03	0.01	0.00	0.01
Married at Age 35	0.01	0.05	0.05	0.04	0.03	0.06	0.03	0.03	0.04
B.A. Degree by Age 35	0.12	0.08	0.16	0.19	0.10	0.22	0.14	0.10	0.18
Depression in 1992	0.01	0.05	0.05	0.04	0.04	0.06	0.02	0.04	0.04
Adj, R^2 Cog, Personality		0.07			0.17			0.11	
	IQ Sample			*AFQT Sample*			*GPA Sample*		
Females	IQ	Personality	Both	AFQT	Personality	Both	GPA	Personality	Both
Earnings at Age 35	0.01	0.03	0.03	0.09	0.05	0.11	0.05	0.04	0.07
Hourly Wage at Age 35	0.05	0.03	0.06	0.12	0.05	0.14	0.06	0.04	0.08
Hours Worked at Age 35	-0.00	0.02	0.02	0.00	0.01	0.00	0.00	0.01	0.01
Jail by Age 35	-0.00	0.01	0.00	0.01	0.02	0.02	0.01	0.01	0.02
Welfare at Age 35	0.02	0.04	0.05	0.10	0.05	0.12	0.05	0.05	0.07
Married at Age 35	0.03	0.03	0.05	0.05	0.04	0.07	0.03	0.03	0.05
B.A. Degree by Age 35	0.10	0.08	0.14	0.17	0.09	0.20	0.10	0.08	0.13
Depression in 1992	0.02	0.05	0.05	0.04	0.05	0.07	0.02	0.05	0.05
Adj, R^2 Cog, Personality		0.10			0.15			0.10	

Source: National Longitudinal Survey of Youth 1979. Table Description: The table shows the adjusted R-squared from regressions of later-life outcomes on measures of personality and cognition. For each cognitive measure, the first column shows the explained variance using only the measures of cognitive ability, the second column shows the explained variance from using only the measure of personality (Personality), and the third column shows the explained variance from using both the measures of personality and cognition (Both). The last row shows the adjusted R-squared from a regression of each cognitive measure on the personality measures. Measures of Personality and Cognition: The measures of personality include minor illegal activity in 1979 (vandalism, shoplifting, petty theft, fraud and fencing), major illegal activity in 1979 (auto theft, breaking/entering private property, grand theft), participation in violent crime in 1979 (fighting, assault and aggravated assault), tried marijuana before age 15, daily smoking before age 15, regular drinking before age 15, and any intercourse before age 15. It also includes measures of self-esteem and locus of control. Self-esteem is measured using the ten-item Rosenberg scale administered in 1980. Locus of control is a measure of how much control an individual believes they have over their life and is measured using the 4-item Rotter scale. IQ and grades are from high school transcripts. IQ is pooled across several IQ tests using IQ percentiles. GPA is the individual's core-subject GPA from 9th grade. The Armed Forces Qualification Test (AFQT) was adjusted for schooling at the time of the test conditional on final schooling as described in Hansen et al. (2004). Outcomes: Due to the biennial nature of the survey after 1994, some respondents are not interviewed at age 35, for these individuals age 36 is used. Earnings includes zero-earners and excludes observations over $200,000 (2005 dollars). Hourly wage excludes observations less than $3 or over $200 (2005 dollars). Hours worked excludes observations less than 80 or more than 4000. Jail by age 35 indicates whether the respondent had listed residing in a jail or prison at some point before age 35. Welfare at age 35 indicates whether the respondent received any positive amount of welfare at age 35. Married at age 35 indicates whether the responded was currently married. B.A. degree by age 35 indicates whether the respondent received a B.A. degree (or higher) by age 35. Depression in 1992 is based on the 7-item Center for Epidemiologic Studies Depression Scale (CES-D). Sample: The sample excludes the military over sample. The samples differ across the IQ, AFQT, and GPA due to missing measures across the samples.

definition, performance on IQ tests is a personality trait because it is an enduring pattern of behavior (how one "behaves" or "performs" on an IQ test).[26]

Personality psychologists primarily measure personality traits using self-reported surveys. They have arrived at a relatively well-accepted taxonomy of traits called the "Big Five," which includes Openness to Experience, Conscientiousness, Extraversion, Agreeableness, and Neuroticism. Table 3 defines these traits and their multiple facets.[27] Some argue that the Big Five are the longitude and latitude of personality, by which all more narrowly defined traits may be categorized (see Costa and McCrae, 1992a). While the Big Five measures are now the most widely used, there are several other taxonomies, including the Big Three, the MPQ, and the Big Nine. They are conceptually and empirically related to the Big Five.[28] Other taxonomies, including psychopathology as measured by the DSM IV and measures of temperament, have also been related to the Big Five.[29] Almlund et al. (2011) show that economic preference parameters are not all that closely related to psychological traits and apparently represent different traits that, along with the psychological traits, govern behavior.

A deeper issue, as yet not systematically investigated in the literature in economics or psychology, is whether the traits captured by the alternative measurement systems are the manifestation of a deeper set of preferences or goals. Achieving certain goals requires certain traits, e.g., a surgeon has to be careful and intelligent; a salesman has to be outgoing and engaging and so forth, etc. Under this view, traits are developed through practice, investment, and habituation. The deeper traits may be the preference parameters that generate the manifest traits. The apparent stability of expressed traits across situations may be a consequence of the stability of the goals and incentives to achieve these goals.[30]

[26]Studies of test-retest reliability of IQ tests show that scores are highly correlated across repeated testing occasions (see, e.g., Niolon, 2005).

[27]See, e.g., Borghans et al. (2008a).

[28]See Borghans et al. (2008a) and Almlund et al. (2011) for a comparison of these taxonomies.

[29]See, e.g., Cloninger et al. (1999).

[30]McAdams and Pals (2006) adds goals to the list of possible traits. Almlund et al. (2011) develop a model in which preferences and traits determine the effort applied to tasks.

Table 3: The Big Five Domains and Their Facets

Big Five Personality Factor	American Psychology Association Dictionary description	Facets (and correlated trait adjective)	Related Traits	Analogous Childhood Temperament Traits
Conscientiousness	"the tendency to be organized, responsible, and hardworking"	Competence (efficient), Order (organized), Dutifulness (not careless), Achievement striving (ambitious), Self-discipline (not lazy), and Deliberation (not impulsive)	Grit, Perseverance, Delay of gratification, Impulse control, Achievement striving, Ambition, and Work ethic	Attention/(lack of) distractibility, Effortful control, Impulse control/delay of gratification, Persistence, Activity*
Openness to Experience	"the tendency to be open to new aesthetic, cultural, or intellectual experiences"	Fantasy (imaginative), Aesthetic (artistic), Feelings (excitable), Actions (wide interests), Ideas (curious), and Values (unconventional)		Sensory sensitivity, Pleasure in low-intensity activities, Curiosity
Extraversion	"an orientation of one's interests and energies toward the outer world of people and things rather than the inner world of subjective experience; characterized by positive affect and sociability"	Warmth (friendly), Gregariousness (sociable), Assertiveness (self-confident), Activity (energetic), Excitement seeking (adventurous), and Positive emotions (enthusiastic)		Surgency, Social dominance, Social vitality, Sensation seeking, Shyness*, Activity*, Positive emotionality, and Sociability/affiliation
Agreeableness	"the tendency to act in a cooperative, unselfish manner"	Trust (forgiving), Straightforwardness (not demanding), Altruism (warm), Compliance (not stubborn), Modesty (not show-off), and Tender-mindedness (sympathetic)	Empathy, Perspective taking, Cooperation, and Competitiveness	Irritability*, Aggressiveness, and Willfulness
Neuroticism/ Emotional Stability	Emotional Stability is "predictability and consistency in emotional reactions, with absence of rapid mood changes." Neuroticism is "a chronic level of emotional instability and proneness to psychological distress."	Anxiety (worrying), Hostility (irritable), Depression (not contented), Self-consciousness (shy), Impulsiveness (moody), Vulnerability to stress (not self-confident)	Internal vs. External, Locus of control, Core self-evaluation, Self-esteem, Self-efficacy, Optimism, and Axis I psychopathologies (mental disorders) including depression and anxiety disorders	Fearfulness/behavioral inhibition, Shyness*, Irritability*, Frustration (Lack of) soothability, Sadness

Notes: Facets specified by the NEO PI-R personality inventory (Costa and McCrae, 1992b). Trait adjectives in parentheses from the Adjective Check List (Gough and Heilbrun, 1983). *These temperament traits may be related to two Big Five factors.
Source: Table adapted from John and Srivastava (1999).

2.3 Identification Problems in Measuring Traits

Measuring traits is difficult, because, as suggested by Roberts' definition of personality, all psychological measurements are calibrated on measured behavior, and the behaviors used to measure one trait can be influenced by incentives and other traits. To infer traits from behaviors requires standardizing for all of the other contributing factors that produce the observed behavior. The inability to parse and localize behaviors that depend on a single trait or ability gives rise to a fundamental identification problem that is typically ignored in empirical research investigating how psychological traits affect outcomes.[31]

There are two primary issues. First, behavior depends on incentives created in situations. Different incentives elicit different amounts of effort on the tasks used to measure traits. Accurately measuring personality traits requires standardizing for the effort applied in any task. Second, behavior in one task can depend on multiple traits. Not standardizing for incentives and other traits can produce misleading estimates of any trait.

These identification problems are empirically important when measuring any given trait. For example, incentives partly determine scores on IQ tests, even though some have argued that performance on IQ tests reflects maximal effort.[32] A series of studies conducted over the past 40 years shows that incentives, like money or candy, can increase IQ scores, particularly among low-IQ individuals. The Black-White gap in IQ can be completely eliminated by incentivizing students with M&M candies.[33] The incentives in one test do not affect performance on future tests.

The recent literature shows that personality traits are associated with standardized achievement test scores, which many analysts use interchangeably with IQ scores.[34] Figures 1 and 2 show how the variance in the scores on two achievement tests, the Armed Forces

[31] See Borghans et al. (2011a) and Almlund et al. (2011).

[32] A leading psychometrician, Carroll (1993), does not accept the notion that IQ captures maximal effort.

[33] See Ayllon and Kelly (1972); Borghans et al. (2008b); Breuning and Zella (1978); Clingman and Fowler (1976); Edlund (1972); Holt and Hobbs (1979); Larson et al. (1994); Segal (2008). This evidence is summarized in Borghans et al. (2008a) and Almlund et al. (2011).

[34] See, e.g., Nisbett (2009).

Qualification Test (AFQT) and the closely related Differential Aptitudes Tests (DAT),[35] are decomposed into IQ and personality measures. Personality traits explain a substantial portion of the variances in both AFQT scores and DAT scores.[36] The personality traits are incrementally valid in that they explain the variance above and beyond the variance that IQ explains in a regression. These findings caution the interpretation that standardized achievement tests only measure cognitive ability. They are bundled with personality traits. In data from the Stella Maris secondary school in Maastricht, Holland, Openness to Experience is strongly correlated with IQ.[37]

Further complicating identification, not everyone responds to incentives in the same way. Borghans et al. (2008b) show that adults spend substantially more time answering questions on IQ tests when rewards are higher. Subjects high in Emotional Stability and Conscientiousness are less affected by rewards. Similarly, Segal (2008) shows that introducing cash incentives for performance on the coding speed test of the Armed Services Vocational Battery (ASVAB) increases performance substantially, particularly for men with lower levels of Conscientiousness.

2.4 Are There Stable Personality Traits?

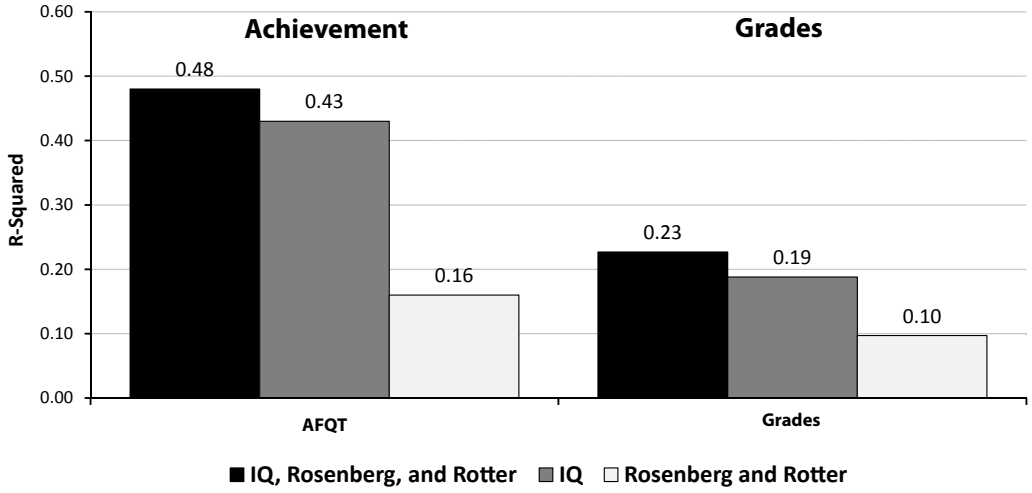
Many have questioned whether personality traits exist. The publication of Walter Mischel's 1968 book, *Personality and Assessment*, gave rise to a heated "personality-situation" debate within psychology, which pitted the social psychologists who favored situational factors as explaining behavior against those who considered stable personality traits as more consequential. Mischel argued that aspects of situations overshadow any effect of personality on

[35]The correlation between DAT and AFQT scores in the National Longitudinal Study of Youth 1979 (NLSY79) is 0.76 to 0.80 (Borghans et al., 2011b). Friedman and Streicher (1985) estimate correlations between 0.65 and 0.82 for in a sample of high school sophomores and juniors. Kettner (1976) estimates correlations between DAT and the AFQT subtests of 0.76 to 0.89 in a sample of juniors and seniors.

[36]The lower explained variance in the sample with DAT is likely a consequence of restriction on range. The DAT data come from a single school, whereas the AFQT data come from a national sample.

[37]See Borghans et al. (2011b) for information on the Stella Marris secondary school and the analysis described in the text.

Figure 1: Decomposing Achievement Tests and Grades into IQ and Personality [NLSY79]



Source: Borghans et al. (2011a), National Longitudinal Survey of Youth 1979 (NLSY79). Notes: Rotter is a measure of locus of control designed to measure the extent to which individuals believe that they have control over their lives through self-motivation or self-determination as opposed to the extent to which individuals believe that the environment controls their lives (Rotter, 1966). Rosenberg is a measure of self-esteem designed to measure the degree of approval or disapproval toward oneself (Rosenberg, 1965). The Armed Forces Qualification Test (AFQT) score is constructed from the Arithmetic Reasoning, Word Knowledge, Mathematical Knowledge, and Paragraph Comprehension Armed Services Vocational Aptitude Battery (ASVAB) subtests. Rotter was administered in 1979. The ASVAB and Rosenberg were administered in 1980. IQ and GPA are from high school transcript data. AFQT, Rosenberg, and Rotter have been adjusted for schooling at the time of the test conditional on final schooling, as described in Hansen et al. (2004). IQ is pooled across several IQ tests using IQ percentiles. GPA is the individual's core subject GPA from 9th grade. Sample excludes the military over-sample.

behavior.[38]

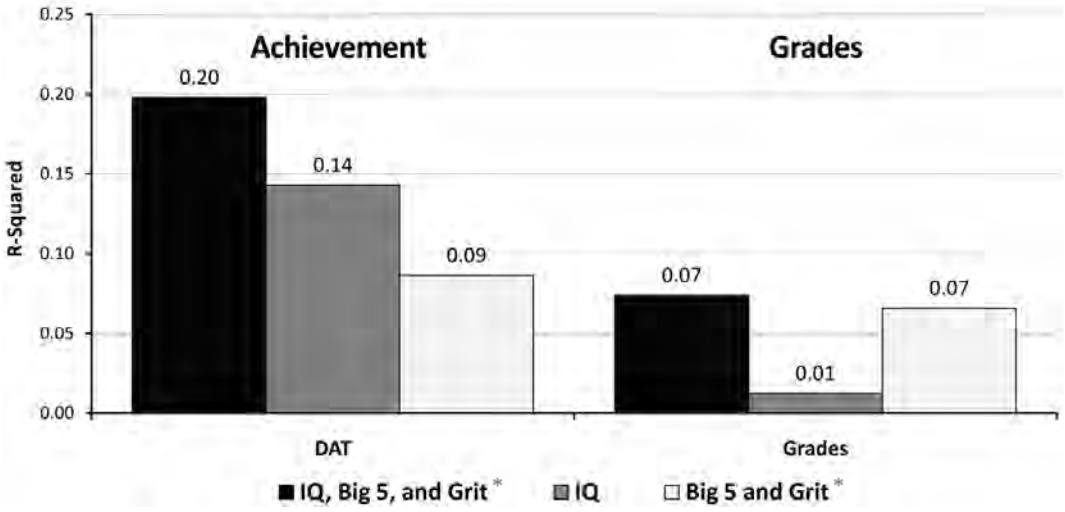
A large body of evidence reviewed in Almlund et al. (2011) shows that stable personality traits exist and are predictive of many behaviors.[39] An important paper by Epstein (1979) presents compelling evidence that, averaging over tasks and situations at a point in time, people act in a predictable fashion with a high level of reliability (R^2 of 0.6-0.8) of average behavior ("measured personality") across situations. The incentives in any situation also matter. Heritability studies show that measures of personality traits tend to be about 40%-60% heritable, suggesting that something tied to the person, rather than the situation, influences behavior (Bouchard and Loehlin, 2001).[40] Evidence in neuroscience suggests that

[38]This theme has been picked up in behavioral economics. See Thaler (2008).

[39]See the special issue of *Journal of Research in Personality* (43), entitled "*Personality and Assessment at Age 40*" for a recent discussion.

[40]Devlin et al. (1997) suggest that traditional estimates of the heritability of IQ may be inflated because

Figure 2: Decomposing Achievement Tests and Grades into IQ and Personality [Stella Maris]



*Grit is a measure of persistence on tasks (Duckworth et al., 2007).

Source: Borghans et al. (2011a).

expression of traits is related to regions of the brain (see Canli, 2006, and DeYoung et al., 2010).

2.5 The Evolution of Personality Traits Over the Life Cycle

Even though personality traits are relatively stable across situations, they are not set in stone. They change over the life cycle. Figure 3 shows that Conscientiousness tends to increase monotonically over the life cycle. Other traits change in different ways over the life cycle.[41] Crystallized intelligence tends to increase monotonically for most of the life cycle, whereas fluid intelligence tends to peak in early adulthood and then decline.[42]

This evidence does not address whether these changes occur naturally ("ontogenic change") or whether they are due to changes in the environments commonly experienced over the life

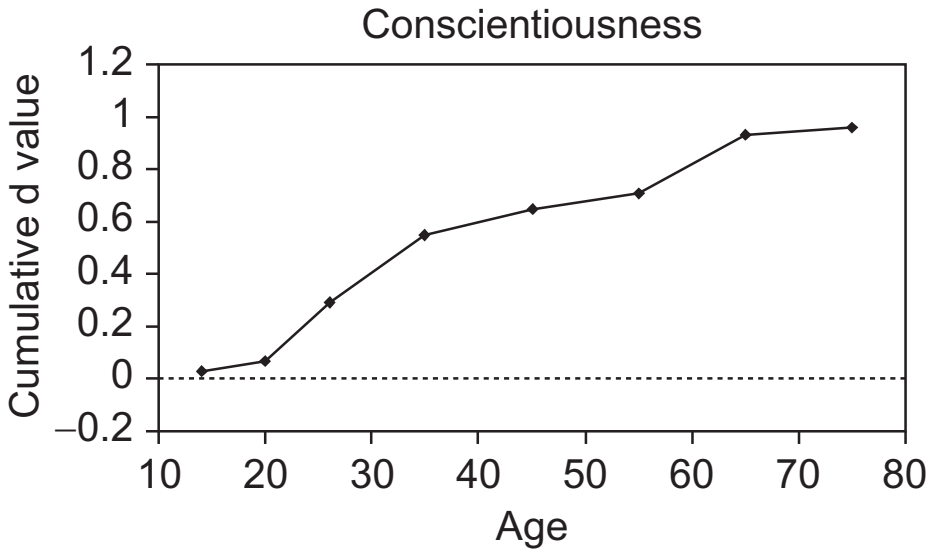
they fail to take into account the effect of the environment on conditions in the maternal womb. See also Rutter (2006) and an emerging literature on epigenetics.

[41]See the evidence collected in Borghans et al. (2008a) and Almlund et al. (2011) for a variety of other traits.

[42]See McArdle et al. (2000).

cycle ("sociogenic change"). No evidence is available in the published literature on the distributions of these profiles over the life cycle. Almlund et al. (2011) review the evidence on how parental investment and interventions promote changes in personality.

Figure 3: Cumulative Mean-Level Changes in Personality Across the Life Cycle



Note: Cumulative d values represent total lifetime change in units of standard deviations ("effect sizes").
Source: Figure taken from Roberts et al. (2006) and Roberts and Mroczek (2008). Reprinted with permission of the authors.

2.6 The Predictive Power of Personality

Table 2 shows that personality traits predict many later-life outcomes as strongly as measures of cognitive ability. Conscientiousness – the tendency to be perseverant and hardworking – stands out as the most predictive of the Big Five traits across many outcomes. Figure 4 presents for males correlations between the Big Five and educational attainment, adjusting and not adjusting for fluid and crystalized intelligence. Conscientiousness predicts educational attainment more than either of the facets of intelligence.[43] Similar patterns appear for many other outcomes, including labor market performance, grades, and health.[44]

A recurrent finding in the literature is that measured IQ is highly predictive of perfor-

[43]Results are similar for women (see Almlund et al., 2011).

[44]See Almlund et al. (2011), Borghans et al. (2008a), and Roberts et al. (2007) for comprehensive reviews of the evidence.

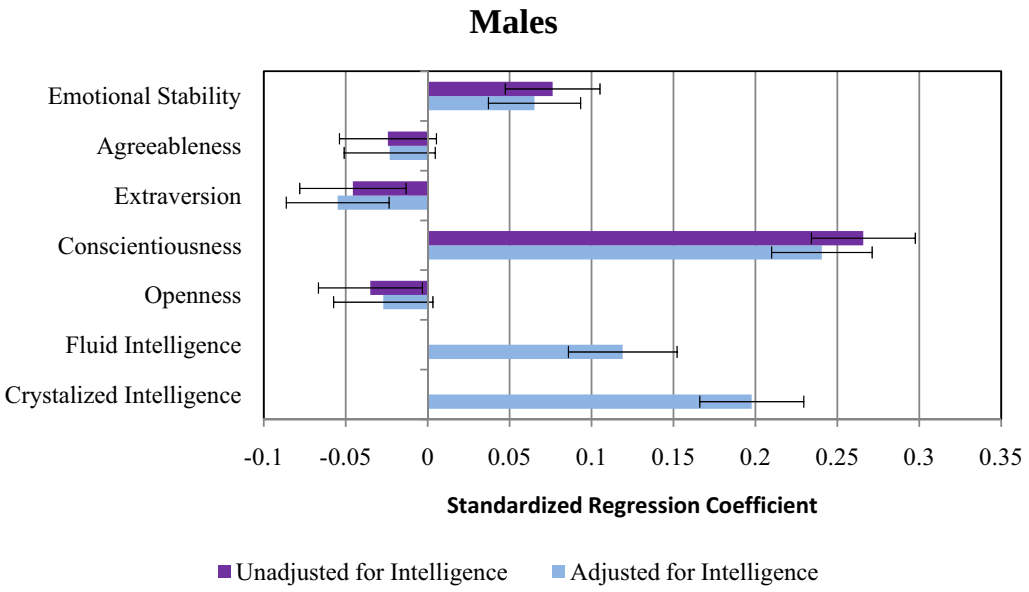
mance on complex tasks and jobs (Gottfredson, 1997). The importance of IQ increases with job complexity, defined as the information processing requirements of the job: cognitive skills are more important for professors, scientists, and senior managers than for semi-skilled or unskilled laborers (Schmidt and Hunter, 2004). In contrast, the importance of Conscientiousness does not vary much with job complexity (Barrick and Mount, 1991), suggesting that it pertains to a wider spectrum of jobs.

The literature in economics establishes that the same bundle of traits has different productivity in different tasks. People also differ in their endowments of traits. These two features lead to sorting in the tasks people pursue in life and are a manifestation of the general principle of comparative advantage in the labor market and in life. (See Almlund et al., 2011; Borghans et al., 2008a; Cattan, 2012; Heckman et al., 2006a, 2011b.)

Achievement test scores are crude, low-dimensional summaries of high-dimensional vectors of traits that operate in conjunction with effort. It is unlikely that these summaries capture the precise combinations of traits required for success in specific life tasks. The thrust of recent research in personality and economics is to isolate the traits that determine life outcomes and to understand how those diverse traits determine choices of tasks.

Most of the evidence in personality psychology is correlational. The reported correlations do not prove that personality traits *cause* higher educational attainment although it is consistent with it. For example, the reported pattern in Figure 4 could arise if educational attainment increased Conscientiousness. We next present causal evidence.

Figure 4: Association of the Big Five and intelligence with years of completed schooling



Notes: The figure displays standardized regression coefficients from a multivariate regression of years of school attended on the Big Five and intelligence, controlling for age and age squared. The bars represent standard errors. The Big Five coefficients are corrected for attenuation bias. The Big Five were measured in 2005. Years of schooling were measured in 2008. Intelligence was measured in 2006. The measures of intelligence were based on components of the Wechsler Adult Intelligence Scale (WAIS). The data is a representative sample of German adults between the ages 21 and 94.
Source: Almlund et al. (2011), German Socio-Economic Panel (GSOEP), waves 2004-2008.

3 Causal Evidence

3.1 Problems with Establishing Causality

Most studies in personality psychology do not address the question of causality, i.e., whether measured traits *cause* (rather than just predict) outcomes. Empirical associations are not a reliable basis for policy analysis. In this section, we discuss difficulties in establishing causality. We also summarize several studies that provide evidence that personality traits *cause* outcomes.

We introduce a simple framework to analyze the effect of traits on outcomes and how traits evolve over time.[45] Equation (1) shows how an outcome at age a, T_a, which is the

[45]This framework draws on Almlund et al. (2011).

performance on a task, depends on cognition C_a, personality P_a, other acquired skills such as education and job training K_a, and the effort allocated to the task e_{T_a}:

$$\underbrace{T_a}_{\substack{\text{Outcome on a}\\ \text{task at age } a}} = \phi_a(\underbrace{C_a}_{\text{Cognition}} , \underbrace{P_a}_{\text{Personality}} , \underbrace{K_a}_{\substack{\text{Other}\\ \text{acquired}\\ \text{skills}}} , \underbrace{e_{T_a}}_{\substack{\text{Effort}\\ \text{devoted to}\\ \text{task}}}) \quad a = 1, \ldots, A. \tag{1}$$

Equation (2) shows how the effort allocated to task T_a depends on cognition C_a, personality P_a, other acquired skills K_a, incentives R_{T_a}, and preferences Υ_a:

$$e_{T_a} = \psi_{T_a}(C_a, P_a, K_a, \underbrace{R_{T_a}}_{\substack{\text{Incentives}\\ \text{to perform}\\ \text{on task}}} , \underbrace{\Upsilon_a}_{\text{Preferences}}). \tag{2}$$

The effort applied to a task is the outcome of a choice problem that depends on traits, preferences, and incentives, much like a supply equation in the standard theory of consumer choice. Preferences can be thought of as additional traits.[46] Some psychological theories posit that people have limited effort that they can divide among different tasks (See, e.g., Baumeister and Tierney, 2011).

Equations (1) and (2) formalize the difficulty in establishing a causal relationship between outcomes and traits. Multiple traits, effort, and acquired skills generate performance in a given task. Many studies in psychology and economics do not control for these inputs and equate measurement of a set of outcomes with the trait the analyst is trying to measure.[47] This practice can lead to a substantial bias in inference about any particular trait.

An additional point is that most studies assume a linear relationship between outcomes and traits. This practice is particularly problematic for measuring personality traits, where the effect of a trait on an outcome is not always linear or even monotonic. Too much of a

[46]The empirical relationship between measured preference parameters and Big Five measures is weak (see Almlund et al., 2011).

[47]Selecting measures and verifying them is part of the sometimes mysterious and inherently subjective process of "construct validity" in psychology. For a discussion, see Borghans et al. (2008a).

good thing can be bad $\left(\frac{\partial \phi_a}{\partial P_a} < 0 \text{ for } P_a > \bar{P} \text{ for threshold } \bar{P}\right)$. For example, extreme levels of traits are associated with psychopathologies. High levels of Conscientiousness are associated with Obsessive Compulsive Disorder, which hinders task performance (Samuel and Widiger, 2008). Nonlinearities can also arise when traits and incentives interact, as in the analyses of Borghans et al. (2008b) and Segal (2008) who show that people with different personality traits respond differently to incentives on tests.[48]

The traits and other acquired skills evolve over time through investment and habituation. Equation (3) shows that traits at age $a+1$ are age-dependent functions of cognitive ability, personality traits, other acquired skills, and investment I_a at age a. In this way, previous levels of traits and acquired skill affect current levels of traits and acquired skill. Equation (3) formalizes the notion that the traits and skills governing performance at a point in time are themselves the outcome of investment and habituation:

$$(C_{a+1}, P_{a+1}, K_{a+1}) = \eta_a(C_a \ , \ P_a \ , \ K_a \ , \ \underbrace{I_a}_{\substack{\text{Investment} \\ \text{and} \\ \text{experience}}}), \qquad a = 1, \ldots, A. \tag{3}$$

In conjunction with resource constraints, a "deeper" set of preference parameters at age a may govern investment decisions and effort allocated to tasks.

3.2 Extreme Examples of Personality Change

Laboratory experiments and brain lesion studies provide some of the most compelling evidence that personality traits can change and that the change affects behaviors. The most famous example is that of Phineas Gage, a railway construction foreman whose head was impaled by a metal spike. Miraculously he retained his problem solving abilities, but he changed from being polite and dependable to being rude and unreliable. His personality change caused him to lose his job and alienate family members (Damasio et al., 2005). Lab-

[48] Formally, this occurs when $\frac{\partial^2 \psi_{T_a}}{\partial P_a \partial R_{T_a}} \neq 0$.

oratory experiments show that expressed traits can be manipulated temporarily. Magnetic disruption of the left lateral prefrontal cortex can increase experimentally elicited discount rates (Figner et al., 2010) and nasal sprays of oxytocin increase trust (Kosfeld et al., 2005).

3.3 Evidence from the GED Testing Program

The GED is a standardized achievement test that serves as an alternative to a high school diploma. High school dropouts can take the seven-and-a-half hour GED exam to certify that they have the "general knowledge" of a high school graduate. The test is widely used. The GED testing program currently produces 12% of high school certificates each year in the United States. We draw on the analysis of Heckman et al. (2012a) and first present results for males. The GED program provides insight into the effects of personality traits on outcomes. GED recipients have the same cognitive ability as high school graduates, but differ in their personality traits.

Table 4 shows the correlations between GED test scores and other achievement test scores. GED test scores are strongly correlated with scores on other standardized achievement tests. The correlations range from 0.61 with the General Aptitude Test Battery (GATB) to 0.88 with the Iowa Test of Educational Development, the progenitor of the GED.

Table 4: Validities of GED Test

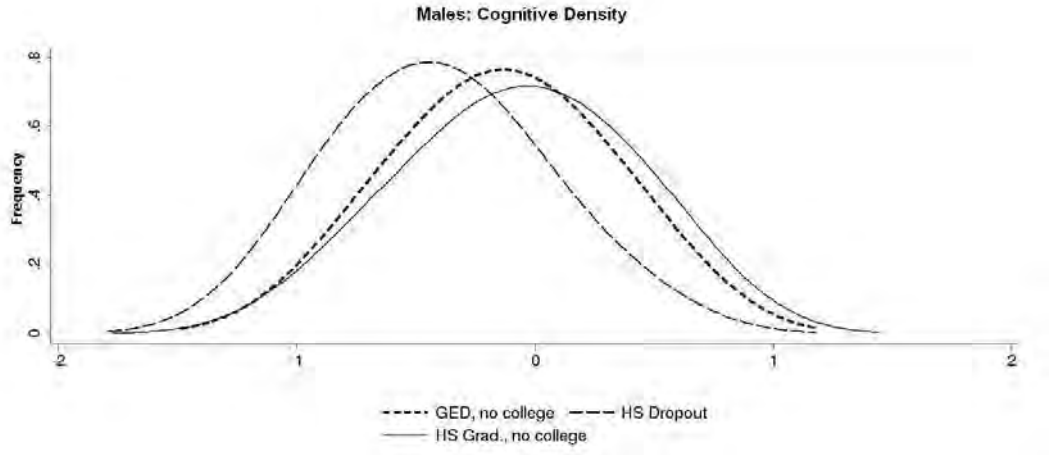
Test	**Correlation**	**Source(s)**
Armed Forces Qualification Test (AFQT)	0.75 - 0.79 †	Means and Laurence (1984)
Iowa Test of Educational Development	0.88 †	Means and Laurence (1984)
ACT	0.80 †	Means and Laurence (1984)
Adult Performance Level (APL) Survey	0.81 †	Means and Laurence (1984)
New York's Degrees of Reading Power (DRP) Test	0.77 †	Means and Laurence (1984)
Test of Adult Basic Education (TABE)	0.66-0.68†	Means and Laurence (1984)
General Aptitude Test Battery (GATB)	0.61-0.67†	Means and Laurence (1984)
National Adult Literacy Survey (NALS) factor	0.78 ‡	Baldwin (1995)

† Uses mean GED subtest scores
‡ Uses a general GED factor

GED recipients are smarter than other dropouts. Figure 5 shows the distributions of a factor extracted from the components of the ASVAB for male high school dropouts, GED recipients, and high school graduates.[49] The sample excludes people who attend post-secondary education. The distribution of the scores of GED recipients is much more like that of high school graduates than that of high school dropouts.

[49]Similar results are found for females.

Figure 5: Cognitive ability by educational status



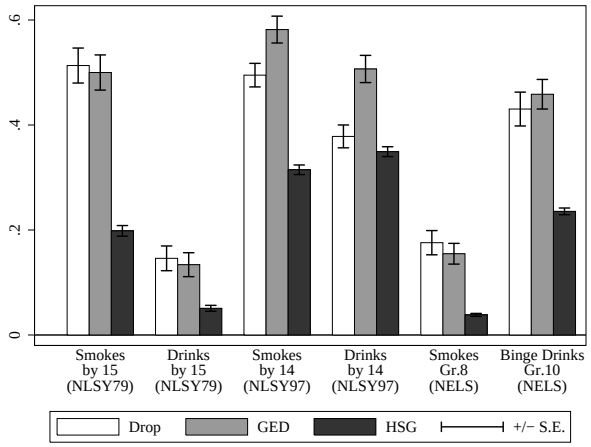
Source: Reproduced from Heckman et al. (2011b), which uses data from the National Longitudinal Study of Youth 1979 (NLSY79). Notes: The distributions above represent cognitive ability factors estimated using a subset of the Armed Services Vocational Aptitude Battery (ASVAB) and educational attainment as laid out in Hansen et al. (2004). The sample is restricted to the cross-sectional subsample for both males and females. Distributions show only those with no post-secondary educational attainment. The cognitive ability factors are normalized by gender to be mean zero standard deviation one.

If they have the same cognitive ability as high school graduates, then why do they drop out of high school? Success in school requires other traits. On a variety of other dimensions, GED recipients behave much more like other dropouts. Figure 6 shows measures of early adolescent drug use, crime, sex, and violence extracted from three data sources.[50] Male high school graduates perform better on all measures than high school dropouts or GED recipients. GED recipients are much more similar to dropouts, but in several cases are statistically significantly *more likely* to engage in risky behaviors than other dropouts. On no outcome measure in that figure are dropouts statistically significantly more likely to engage in risky behaviors compared to GED recipients. Figure 7 summarizes these adolescent behaviors using a single factor and shows that unlike the cognitive summary measures, the distribution of the noncognitive (personality) summary measure of GED recipients is much closer to that of dropouts than to that of high school graduates.

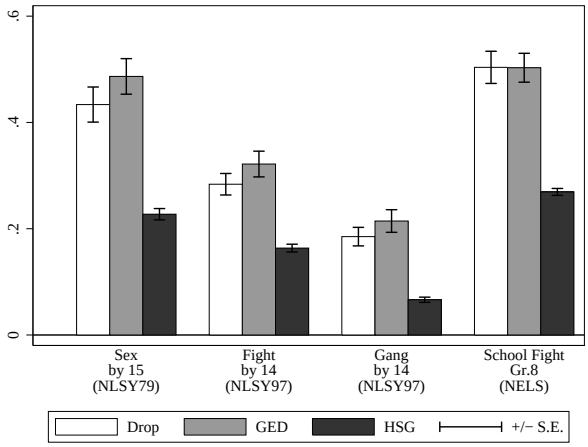
[50]The data sets are the National Longitudinal Survey of Youth 1979 (NLSY79), National Longitudinal Survey of Youth 1997 (NLSY97), and National Educational Longitudinal Survey (NELS). For discussion of these data sets, see Heckman et al. (2012a).

Figure 6: Measures of Adolescent Behaviors for Male Dropouts, GED Recipients, and High School Graduates

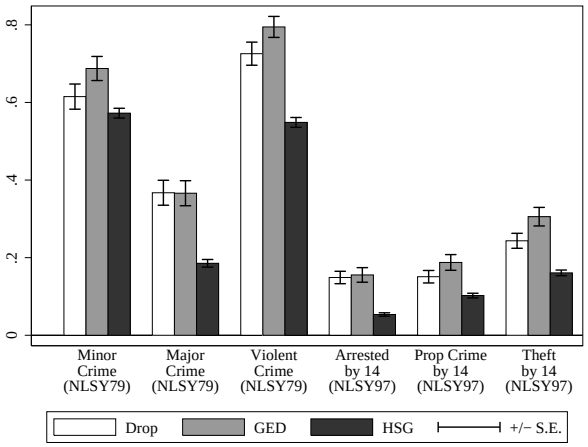
(a) Smoking and Drinking



(b) Sex and Violent Behavior

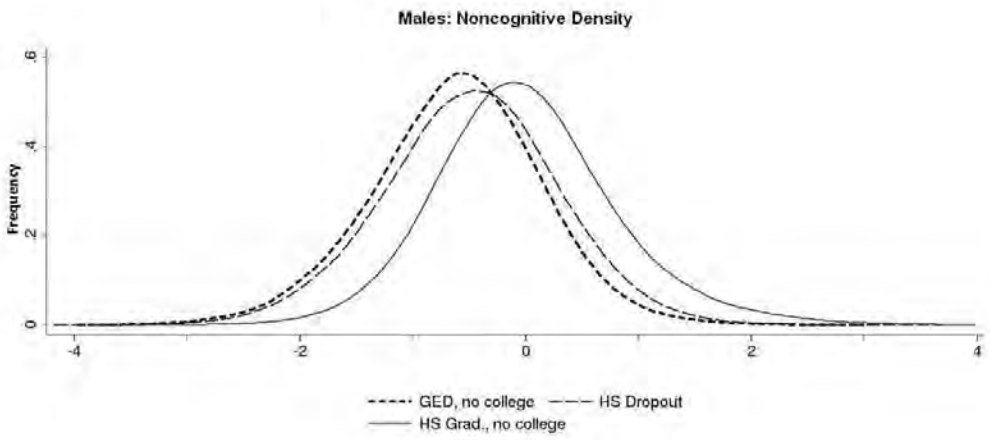


(c) Criminal Behavior



Sources: Heckman et al. (2012a, Chapter 3). National Longitudinal Survey of Youth 1979 (NLSY79), National Longitudinal Survey of Youth 1997 (NLSY97), National Educational Longitudinal Survey (NELS). Notes: Minor crime includes vandalism, shoplifting, petty theft, fraud, holding or selling stolen goods. Major crime includes auto theft, breaking/entering private property, grand theft. Violent crime includes fighting, assault, aggravated assault. Tests of Significance: The estimates for GED recipients and high school graduates are statistically significantly different at the 5% level for all variables. The estimates for dropouts and high school graduates are statistically significantly different at the 5% level for all variables, except for "Minor Crime (NLSY79)" and "Drinks by 14 (NLSY97)." The estimates of "Smokes by 14 (NLSY97)," "Drinks by 14 (NLSY97)," and "Theft by 14 (NLSY97)" between GED recipients and dropouts are statistically significantly different at the 5% level.

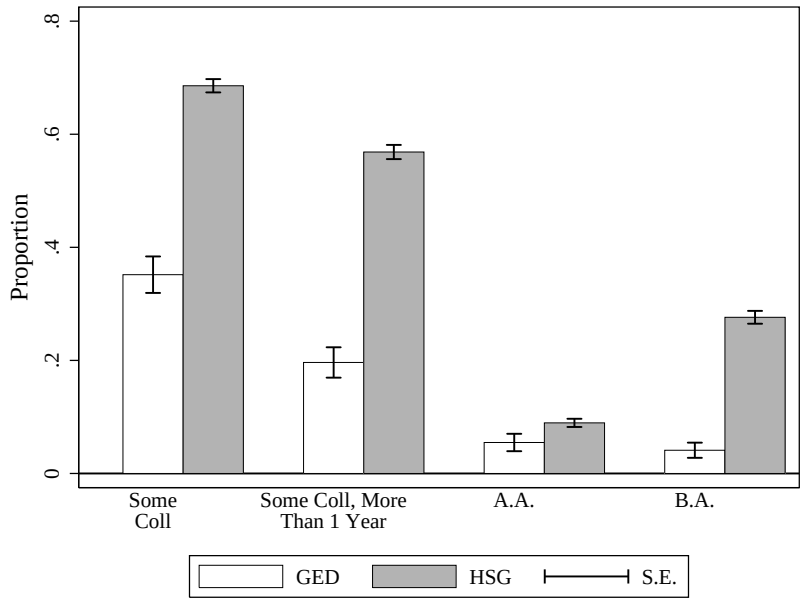
Figure 7: Distribution of a Summary Measure of Noncognitive Ability by Education Group



Source: Reproduced from Heckman et al. (2011b), which uses data from the National Longitudinal Study of Youth 1979 (NLSY79). Notes: The distributions above represent noncognitive ability factors estimated using measures of early violent crime, minor crime, marijuana use, regular smoking, drinking, early sexual intercourse, and educational attainment as in Hansen et al. (2004). Sample restricted to the cross-sectional subsample for both males and females. Distributions show only those with no post-secondary educational attainment. The noncognitive ability factors normalized to be mean zero standard deviation one.

The traits that cause GED recipients to drop out of high school manifest themselves in many other life outcomes. One potential benefit of the GED certificate is that it opens doors to post-secondary education. Figure 8 shows post-secondary educational attainment for GED recipients and high school graduates. About 40% of GED recipients enroll in a 2- or 4- year college. Nearly half drop out within the first year. Fewer than 5% earn a B.A. degree and fewer than 10% earn an A.A. degree.

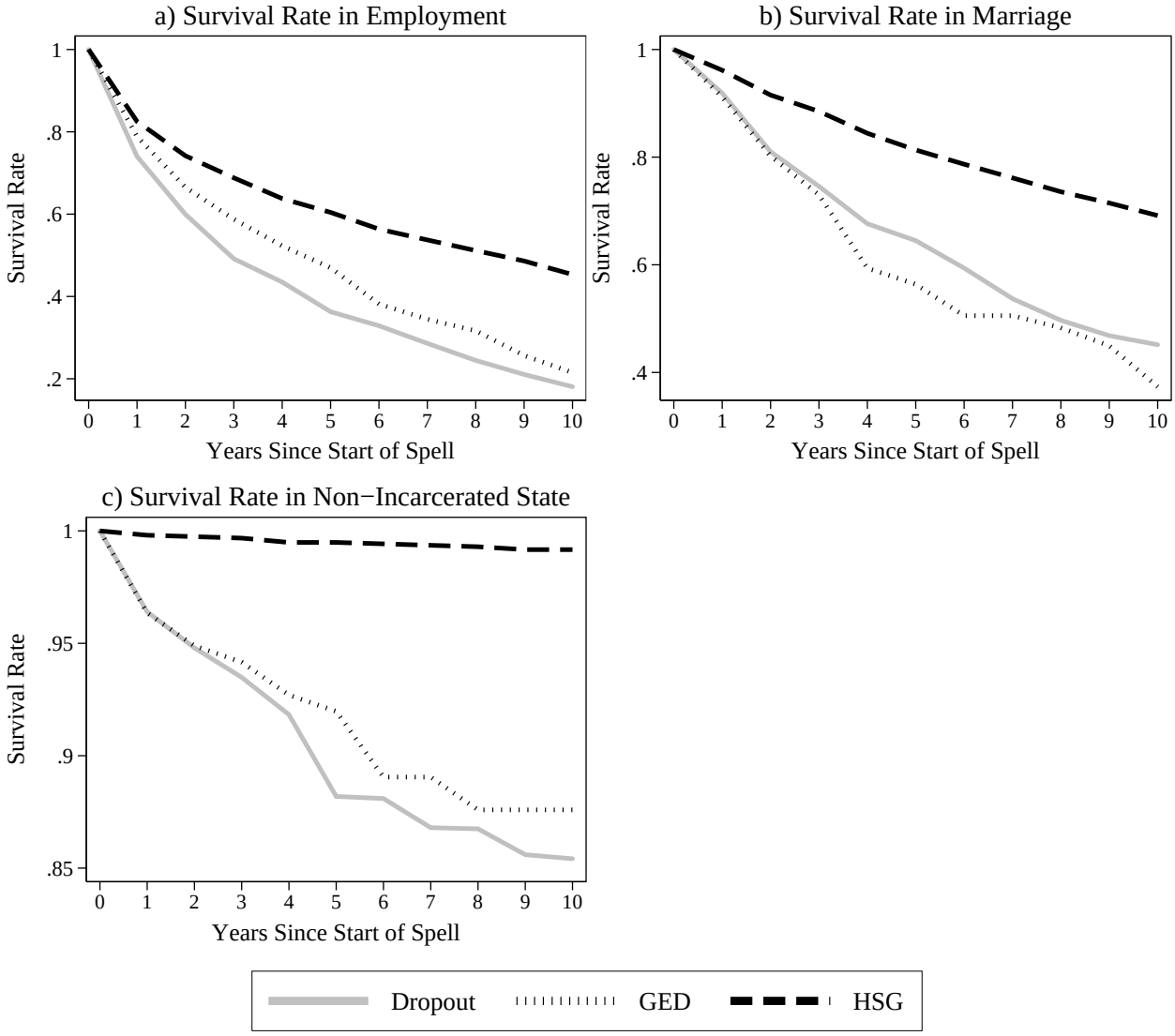
Figure 8: Post-Secondary Educational Attainment Across Education Groups Through Age 40 - Males



Sources: Heckman et al. (2012a, Chapter 4). National Longitudinal Survey of Youth 1979 (NLSY79). Notes: The graph shows post-secondary educational attainment of GED recipients and high school graduates. Variable Definitions: "Some College" represents people who entered any post-secondary institution ever. "Some College, More Than a Year" represents people who completed at least a year of some post-secondary education ever. "A.A." represents people who obtained associate's degrees ever. "B.A." represents people who obtained bachelor's degrees ever. "B.A." also includes people with higher education: M.A. Ph.D and professional degrees. Tests of Significance: The estimates for GED recipients and high school graduates are statistically significantly different at the 5% level for all but attainment of the A.A. degree.

GED recipients lack persistence in a variety of tasks in life. Figure 9 shows the survival rates in employment, marriage, and in the condition of not having been incarcerated. GED recipients tend to exit employment, become divorced, and enter jail at rates similar to those of high school dropouts, while high school graduates are much more persistent.

Figure 9: Survival Rates in Various States for Male Dropouts, GED Recipients, and High School Dropouts

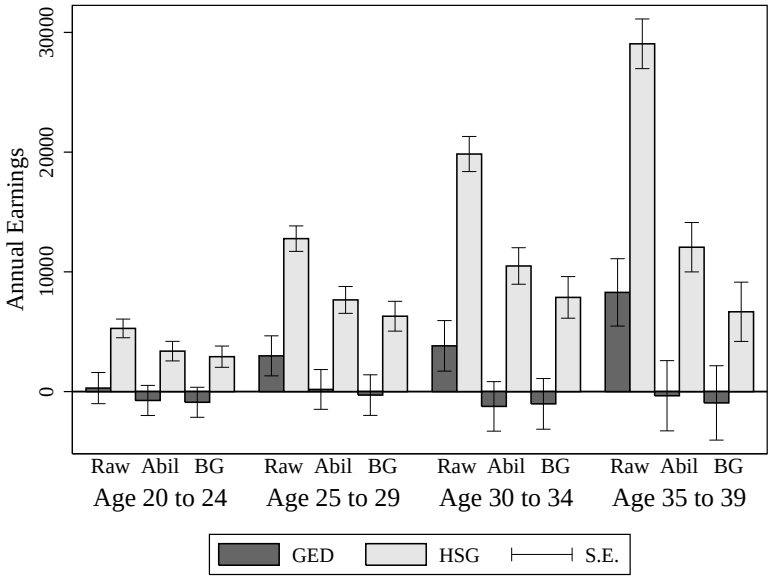


Source: Heckman et al. (2012a, Chapter 4). National Longitudinal Survey of Youth 1979 (NLSY79), nationally representative cross sectional sample. Notes: The "Survival Rate in Marriage" is based on the first marriage spell that began after 1979. People who were already married or divorced in 1979 were excluded from the sample, because the length of their spell is unknown. The "Survival Rate in Employment" is based on all employment spells that began after 1979 and after the respondent was 16. People are excluded from the employment estimates if they have been to jail. The "Survival Rate in Non-Incarcerated State" is based on the time until first incarceration starting at age 22 (the youngest age for which the jail status is available for all respondents). Respondents who were already in jail at age 22 were excluded from the sample. Tests of Significance: The estimates for GED recipients and high school graduates are statistically significantly different at the 5% level in all cases except for the first year of the "Survival Rate in Employment" and the first year of the "Survival Rate in Marriage." The estimates for dropouts and high school graduates are statistically significantly different at the 5% level in all cases. The estimates for dropouts and GED recipients are significantly different at the 5% level for years three through five of the "Survival Rate in Employment."

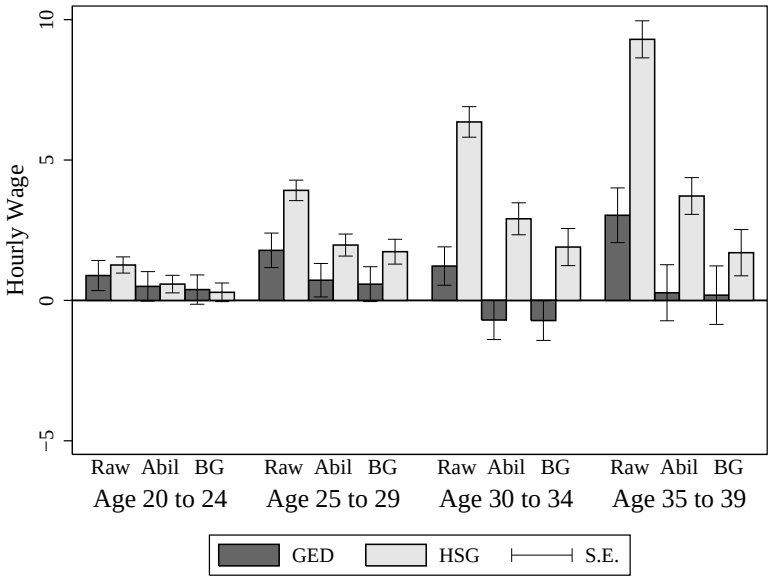
Adjusting for their differences in cognitive ability, male GED recipients perform virtually the same as high school dropouts in the labor market. Figure 10 shows the hourly wages and annual earnings of male GED recipients and high school graduates compared to high school dropouts for different age groups. The first set of bars shows the outcomes after adjusting for age, race, year, and region of residence. The second set of bars shows the effects after additionally adjusting for AFQT scores. The third set of bars shows the effects after additionally adjusting for standard measures of family background. GED recipients and high school graduates outperform dropouts in regressions that only adjust for age, race, year, and region of residence. After adjusting for cognitive ability, GED recipients are indistinguishable from dropouts, whereas high school graduates earn more and have higher hourly wages. Controlling for family background characteristics does not change the story.

Figure 10: Labor Market Outcomes Differences - By Age - NLSY79 - Males

(a) Annual Earnings



(b) Hourly Wage



Source: Heckman et al. (2012a, Chapter 3). National Longitudinal Survey of Youth 1979 (NLSY79). Controls: *"Raw"* – age, race, and region of residence; *"Abil"* –age, race, year, region of residence, and Armed Forces Qualification Test (AFQT) adjusted for schooling at time of test; *"BG"* – age, race, year, region of residence, mother's highest grade completed, urban status at age 14, family income in 1978, broken home status at age 14, south at age 14, AFQT, and factors based on adolescent behavioral measures, crime and school performance. Regressions exclude those reporting earning more than $300,000 or working more than 4,000 hours. Notes: All regressions allow for heteroskedastic errors and when appropriate clustering at the individual level.

Most of the patterns found for women parallel those found for men. However, there are some important differences.[51] While female GED recipients share similar cognitive and personality traits as male GED recipients, their outcomes differ. After accounting for differences in cognitive ability, female GED recipients do not earn higher hourly wages than other dropouts, but unlike men they have higher annual earnings because they are more likely to participate in the labor force.[52]

3.4 Evidence from The Perry Preschool Program and Other Interventions

Evidence from the Perry Preschool Program shows how personality traits can be changed in ways that produce beneficial lifetime outcomes. The Perry preschool Program enriched the lives of three- and four-year-old low-income, Black children with initial IQs below 85 at age 3.[53]

Participants were taught social skills in a "plan-do-review" sequence where students planned a task, executed it, and then reviewed it with teachers and fellow students. They learned to work with others when problems arose.[54] In addition, home visits promoted parent-child interactions. The program ended after two years of enrollment and both treatments and controls entered the same school. The program was evaluated by the method of random assignment.

The program did not improve IQ scores in a lasting way. Figure 11 shows that, by age ten, treatment and control groups had the same average IQ scores. Many critics of early childhood programs seize on this finding and related evidence to dismiss the value of early

[51] See Heckman et al. (2012a).

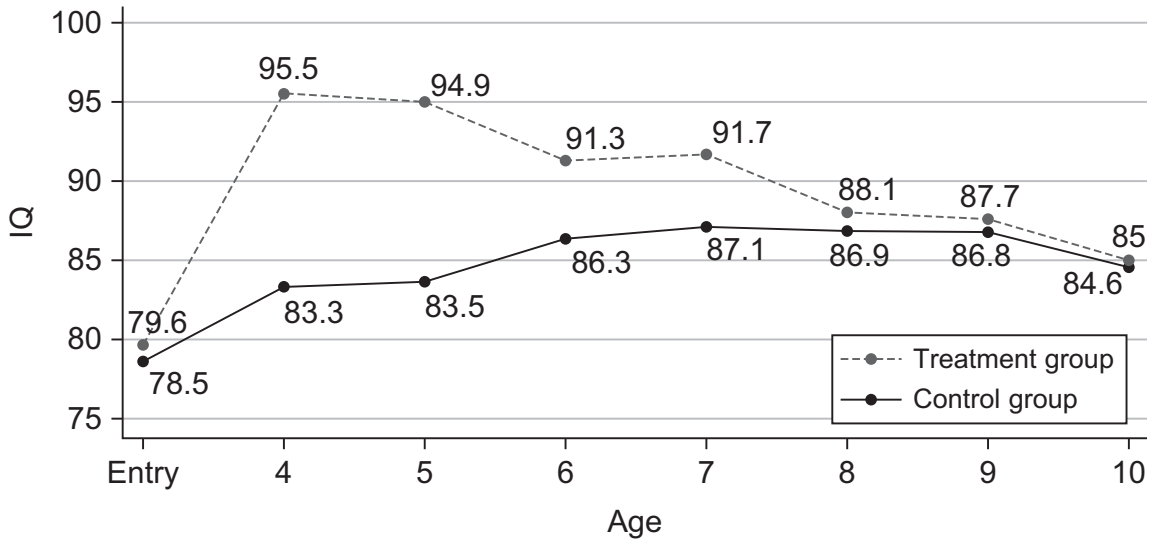
[52] The increased labor supply response is largely due to female GED recipients who attain some post-secondary education or who have dropped out of high school due to pregnancy. See Heckman et al. (2012a) for a full discussion of the evidence on the performance of GED recipients.

[53] We draw on the analysis of Heckman et al. (2012b).

[54] Sylva (1997) describes the Perry program as a Vygotskian program fostering personality traits. Vygotsky developed a psychology of child development in structured social settings that emphasized development of social and personality skills. The Vygotskian approach strongly influences the Tools of the Mind program (see Bodrova and Leong, 2001, 2007).

intervention studies.

Figure 11: Perry Preschool Program: IQ, by Age and Treatment Group



Notes: IQ measured on the Stanford-Binet Intelligence Scale (Terman and Merrill, 1960). The test was administered at program entry and at each of the ages indicated. Source: Cunha et al. (2006) and Heckman and Masterov (2007) based on data provided by the High Scope Foundation.

Nevertheless, the program improved outcomes for both boys and girls, resulting in a statistically significant rate of return of around 6-10% per annum for both boys and girls (see Heckman et al., 2010a,b). These returns are above the post-World War II, pre-2008 meltdown in stock market returns to equity estimated to be 5.8% per annum.[55]

The Perry Preschool Program worked primarily through improving personality traits. Participants had better direct measures of personal behavior (a weighted average of "absences and truancies," "lying and cheating," "stealing," and "swears or uses obscene words" measured by teachers in the elementary school years). Participants of both genders improved their "externalizing behavior," a psychological construct related to Agreeableness and Conscientiousness. For girls, the program improved Openness to Experience (proxied by academic motivation). The program also improved scores on the California Achievement

[55]See DeLong and Magin (2009).

Test (CAT). This evidence is consistent with the evidence presented in the previous section that shows that performance on achievement tests depends on personality traits.

Other studies are broadly consistent with the evidence from the Perry Preschool study. Analyses of data from Project STAR, a program that randomly assigned kindergartners and teachers to classes of different sizes, yields results similar to the Perry Program. Using data from Project STAR, Dee and West (2011) find that assignment to a small class is associated with positive changes in personality. In a follow-up analysis, Chetty et al. (2011) examine the Project STAR program and find that students placed in higher quality kindergarten classes–as measured by their peer's average performance on a Stanford Achievement Test–had significantly higher earnings in early adulthood.

The curriculum of Promoting Alternative Thinking Strategies (PATHS) teaches self-control, emotional awareness, and social problem-solving skills and is aimed at elementary school children (see Bierman et al., 2010). A recent random-assignment, longitudinal study demonstrates that the PATHS curriculum reduces teacher and peer ratings of aggression, improves teacher and peer ratings of prosocial behavior, and improves teacher ratings of academic engagement.[56] PATHS is an exemplar of school-based social and emotional learning (SEL) programs. A recent meta-analysis shows that the program improved grades by 0.33 standard deviations and achievement test scores by 0.27 standard deviations (Durlak et al., 2011).[57]

Likewise, several random assignment evaluations of *Tools of the Mind*, a preschool and early primary school curriculum targeting development of self-control, show that it improves classroom behavior as well as executive function, defined as higher-level cognitive skills including inhibitory control, working memory, and cognitive flexibility (Barnett et al., 2008, 2006; Bodrova and Leong, 2001, 2007; Diamond et al., 2007; Lillard and Else-Quest, 2006).[58]

[56]See Bierman et al. (2010).

[57]Note, however, that the largest federal study to date on character education programs, including PATHS, failed to find evidence for improvements in behavior or academic performance (see Social and Character Development Research Consortium, 2010).

[58]However, a more recent large-scale study (Farran et al., 2011) does not find any effect of the program on self-regulation or literacy, language, and mathematics achievement.

Positive findings are reported for the Montessori preschool curriculum (Lillard and Else-Quest, 2006). Unlike the Perry study, these studies do not have long-term followups.

There is evidence that targeted intervention efforts can improve aspects of Conscientiousness. In contrast to the multi-faceted curricula described above, studies targeting improvement in this trait are designed to isolate a particular mechanism producing behavioral change. For instance, Rueda et al. (2005) designed a set of computer exercises to train attention in children between four and six years of age. Children in the intervention group improved in performance on computer tasks of attention relative to children who instead watched interactive videos for a comparable amount of time. Similarly, Stevens et al. (2008) designed a 6-week computerized intervention and showed that it can improve selective auditory attention (i.e., the ability to attend to a target auditory signal in the face of an irrelevant, distracting auditory signal). As is typical of much of the literature, all of these programs have only short-term follow-ups.

Several studies suggest that personality can be remediated in adolescence. Martins (2010) analyzes data from EPSIS, a program developed to improve student achievement of 13-15 year-olds in Portugal by increasing motivation, self-esteem, and study skills. The program consists of one-on-one meetings with a trained staff member or meetings in small groups. The intervention was tailored to each participant's individual skill deficit. Overall, the program was successful and cost-effective, decreasing grade retention by 10 percentage points.

Other life experiences, like employment, can improve personality. Gottschalk (2005) analyzes evidence from a randomized control trial that working at a job can improve locus of control, a trait related to Neuroticism that measures the extent to which individuals believe that they have control over their lives through self-motivation or self-determination as opposed to the extent that the environment controls their lives (Rotter, 1966).[59] He uses data from the Self-Sufficiency Project (SSP) in which some welfare recipients were randomly offered substantial subsidies to work. The subsidy more than doubled the earnings of a

[59]The relationship between locus of control and the Big Five trait of Neuroticism is discussed in Almlund et al. (2011).

minimum wage worker. People in the experimental group worked about 30% more hours than those in the control group. After 36 months, those who received the subsidy were more likely to have an improved locus of control.

3.5 Additional Evidence

Studies that account for the endogeneity of investment and education provide further evidence of the causal effect of education and cognitive and personality traits on outcomes. Heckman et al. (2011b) estimate a sequential model of education to study the effects of education on a variety of outcomes. Correcting for selection into education, they find that early cognitive and personality traits affect schooling choices, labor market outcomes, adult health, and social outcomes and that increasing education promotes beneficial labor market, health, and social outcomes.

Heckman et al. (2006b) estimate a version of Equation (3) to analyze the effects of increases in education on measured cognition and personality measures.[60] Controlling for the problem of reverse causality that schooling may be caused by traits, they find that schooling improves both personality and cognitive traits and that these traits, in turn, boost outcomes.[61]

Cunha et al. (2010) estimate a model of the technology of skill formation using longitudinal data on the development of children with rich measures of parental investment and child traits. They control for the endogeneity of investment using shocks to family income along with other instruments. Their model is a version of Equation (3). Traits are self-productive and exhibit dynamic complementarity – current values of traits affect the evolution of future traits through direct and cross effects. A leading example of a cross effect is that more motivated children are more likely to learn. They estimate parameters that summarize how

[60] They estimate the effect of schooling on self-esteem and locus of control, personality traits related to Neuroticism. The Rosenberg Self-Esteem Scale attempts to assess the degree of approval or disapproval of oneself (Rosenberg, 1965). The relationship between these measures and the Big Five traits of Neuroticism is discussed in Almlund et al. (2011).

[61] Both Heckman et al. (2011b) and Heckman et al. (2006b) use an identification strategy based on matching on proxies for unobserved traits that corrects for measurement error and the endogeneity of schooling.

past personality traits affect future cognitive traits.

They find that self-productivity becomes stronger as children become older, for both cognitive and personality traits. The elasticity of substitution for cognitive inputs is *smaller* later in life. This means that it is more difficult to compensate for the effects of adverse environments on cognitive endowments at later ages than it is at earlier ages. This finding is consistent with the high rank stability of cognition over ages past 10-12 reported in the literature. It also helps to explain the evidence on the ineffectiveness of cognitive remediation strategies for disadvantaged adolescents documented in Cunha et al. (2006); Knudsen et al. (2006) and Cunha and Heckman (2007).

Personality traits foster the development of cognition but not vice versa. It is equally easy at all stages of the child's life cycle to compensate for early disadvantage in endowments using personality traits. (Elasticities of substitution for these traits are essentially the same at different stages of the life cycle.) The most effective adolescent interventions target personality traits.[62]

4 Summary

This paper reviews recent evidence on the importance of personality in economic and social life. It shows that success in life depends on many traits, not just those measured by IQ, grades, and standardized achievements tests. Personality traits predict and *cause* outcomes.

All psychological traits are measured by performance on tasks. Psychological traits have different productivities in different tasks. Performance on tasks depends on incentives and multiple traits, giving rise to a fundamental identification problem when measuring any single trait. This identification problem is empirically important even for measures of cognitive traits.

The importance of cognitive ability increases with the complexity of the task. Given their

[62] Cunha et al. (2006) report that 16% of the variation in educational attainment is explained by adolescent cognitive traits, 12% is due to adolescent personality (socioemotional traits), and 15% is due to measured parental investments.

endowments of traits and the incentives they face, people sort into tasks in life in pursuit of their comparative advantage.

Traits are stable across situations, but their manifestation depends on incentives to apply effort in the situations where they are measured and also depends on other traits and skills. However, traits are not set in stone. They change over the life cycle and can be enhanced by education, parenting, and environment to different degrees at different ages.

Scores on achievement tests capture both cognitive and personality traits. Children who are more academically motivated and more curious learn more and have higher test scores. More motivated children also try harder on achievement tests.

The evidence in this paper should give pause to analysts and policy makers who rely solely on achievement tests to monitor school performance and school systems. Standardized achievement tests do not adequately capture many skills that matter in life. GED recipients perform about as well as high school graduates on achievement tests but perform much worse in many aspects of life because they lack important personality traits. Categorizing GED recipients as high school graduates misrepresents national statistics on educational attainment.[63] The Perry Preschool Program improved the lives of its participants without increasing their IQ scores, demonstrating why it is problematic to focus curricula exclusively on improving cognitive test scores.

Monitoring school progress and creating programs to enhance skills requires a broader framework of measurement. Interventions that promote beneficial changes in personality have an important place in a portfolio of public policies to foster human development.

[63]See Heckman and LaFontaine (2010).

References

Ackerman, Phillip L., and Eric D. Heggestad. "Intelligence, personality, and interests: Evidence for overlapping traits." *Psychological Bulletin* 121: (1997) 219–245.

ACT, Inc. *The ACT Technical Manual*. Iowa City, IA: ACT, Inc., 2007.

Almlund, Mathilde, Angela Duckworth, James J. Heckman, and Tim Kautz. "Personality Psychology and Economics." In *Handbook of the Economics of Education*, edited by E. A. Hanushek, S. Machin, and L. Wößmann, Amsterdam: Elsevier, 2011, volume 4, 1–181.

Ayllon, Teodoro, and Kathy Kelly. "Effects of reinforcement on standardized test performance." *Journal of Applied Behavior Analysis* 5, 4: (1972) 477–484.

Baldwin, Janet. *Who Took the GED? GED 1994 Statistical Report*. Washington, D.C.: American Council on Education, GED Testing Service, Center for Adult Learning, 1995.

Barnett, W. Steven, Kwanghee Jung, Donald J. Yarosz, Jessica Thomas, Amy Hornbeck, Robert Stechuk, and Susan Burns. "Educational Effects of the Tools of the Mind Curriculum: A Randomized Trial." *Early Childhood Research Quarterly* 23, 3: (2008) 299–313.

Barnett, W. Steven, Donald J. Yarosz, Jessica Thomas, and Amy Hornbeck. "Educational effectiveness of a Vygotskian approach to preschool education: A randomized trial." Technical report, National Institute for Early Education Research, Rutgers, The State University of New Jersey, 2006.

Barrick, Murray R., and Michael K. Mount. "The Big Five personality dimensions and job performance: A meta-analysis." *Personnel Psychology* 44, 1: (1991) 1–26.

Baumeister, Roy F., and John (John Marion) Tierney. *Willpower : rediscovering the greatest human strength*. New York: Penguin Press, 2011.

Benjamin, Daniel J., Sebastian A. Brown, and Jesse M. Shapiro. "Who is 'Behavioral'? Cognitive Ability and Anomalous Preferences." Unpublished manuscript, Cornell University, Ithaca, NY, 2006.

Bierman, Karen L., John D. Coie, Kenneth A. Dodge, Mark T. Greenberg, John E. Lochman, Robert J. McMahon, and Ellen Pinderhughes. "The effects of a multiyear universal social-emotional learning program: The role of student and school characteristics." *Journal of Consulting and Clinical Psychology* 78, 2: (2010) 156–168.

Binet, Alfred, and Theodore Simon. *The development of intelligence in children (The Binet-Simon Scale)*. Psychological Science. Baltimore, MD: Williams & Wilkins Co, 1916.

Bodrova, Elena, and Deborah J. Leong. *Tools of the Mind: A case study of implementing the Vygotskian approach in American early childhood and primary classrooms*. Geneva: International Bureau of Education, UNESCO, 2001.

———. *Tools of the Mind: The Vygotskian Approach to Early Childhood Education*. Upper Saddle River: Pearson Education, Inc, 2007.

Borghans, Lex, Angela L. Duckworth, James J. Heckman, and Bas ter Weel. "The Economics and Psychology of Personality Traits." *Journal of Human Resources* 43, 4: (2008a) 972–1059.

Borghans, Lex, Bart H. H. Golsteyn, James J. Heckman, and John Eric Humphries. "Identification Problems in Personality Psychology." *Personality and Individual Differences* 51, Special Issue on Personality and Economics: (2011a) 315–320. E. Ferguson, J.J. Heckman, and P. Corr, editors.

———. "Reinterpreting Estimated Effects of Cognition on Social Outcomes." Unpublished manuscript, Department of Economics, University of Chicago, 2011b.

Borghans, Lex, Huub Meijers, and Bas ter Weel. "The Role of Noncognitive Skills in Explaining Cognitive Test Scores." *Economic Inquiry* 46, 1: (2008b) 2–12.

Bouchard, Thomas J., and John C. Loehlin. "Genes, Evolution and Personality." *Behavior Genetics* 31, 3: (2001) 243–273.

Bound, John, Charles Brown, and Nancy Mathiowetz. "Measurement Error in Survey Data." In *Handbook of Econometrics*, edited by James J. Heckman, and Edward Leamer, Amsterdam: Elsevier Science, 2001, volume 5 of *Handbooks in Economics*, 3705–3843.

Bowen, William G., Matthew M. Chingos, and Michael S. McPherson. "Test scores and high school grades as predictors." In *Crossing the finish line: Completing college at America's public universities*, Princeton, NJ: Princeton University Press, 2009, 112–133.

Bowles, Samuel, and Herbert Gintis. *Schooling in Capitalist America: Educational Reform and the Contradictions of Economic Life*. New York: Basic Books, 1976.

Bowles, Samuel, Herbert Gintis, and Melissa Osborne. "The Determinants of Earnings: A Behavioral Approach." *Journal of Economic Literature* 39, 4: (2001) 1137–1176.

Breuning, Stephen E., and William F. Zella. "Effects of individualized incentives on norm-referenced IQ test performance of high school students in special education classes." *Journal of School Psychology* 16, 3: (1978) 220.

Canli, Turhan. *Biology of Personality and Individual Differences*. New York: Guilford Press, 2006.

Carroll, Christopher D. "How Does Future Income Affect Current Consumption?" *Quarterly Journal of Economics* 109, 1: (1994) 111–147.

Carroll, John B. *Human Cognitive Abilities: A Survey of Factor-Analytic Studies*. New York: Cambridge University Press, 1993.

Cattan, Sarah. "Heterogeneity and Selection in the Labor Market." PhD Thesis, Economics Department, University of Chicago, 2012.

Chetty, Raj, John N. Friedman, Nathaniel Hilger, Emmanuel Saez, Schanzenbach Whitmore Diane, and Danny Yagan. "How Does Your Kindergarten Classroom Affect Your Earnings? Evidence from Project STAR." *Quarterly Journal of Economics* 126, 4: (2011) 1593–1660.

Clingman, Joy, and Robert L. Fowler. "The effects of primary reward on the I.Q. performance of grade-school children as a function of initial I.Q. level." *Journal of Applied Behavior Analysis* 9, 1: (1976) 19–23.

Cloninger, C. Robert, Dragan M. Svrakic, Carmen Bayon, and Thomas R. Przybeck. "Measurement of psychopathology as variants of personality." In *Personality and psychopathology*, edited by C. Robert Cloninger, Arlington, VA: American Psychiatric Publishing, Inc., 1999.

Costa, Paul T., and Robert R. McCrae. "Four Ways Five Factors are Basic." *Personality and Individual Difference* 13, 6: (1992a) 653–665.

———. *Revised NEO Personality Inventory (NEO PI-R) and the NEO Five-Factor Inventory (NEO-FFI) professional manual*. Odessa, FL: Psychological Assessment Resources, 1992b.

Cunha, Flavio, and James J. Heckman. "The Technology of Skill Formation." *American Economic Review* 97, 2: (2007) 31–47.

Cunha, Flavio, James J. Heckman, Lance J. Lochner, and Dimitriy V. Masterov. "Interpreting the Evidence on Life Cycle Skill Formation." In *Handbook of the Economics of Education*, edited by Eric A. Hanushek, and Frank Welch, Amsterdam: North-Holland, 2006, chapter 12, 697–812.

Cunha, Flavio, James J. Heckman, and Susanne M. Schennach. "Estimating the Technology of Cognitive and Noncognitive Skill Formation." *Econometrica* 78, 3: (2010) 883–931.

Damasio, Hanna, Thomas Grabowski, Randall Frank, Albert M. Galaburda, and Antonio R. Damasio. "The return of Phineas Gage: Clues about the brain from the skull of a famous patient." In *Social neuroscience: Key readings*, edited by John T. Cacioppo, and Gary G. Berntson, New York, NY: Psychology Press, 2005, 21–28.

Dee, Thomas S., and Martin R. West. "The Non-Cognitive Returns to Class Size." *Educational Evaluation and Policy Analysis* 33, 1: (2011) 23–46.

DeLong, J. Bradford, and Konstantin Magin. "The U.S. Equity Return Premium: Past, Present and Future." *Journal of Economic Perspectives* 23, 1: (2009) 193–208.

Devlin, Bernie, Michael Daniels, and Kathryn Roeder. "The heritability of IQ." *Nature* 388, 6641: (1997) 468–471.

DeYoung, Colin G., Jacob B. Hirsh, Matthew S. Shane, Xenophon Papademetris, Nallakkandi Rajeevan, and Jeremy R. Gray. "Testing Predictions From Personality Neuroscience: Brain Structure and the Big Five." *Psychological Science* 21, 6: (2010) 820–828.

Diamond, Adele, Steven Barnett, Jessica Thomas, and Sarah Munro. "Preschool Program Improves Cognitive Control." *Science* 318, 5855: (2007) 1387–1388.

Duckworth, Angela L., Christopher Peterson, Michael D. Matthews, and Dennis R. Kelly. "Grit: Perseverance and Passion for Long-Term Goals." *Journal of Personality and Social Psychology* 92, 6: (2007) 1087–1101.

Durlak, Joseph A., Roger P. Weissberg, Allison B. Dymnicki, Rebecca D. Taylor, and Kriston B. Schellinger. "The Impact of Enhancing Students Social and Emotional Learning: A Meta-Analysis of School-Based Universal Interventions." *Child Development* 82, 1: (2011) 405–432.

Edlund, Calvin V. "The effect on the behavior of children, as reflected in the IQ scores, when reinforced after each correct response." *Journal of Applied Behavior Analysis* 5, 3: (1972) 317–319.

Epstein, Seymore. "The Stability of Behavior: I. On Predicting Most of the People Much of the Time." *Journal of Personality and Social Psychology* 37, 7: (1979) 1097–1126.

Farran, Dale C., Mark W. Lipsey, and Sandra Wilson. "Experimental Evaluation of the Tools of the Mind Pre-K Curriculum." Technical report, Peabody Research Institute Report, 2011.

Feingold, Alan. "The validity of the information and vocabulary subtests of the WAIS." *Journal of Clinical Psychology* 38, 1: (1982) 169–174.

Figner, Bernd, Daria Knoch, Eric J. Johnson, Amy R. Krosch, Sarah H. Lisanby, Ernst Fehr, and Elke U. Weber. "Lateral prefrontal cortex and self-control in intertemporal choice." *Nature Neuroscience* 13, 5: (2010) 538–539.

Flynn, James R. *What is Intelligence?: Beyond the Flynn Effect*. New York: Cambridge University Press, 2007.

Friedman, David, and Arline H. Streicher. "Reliability of Scores for Fiscal Year 1981 Army Applicants: Armed Services Vocational Aptitude Battery Forms 8, 9, and 10." Technical report, Defense Technical Information Center, 1985.

GED Testing Service. "The Technical Manual: 2002 Series GED Tests." Technical manual, American Council on Education and GED Testing Service, Washington, DC, 2009. `http://www.acenet.edu/Content/NavigationMenu/ged/pubs/TechnicalManual_2002SeriesGEDTests.pdf`.

Gensowski, Miriam. "Personality, IQ, and Lifetime Earnings." Unpublished manuscript, University of Chicago, Department of Economics, 2012.

Gottfredson, Linda S. "Why g Matters: The Complexity of Everyday Life." *Intelligence* 24, 1: (1997) 79–132.

Gottschalk, Peter. "Can work alter welfare recipients' beliefs?" *Journal of Policy Analysis and Management* 24, 3: (2005) 485–498.

Gough, Harrison G., and Alfred B. Heilbrun. *The Adjective Check List Manual*. Palo Alto, CA: Consulting Psychologists Press, 1983.

Greene, Anthony C., Gary L. Sapp, and Brad Chissom. "Validation of the Stanford-Binet Intelligence Scale: Fourth Edition With Exceptional Black Male Students." *Psychology in the Schools* 27, 1: (1990) 35–41.

Grek, S. "Governing by numbers: the PISA 'effect' in Europe." *Journal of Education Policy* 24, 1: (2009) 23–37.

Hansen, Karsten T., James J. Heckman, and Kathleen J. Mullen. "The Effect of Schooling and Ability on Achievement Test Scores." *Journal of Econometrics* 121, 1-2: (2004) 39–98.

Hartlage, Lawrence C., and Carol T. Steele. "WISC and WISC-R correlates of academic achievement." *Psychology in the Schools* 14, 1: (1977) 15–18.

Heckman, James J., John Eric Humphries, and Tim Kautz. "*The GED and the Role of Character in American Life*." Unpublished book manuscript, University of Chicago, Department of Economics, 2012a.

Heckman, James J., John Eric Humphries, and Nicholas Mader. "The GED." In *Handbook of the Economics of Education*, edited by Eric A. Hanushek, Stephen Machin, and Ludger Wößmann, Amsterdam: North Holland, Elsevier, 2011a, volume 3, chapter 9, 423–484.

Heckman, James J., John Eric Humphries, Sergio Urzúa, and Gregory Veramendi. "The Effects of Educational Choices on Labor Market, Health, and Social Outcomes." Unpublished manuscript, University of Chicago, Department of Economics, 2011b.

Heckman, James J., and Paul A. LaFontaine. "The American High School Graduation Rate: Trends and Levels." *Review of Economics and Statistics* 92, 2: (2010) 244–262.

Heckman, James J., Lena Malofeeva, Rodrigo Pinto, and Peter A. Savelyev. "Understanding the Mechanisms Through Which an Influential Early Childhood Program Boosted Adult Outcomes." Unpublished manuscript, University of Chicago, Department of Economics (first draft, 2008). Under revision, *American Economic Review*, 2012b.

Heckman, James J., and Dimitriy V. Masterov. "The Productivity Argument for Investing in Young Children." *Review of Agricultural Economics* 29, 3: (2007) 446–493.

Heckman, James J., Seong Hyeok Moon, Rodrigo Pinto, Peter A. Savelyev, Azeem Shaikh, and Adam Q. Yavitz. "The Perry Preschool Project: A Reanalysis." Unpublished manuscript, University of Chicago, Department of Economics, 2006a.

Heckman, James J., Seong Hyeok Moon, Rodrigo Pinto, Peter A. Savelyev, and Adam Q. Yavitz. "Analyzing Social Experiments as Implemented: A Reexamination of the Evidence From the HighScope Perry Preschool Program." *Quantitative Economics* 1, 1: (2010a) 1–46. First draft, September, 2006.

———. "The Rate of Return to the HighScope Perry Preschool Program." *Journal of Public Economics* 94, 1-2: (2010b) 114–128.

Heckman, James J., Jora Stixrud, and Sergio Urzúa. "The Effects of Cognitive and Noncognitive Abilities on Labor Market Outcomes and Social Behavior." *Journal of Labor Economics* 24, 3: (2006b) 411–482.

Herrnstein, Richard J., and Charles A. Murray. *The Bell Curve: Intelligence and Class Structure in American Life*. New York: Free Press, 1994.

Holt, Michael M., and Tom R. Hobbs. "The effects of token reinforcement, feedback and

response cost on standardized test performance." *Behaviour Research and Therapy* 17, 1: (1979) 81–83.

Jencks, Christopher. *Who Gets Ahead? The Determinants of Economic Success in America*. New York: Basic Books, 1979.

John, Oliver P., and Sanjay Srivastava. "The Big Five Trait Taxonomy: History, Measurement and Theoretical Perspectives." In *Handbook of Personality: Theory and Research*, edited by L. A. Pervin, and O. P. John, New York: The Guilford Press, 1999, chapter 4, 102–138.

Kettner, Norman. "Armed Services Vocational Aptitude Battery (ASVAB Form 5): Comparison with GATB and DAT Tests: Final Report for Period May 1975–October 1976." Technical report, DTIC Document: Department of Defense, Department of the Air Force, Air Force Systems Command, Air Force Human Resources Laboratory, 1976.

Knudsen, Eric I., James J. Heckman, Judy Cameron, and Jack P. Shonkoff. "Economic, Neurobiological, and Behavioral Perspectives on Building America's Future Workforce." *Proceedings of the National Academy of Sciences* 103, 27: (2006) 10,155–10,162.

Kobrin, Jennifer L., Brian F. Patterson, Emily J. Shaw, Krista D. Mattern, and Sandra M. Barbuti. "Validity of the SAT for predicting first-year college grade point average." *The College Board* 5: (2008) 1–10.

Kosfeld, Michael, Markus Heinrichs, Paul J. Zak, Urs Fischbacher, and Ernst Fehr. "Oxytocin increases trust in humans." *Nature* 435, 7042: (2005) 673–676.

Larson, Gerald E., Dennis P. Saccuzzo, and James Brown. "Motivation: Cause or confound in information processing/intelligence correlations?" *Acta Psychologica* 85, 1: (1994) 25–37.

Lemann, Nicholas. *The Big Test: The Secret History of the American Meritocracy.* New York: Farrar, Straus and Giroux, 1999.

Lillard, Angeline, and Nicole Else-Quest. "The Early Years: Evaluating Montessori." *Science* 313, 5795: (2006) 1893–1894.

Lindquist, Everet Franklin. "Preliminary Considerations in Objective Test Construction." In *Educational Measurement*, edited by E. F. Lindquist, Washington, DC: American Council on Education, 1951, 119–184.

Martins, Pedro S. "Can Targeted, Non-Cognitive Skills Programs Improve Achievement?" Discussion Paper 5266, IZA, 2010.

McAdams, Dan P., and Jennifer L. Pals. "A New Big Five: Fundamental Principles for an Integrative Science of Personality." *American Psychologist* 61, 3: (2006) 204–217.

McArdle, John J., Fumiaki Hamagami, William Meredith, and Katherine P. Bradway. "Modeling the dynamic hypotheses of Gf-Gc theory using longitudinal life-span data." *Learning and Individual Differences* 12, 1: (2000) 53–79.

Means, B., and Janice H. Laurence. "Characteristics and Performance of Recruits Enlisted with General Educational Development (GED) Credentials." Technical Report FR-PRD-84-6, Human Resources Research Organization, Alexandria, VA, 1984.

Michalko, K. T., and D. H. Saklofske. "A Psychometric Investigation of the Wechsler Individual Achievement Test with a Sample of Saskatchewan Schoolchildren." *Canadian Journal of School Psychology* 12, 1: (1996) 44–54.

Mischel, Walter. *Personality and Assessment.* New York: Wiley, 1968.

Murray, Henry Alexander. *Explorations in personality: a clinical and experimental study of fifty men of college age.* New York: Oxford University Press, 1938.

National Center for Education Statistics. "Digest of Education Statistics." Institute of Education Sciences, U.S. Department of Education. Washington, DC., Various.

Niolon, Richard. "Introduction to the WAIS III." Available at `http://www.psychpage.com/learning/library/intell/wais_history.html`, posted August, 2005, 2005.

Nisbett, Richard E. *Intelligence and How to Get It: Why Schools and Cultures Count*. New York, NY: W. W. Norton and Company, 2009.

Nisbett, Richard E., Joshua Aronson, Clancy Blair, William Dickens, James Flynn, Diane F. Halpern, and Eric Turkheimer. "Intelligence: New findings and theoretical developments." *American Psychologist* 67, 2: (2012) 130–159.

O'Leary, Una-Marie, Kathleen M. Rusch, and Stephen J. Guastello. "Estimating Age-Stratified WAIS-R IQs from scores on the Raven's Standard Progressive Matrices." *Journal of Clinical Psychology* 47, 2: (1991) 277–284.

Omizo, Michael M. "The Differential Aptitude Tests as Predictors of Success in a High School for Engineering Program." *Educational and Psychological Measurement* 40, 1: (1980) 197–203.

R. R. Bowker Publishing. "The Bowker Annual: Library and Book Trade Almanac.", Various.

Raven, J., J. C. Raven, and J.H. Court. *Manual for Raven's progressive matrices and vocabulary scales*. San Antonio, TX: Harcourt Assessment, 1988.

Raven, John C. *Advanced progressive matrices: Sets I and II*. London: H.K. Lewis, 1962, revised edition.

Roberts, B. W., N. R. Kuncel, R. L. Shiner, A. Caspi, and L. R. Goldberg. "The power of personality: The comparative validity of personality traits, socioeconomic status, and

cognitive ability for predicting important life outcomes." *Perspectives in Psychological Science* 2, 4: (2007) 313–345.

Roberts, Brent W. "Back to the Future: Personality and Assessment and Personality Development." *Journal of Research in Personality* 43, 2: (2009) 137–145.

Roberts, Brent W., and Daniel Mroczek. "Personality Trait Change in Adulthood." *Current Directions in Psychological Science* 17, 1: (2008) 31–35.

Roberts, Brent W., Kate E. Walton, and Wolfgang Viechtbauer. "Patterns of mean-level change in personality traits across the life course: A meta-analysis of longitudinal studies." *Psychological Bulletin* 132, 1: (2006) 1–25.

Roberts, Richard D., Ginger Nelson Goff, Fadi Anjoul, P. C. Kyllonen, Gerry Pallier, and Lazar Stankov. "The Armed Services Vocational Aptitude Battery (ASVAB): Little more than acculturated learning (Gc)!?" *Learning and Individual Differences* 12, 1: (2000) 81–103.

Rosenberg, Morris. *Society and the Adolescent Self-Image*. Princeton, NJ: Princeton University Press, 1965.

Rothlisberg, Barbara. "Comparing the Stanford-Binet, Fourth Edition to the WISC-R: A Concurrent Validity Study." *Journal of School Psychology* 25, 2: (1987) 193–196.

Rotter, Julian B. *Generalized Expectancies for Internal versus External Control of Reinforcement*. Washington DC: American Psychological Association, 1966.

Rueda, M. Rosario, Mary K. Rothbart, Bruce D. McCandliss, Lisa Saccomanno, and Michael I. Posner. "Training, maturation, and genetic influences on the development of executive attention." *Proceedings of the National Academy of Sciences* 102, 41: (2005) 14,931–14,936.

Rutter, Michael. "Implications of Resilience Concepts for Scientific Understanding." *Annals of the New York Academy of Sciences* 1094, 1: (2006) 1–12.

Samuel, Douglas B., and Thomas A. Widiger. "A meta-analytic review of the relationships between the five-factor model and DSM-IV-TR personality disorders: A facet level analysis." *Clinical Psychology Review* 28, 8: (2008) 1326–1342.

Savelyev, Peter. "Conscientiousness, Education, and Longevity of High-Ability Individuals." Unpublished manuscript, University of Chicago, Department of Economics, 2011.

Schmidt, Frank L., and John Hunter. "General Mental Ability in the World of Work: Occupational Attainment and Job Performance." *Journal of Personality and Social Psychology* 86, 1: (2004) 162–173.

Segal, Carmit. "Motivation, Test Scores, and Economic Success." Economics working papers, Department of Economics and Business, Universitat Pompeu Fabra, Barcelona, Spain, 2008.

Social and Character Development Research Consortium. "Efficacy of Schoolwide Programs to Promote Social and Character Development and Reduce Problem Behavior in Elementary School Children." Research Report NCER 20112001, National Center for Education Research, Institute of Education Sciences, U.S. Department of Education, 2010.

Stevens, Courtney, Jessica Fanning, Donna Coch, Lisa Sanders, and Helen Neville. "Neural mechanisms of selective auditory attention are enhanced by computerized training: Electrophysiological evidence from language-impaired and typically developing children." *Brain Research* 1205: (2008) 55–69.

Sylva, Kathy. "The Quest for Quality in Curriculum." In *Lasting Differences: The High/Scope Preschool Curriculum Comparison Study through Age 23*, edited by L. J. Schweinhart, and D. P. Weikart, Ypsilanti: High/Scope Press, 1997, 89–93.

Terman, Lewis M., Bird T. Baldwin, Edith Bronson, James C. DeVoss, Florence Fuller, Truman Lee Kelley, Margaret Lima, Helen Marshall, Albert H. Moore, A. S. Raubenheimer, G. M. Ruch, Raymond L. Willoughby, Jennie Benson Wyman, and Dorothy Hazeltine Yates. *Genetic Studies of Genius: Mental and Physical Traits of a Thousand Gifted Children*, volume 1. Stanford University, CA: Stanford University Press, 1925.

Terman, Lewis M., Melita H. Oden, Nancy Bayley, Helen Marshall, Quinn McNemar, and Ellen B. Sullivan. *Genetic Studies of Genius: The Gifted Child Grows Up: Twenty-Five Years' Follow-Up of a Superior Group*, volume 4. Stanford University, CA: Stanford University Press, 1947.

Terman, Lewis Madison, and Maud A. Merrill. *Stanford-Binet Intelligence Scale: Manual for the Third Revision Form L-M*. Boston: Houghton Mifflin, 1960.

Thaler, Richard H. "A Short Course in Behavioral Economics." `http://www.edge.org/3rd_culture/thaler_sendhil08/thaler_sendhil_index.html`. Edge Master Class, Sonoma, CA, July 25-27, 2008., 2008.

No FEAR Act Data

No FEAR Act Notice

PDF

The Notification and Federal Employee Anti-discrimination and Retaliation Act (No FEAR Act) of 2002 increases federal agency accountability for acts of discrimination or reprisal against employees.

The No FEAR Act requires agencies to post on their public websites statistical data relating to equal employment opportunity complaints filed against the respective agencies.

The Federal Reserve Board's public website contains statistical data in accordance with the No FEAR Act.

Information updated as of June 30, 2014

Complaint activity	Comparative data Previous fiscal year data					Fiscal Year 2014 10/2013 - 6/2014
	2009	2010	2011	2012	2013	
Number of complaints filed	1	7	10	12	6	7
Number of complainants	3	9	17	23	16	21
Repeat filers	0	0	0	0	0	0

Return to top

Complaints by basis Note: Complaints can be filed alleging multiple bases. The sum of the bases may not equal total complaints filed	Comparative data Previous fiscal year data					Fiscal Year 2014 10/2013 - 6/2014
	2009	2010	2011	2012	2013	
Race	1	6	10	16	15	17
Color	0	1	2	3	4	5
Religion	0	0	0	2	2	3
Reprisal	1	2	5	11	8	7
Sex	1	5	8	11	11	11
National origin	1	2	3	3	1	2
Equal Pay Act	0	0	0	1	3	4
Age	3	6	8	15	9	9
Disability	0	3	2	5	2	3
Non EEO	0	0	0	0	0	0

Return to top

Complaints by issue	Comparative data Previous fiscal year data	Fiscal Year 2014 10/2013 - 6/2014

Note: Complaints can be filed alleging multiple issues. The sum of the issues may not equal total complaints filed	2009	2010	2011	2012	2013	
Appointment/hire	0	0	0	0	0	1
Assignment of duties	0	2	3	4	4	4
Awards	0	0	0	0	0	0
Conversion to full-time	0	0	0	0	0	0
Disciplinary action						
Demotion	0	0	0	0	0	0
Reprimand	0	0	0	1	2	3
Removal	0	2	2	2	1	3
Suspension	0	0	0	0	0	0
Other	0	0	0	1	1	0
Duty hours	0	1	0	0	0	1
Evaluation appraisal	1	1	2	4	3	4
Examination/test	0	0	0	0	0	0
Harassment						
Nonsexual	0	4	8	11	10	12
Sexual	0	1	2	1	1	0
Medical examination	0	0	0	0	0	0
Pay (including overtime)	0	1	1	1	3	4
Promotion/nonselection	2	5	6	10	10	11
Reassignment						
Denied	0	0	0	0	0	0
Directed	0	0	0	0	0	0
Reasonable accommodation	0	1	1	3	2	3
Reinstatement	0	0	0	0	0	0
Retirement	0	0	0	0	0	0
Termination	0	0	2	2	0	0
Terms/conditions of employment	0	2	2	9	5	6
Time and attendance	0	0	0	0	0	0
Training	0	0	0	0	1	1
Other	0	3	4	1	2	3

Return to top

Processing time	Comparative data Previous fiscal year data					Fiscal Year 2014 10/2013 - 6/2014
	2009	2010	2011	2012	2013	
Complaints pending during fiscal year						
Average number of days in investigation stage	209	68	151	133	228	136
Average number of days in final action stage	28	28	36	53	26	0
Complaints pending during fiscal year where hearing was requested						
Average number of days in investigation stage	209	93	183	148	151	100
Average number of days in final action stage	28	28	36	47	27	0
Complaints pending during fiscal year where hearing was not requested						
Average number of days in investigation stage	0	87	0	93	220	317
Average number of days in final action stage	0	62	0	92	24	0

Return to top

Complaints dismissed by agency	Comparative data Previous fiscal year data					Fiscal Year 2014 10/2013 - 6/2014
	2009	2010	2011	2012	2013	
Total complaints dismissed by agency	0	0	1	0	1	0
Average days pending prior to dismissal	0	0	531	0	27	0

Complaints withdrawn by complainants						
Total complaints withdrawn by complainants	1	0	0	1	1	1

Return to top

Total final actions finding discrimination	Comparative data Previous fiscal year data										Fiscal Year 2014 10/2013 - 6/2014	
	2009		2010		2011		2012		2013			
	#	%	#	%	#	%	#	%	#	%	#	%
Total number findings	**0**		**0**		**0**		**0**		**0**		**0**	
Without hearing	0	0	0	0	0	0	0	0	0	0	0	0
With hearing	0	0	0	0	0	0	0	0	0	0	0	0

Return to top

Findings of discrimination rendered by basis Note: Complaints can be filed alleging multiple bases. The sum of the bases may not equal total complaints and findings	Comparative data Previous fiscal year data										Fiscal Year 2014 10/2013 - 6/2014	
	2009		2010		2011		2012		2013			
	#	%	#	%	#	%	#	%	#	%	#	%
Total number findings	**0**		**0**		**0**		**0**		**0**		**0**	
Race	0	0	0	0	0	0	0	0	0	0	0	0
Color	0	0	0	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0	0	0	0
Reprisal	0	0	0	0	0	0	0	0	0	0	0	0
Sex	0	0	0	0	0	0	0	0	0	0	0	0
National orgin	0	0	0	0	0	0	0	0	0	0	0	0
Equal Pay Act	0	0	0	0	0	0	0	0	0	0	0	0
Age	0	0	0	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0	0	0	0
Non EEO	0	0	0	0	0	0	0	0	0	0	0	0
Findings after hearing	**0**		**0**		**0**		**0**		**0**		**0**	
Race	0	0	0	0	0	0	0	0	0	0	0	0
Color	0	0	0	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0	0	0	0
Reprisal	0	0	0	0	0	0	0	0	0	0	0	0
Sex	0	0	0	0	0	0	0	0	0	0	0	0
National orgin	0	0	0	0	0	0	0	0	0	0	0	0
Equal Pay Act	0	0	0	0	0	0	0	0	0	0	0	0
Age	0	0	0	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0	0	0	0
Non EEO	0	0	0	0	0	0	0	0	0	0	0	0
Findings without hearings	**0**		**0**		**0**		**0**		**0**		**0**	
Race	0	0	0	0	0	0	0	0	0	0	0	0
Color	0	0	0	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0	0	0	0
Reprisal	0	0	0	0	0	0	0	0	0	0	0	0
Sex	0	0	0	0	0	0	0	0	0	0	0	0
National orgin	0	0	0	0	0	0	0	0	0	0	0	0
Equal Pay Act	0	0	0	0	0	0	0	0	0	0	0	0
Age	0	0	0	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0	0	0	0
Non EEO	0	0	0	0	0	0	0	0	0	0	0	0

Return to top

Findings of discrimination rendered,	Comparative data	Fiscal Year

by issue	Previous fiscal year data										2014 10/2013 - 6/2014	
	2009		2010		2011		2012		2013			
	#	%	#	%	#	%	#	%	#	%	#	%
Total number findings	**0**		**0**		**0**		**0**		**0**		**0**	
Appointment/hire	0	0	0	0	0	0	0	0	0	0	0	0
Assignment of duties	0	0	0	0	0	0	0	0	0	0	0	0
Awards	0	0	0	0	0	0	0	0	0	0	0	0
Conversion to full-time	0	0	0	0	0	0	0	0	0	0	0	0
Disciplinary action	0	0	0	0	0	0	0	0	0	0	0	0
Demotion	0	0	0	0	0	0	0	0	0	0	0	0
Reprimand	0	0	0	0	0	0	0	0	0	0	0	0
Suspension	0	0	0	0	0	0	0	0	0	0	0	0
Removal	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0
Duty hours	0	0	0	0	0	0	0	0	0	0	0	0
Evaluation appraisal	0	0	0	0	0	0	0	0	0	0	0	0
Examination/test	0	0	0	0	0	0	0	0	0	0	0	0
Harassment	0	0	0	0	0	0	0	0	0	0	0	0
Nonsexual	0	0	0	0	0	0	0	0	0	0	0	0
Sexual	0	0	0	0	0	0	0	0	0	0	0	0
Medical examination	0	0	0	0	0	0	0	0	0	0	0	0
Pay (including overtime)	0	0	0	0	0	0	0	0	0	0	0	0
Promotion/nonselection	0	0	0	0	0	0	0	0	0	0	0	0
Reassignment	0	0	0	0	0	0	0	0	0	0	0	0
Denied	0	0	0	0	0	0	0	0	0	0	0	0
Directed	0	0	0	0	0	0	0	0	0	0	0	0
Reasonable accommodation	0	0	0	0	0	0	0	0	0	0	0	0
Reinstatement	0	0	0	0	0	0	0	0	0	0	0	0
Retirement	0	0	0	0	0	0	0	0	0	0	0	0
Termination	0	0	0	0	0	0	0	0	0	0	0	0
Terms/conditions of employment	0	0	0	0	0	0	0	0	0	0	0	0
Time and attendance	0	0	0	0	0	0	0	0	0	0	0	0
Training	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0
Findings after hearings	**0**		**0**		**0**		**0**		**0**		**0**	
Appointment/hire	0	0	0	0	0	0	0	0	0	0	0	0
Assignment of duties	0	0	0	0	0	0	0	0	0	0	0	0
Awards	0	0	0	0	0	0	0	0	0	0	0	0
Conversion to full-time	0	0	0	0	0	0	0	0	0	0	0	0
Disciplinary action	0	0	0	0	0	0	0	0	0	0	0	0
Demotion	0	0	0	0	0	0	0	0	0	0	0	0
Reprimand	0	0	0	0	0	0	0	0	0	0	0	0
Suspension	0	0	0	0	0	0	0	0	0	0	0	0
Removal	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0
Duty hours	0	0	0	0	0	0	0	0	0	0	0	0
Evaluation appraisal	0	0	0	0	0	0	0	0	0	0	0	0
Examination/test	0	0	0	0	0	0	0	0	0	0	0	0
Harassment	0	0	0	0	0	0	0	0	0	0	0	0
Nonsexual	0	0	0	0	0	0	0	0	0	0	0	0
Sexual	0	0	0	0	0	0	0	0	0	0	0	0
Medical examination	0	0	0	0	0	0	0	0	0	0	0	0
Pay (including overtime)	0	0	0	0	0	0	0	0	0	0	0	0
Promotion/nonselection	0	0	0	0	0	0	0	0	0	0	0	0
Reassignment	0	0	0	0	0	0	0	0	0	0	0	0
Denied	0	0	0	0	0	0	0	0	0	0	0	0

Directed	0	0	0	0	0	0	0	0	0	0	0	0
Reasonable accommodation	0	0	0	0	0	0	0	0	0	0	0	0
Reinstatement	0	0	0	0	0	0	0	0	0	0	0	0
Retirement	0	0	0	0	0	0	0	0	0	0	0	0
Termination	0	0	0	0	0	0	0	0	0	0	0	0
Terms/conditions of employment	0	0	0	0	0	0	0	0	0	0	0	0
Time and attendance	0	0	0	0	0	0	0	0	0	0	0	0
Training	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0
Findings without hearing	**0**		**0**		**0**		**0**		**0**		**0**	
Appointment/hire	0	0	0	0	0	0	0	0	0	0	0	0
Assignment of duties	0	0	0	0	0	0	0	0	0	0	0	0
Awards	0	0	0	0	0	0	0	0	0	0	0	0
Conversion to full-time	0	0	0	0	0	0	0	0	0	0	0	0
Disciplinary action	0	0	0	0	0	0	0	0	0	0	0	0
Demotion	0	0	0	0	0	0	0	0	0	0	0	0
Reprimand	0	0	0	0	0	0	0	0	0	0	0	0
Suspension	0	0	0	0	0	0	0	0	0	0	0	0
Removal	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0
Duty hours	0	0	0	0	0	0	0	0	0	0	0	0
Evaluation appraisal	0	0	0	0	0	0	0	0	0	0	0	0
Examination/test	0	0	0	0	0	0	0	0	0	0	0	0
Harassment	0	0	0	0	0	0	0	0	0	0	0	0
Nonsexual	0	0	0	0	0	0	0	0	0	0	0	0
Sexual	0	0	0	0	0	0	0	0	0	0	0	0
Medical examination	0	0	0	0	0	0	0	0	0	0	0	0
Pay (including overtime)	0	0	0	0	0	0	0	0	0	0	0	0
Promotion/nonselection	0	0	0	0	0	0	0	0	0	0	0	0
Reassignment	0	0	0	0	0	0	0	0	0	0	0	0
Denied	0	0	0	0	0	0	0	0	0	0	0	0
Directed	0	0	0	0	0	0	0	0	0	0	0	0
Reasonable accommodation	0	0	0	0	0	0	0	0	0	0	0	0
Reinstatement	0	0	0	0	0	0	0	0	0	0	0	0
Retirement	0	0	0	0	0	0	0	0	0	0	0	0
Termination	0	0	0	0	0	0	0	0	0	0	0	0
Terms/conditions of employment	0	0	0	0	0	0	0	0	0	0	0	0
Time and attendance	0	0	0	0	0	0	0	0	0	0	0	0
Training	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0

Return to top

Pending complaints filed in previous fiscal years, by status	**Comparative data Previous fiscal year data**					**Fiscal Year 2014 10/2013 - 6/2014**
	2009	**2010**	**2011**	**2012**	**2013**	
Total complaints from previous fiscal years	2	2	10	10	14	15
Number of complaints pending						
Investigation	0	0	0	0	4	3
Hearing	1	1	6	4	7	9
Final action	0	0	0	0	0	0
Appeal with EEOC Office of Federal Operations	1	1	1	0	2	2
Class Certification with EEOC Office of Federal Operations	0	0	1	4	0	0
District Court	0	0	2	2	1	1

Return to top

Complaint investigations	Comparative data Previous fiscal year data					Fiscal Year 2014 10/2013 - 6/2014
	2009	2010	2011	2012	2013	
Pending complaints where investigations exceed required time frames	2	3	0	2	8	7

Return to top

For further information, please contact the Diversity & Inclusion Director.

Diversity & Inclusion Director, Stop 156
Board of Governors of the Federal Reserve System
20th and Constitution Avenue, N.W.
Washington, D.C. 20551

Last update: September 18, 2014

Employer Information Report EEO-1

Current | Archive: 2011 GO

Federal Reserve Board, 2012 Employer Information Report

Occupational Categories	Total Employees			Race/Ethnicity													
				Hispanic or Latino		Non- Hispanic or Latino: White		Black or African American		Asian		Native Hawaiian or Other Pacific Islander		American Indian or Alaska Native		Two or More Races	
	All	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female
1.1 Exec. Sr. Level Managers, Governors, Officers, FR-29 & FR-28																	
By total	351	211	140	4	6	176	101	19	21	11	10	1	1	0	0	0	1
By percent	100.00%	60.11%	39.89%	1.14%	1.71%	50.14%	28.77%	5.41%	5.98%	3.13%	2.85%	0.28%	0.28%	0.00%	0.00%	0.00%	0.28%
1.2 1st/Mid. Level																	
By total	78	27	51	0	1	15	30	8	19	4	1	0	0	0	0	0	0
By percent	100.00%	34.62%	65.38%	0.00%	1.28%	19.23%	38.46%	10.26%	24.36%	5.13%	1.28%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Officials and Managers Total																	
By total	429	238	191	4	7	191	131	27	40	15	11	1	1	0	0	0	1
By percent	100.00%	55.48%	44.52%	0.93%	1.63%	80.25%	30.54%	6.29%	9.32%	3.50%	2.56%	0.23%	0.23%	0.00%	0.00%	0.00%	0.23%
2. Professionals																	
By total	1,562	839	723	39	41	559	355	86	186	133	126	17	15	1	0	4	0
By percent	100.00%	53.71%	46.29%	2.50%	2.62%	66.63%	22.73%	5.51%	11.91%	8.51%	8.07%	1.09%	0.96%	0.06%	0.00%	0.26%	0.00%
3. Technicians																	
By total	6	2	4	0	0	0	2	2	2	0	0	0	0	0	0	0	0
By percent	100.00%	33.33%	66.67%	0.00%	0.00%	0.00%	33.33%	33.33%	33.33%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
4. Sales Workers																	
By total	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
By percent	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
5. Admin. Support Workers																	
By total	145	26	119	1	5	6	15	18	93	1	4	0	0	0	2	0	0
By percent	100.00%	17.93%	82.07%	0.69%	3.45%	4.14%	10.34%	12.41%	64.14%	0.69%	2.76%	0.00%	0.00%	0.00%	1.38%	0.00%	0.00%
6. Craft Workers																	
By total	42	41	1	0	0	23	0	13	1	4	0	1	0	0	0	0	0
By percent	100.00%	97.62%	2.38%	0.00%	0.00%	54.76%	0.00%	30.95%	2.38%	9.52%	0.00%	2.38%	0.00%	0.00%	0.00%	0.00%	0.00%
7. Operatives																	
By total	11	11	0	0	0	0	0	11	0	0	0	0	0	0	0	0	0
By percent	100.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
8. Laborers and Helpers																	
By total	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
By percent	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
9. Service Workers																	
By total	192	158	34	9	0	53	4	93	28	3	1	0	1	0	0	0	0
By percent	100.00%	82.29%	17.71%	4.69%	0.00%	27.60%	2.08%	48.44%	14.58%	1.56%	0.52%	0.00%	0.52%	0.00%	0.00%	0.00%	0.00%
Total Workforce																	
By total	2,387	1,315	1,072	53	53	832	507	250	350	156	142	19	17	1	2	4	1
By percent	100.00%	55.09%	44.91%	2.22%	2.22%	34.86%	21.24%	10.47%	14.66%	6.54%	5.95%	0.80%	0.71%	0.04%	0.08%	0.17%	0.04%

Last update: August 2, 2013

Press Release

Release Date: November 4, 2010

For immediate release

The Federal Reserve Board on Thursday established the Office of Financial Stability Policy and Research and appointed Board economist J. Nellie Liang as its director.

The office will bring together economists, banking supervisors, markets experts, and others in the Federal Reserve who will be dedicated to supporting the Board's financial stability responsibilities. The office will develop and coordinate staff efforts to identify and analyze potential risks to the financial system and the broader economy, including through the monitoring of asset prices, leverage, financial flows, and other market risk indicators; follow developments at key institutions; and analyze policies to promote financial stability. It will also support the supervision of large financial institutions and the Board's participation on the Financial Stability Oversight Council.

"The Office of Financial Stability Policy and Research brings together a skilled group of people with a wide range of expertise to focus solely on financial stability," Federal Reserve Chairman Ben S. Bernanke said. "The financial stability team will play an important role in implementing the Dodd-Frank Wall Street Reform and Consumer Protection Act, in our oversight of systemically important financial institutions, and in our overall surveillance of the financial markets and the economy. I am pleased that such a strong economist and leader as Nellie is leading this group."

Liang joined the Board in 1986, acting most recently as a senior associate director in the Division of Research and Statistics. In that role, she has led a group of economists focused on the intersection of economics and finance, including oversight of capital markets, financial institutions, consumer finance, and financial flows. Liang was a key participant in crafting the Federal Reserve's response to the financial crisis and helped lead the Supervisory Capital Assessment Program, or bank stress tests, which helped increase public confidence in the banking system in 2009. Liang has a Ph.D. in economics from the University of Maryland and an undergraduate degree in economics from the University of Notre Dame.

2010 Other Announcements

OFFICE OF INSPECTOR GENERAL

Audit Report 2015-MO-B-006

The Board Can Enhance Its Diversity and Inclusion Efforts

March 31, 2015

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU

Report Contributors

Anna Saez, OIG Manager
Kimberly Perteet, Project Lead and Senior Auditor
Victor Calderon, Senior Forensic Auditor
Sopeany Keo, Senior Auditor
Brian Murphy, Auditor
Sean Newman, Auditor
Timothy Rogers, Senior OIG Manager for Management and Operations
Melissa Heist, Associate Inspector General for Audits and Evaluations

Abbreviations

ACS	American Community Survey
Board	Board of Governors of the Federal Reserve System
C.F.R.	*Code of Federal Regulations*
COSO	Committee of Sponsoring Organizations of the Treadway Commission
Dodd-Frank Act	Dodd-Frank Wall Street Reform and Consumer Protection Act
EEO	equal employment opportunity
EEOC	U.S. Equal Employment Opportunity Commission
ER	Employee Relations
FY	fiscal year
GAO	U.S. Government Accountability Office
HR	Human Resources
MD-715	*Management Directive 715*
No FEAR Act	Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002
OD&I	Office of Diversity and Inclusion
OD&L	Organizational Development and Learning
OIG	Office of Inspector General
OMWI	Office of Minority and Women Inclusion
OPM	U.S. Office of Personnel Management
U.S.C.	*United States Code*

Executive Summary:

The Board Can Enhance Its Diversity and Inclusion Efforts

2015-MO-B-006 March 31, 2015

Purpose

The Office of Inspector General conducted this audit in response to a congressional request for information on the Board of Governors of the Federal Reserve System's (Board) activities related to diversity and inclusion. Our objective was to assess the Board's human resources–related operations and other efforts to provide for equal employment opportunities, including equal opportunity for minorities and women to obtain senior management positions, and increase racial, ethnic, and gender diversity in the workforce.

Background

Section 10 of the Federal Reserve Act (12 U.S.C. § 244) grants the Board broad authority and independence over matters of employment. As such, the Board is generally not subject to the personnel provisions of title 5 of the *United States Code*, including those relating to recruiting and hiring, performance management, promotions, and employee satisfaction surveys. However, as part of its employment rules, the Board has adopted equal employment opportunity (EEO) provisions that prohibit employment discrimination, including provisions of the No FEAR Act.

The Dodd-Frank Wall Street Reform and Consumer Protection Act required the Board to establish an Office of Minority and Women Inclusion that is responsible for all agency matters relating to diversity in management.

Findings

The Board has established diversity and inclusion practices that are embedded in its longstanding EEO programs. Recent activities include adopting a more standardized process for recruiting officers, developing a formal agency-wide succession planning program to help identify a diverse pool of candidates for senior management positions, and conducting an agency-wide employee survey.

We identified areas of the Board's diversity and inclusion efforts that can be enhanced. First, the Board can enhance its efforts to track and analyze certain types of workforce data that can be used to identify diversity and inclusion trends. Second, the Office of Diversity and Inclusion can increase its interaction with all Board divisions and provide diversity and inclusion and EEO training on a regular basis. Third, the Board should formalize standards for equal employment opportunity and the racial, ethnic, and gender diversity of the workforce to fully comply with section 342 of the Dodd-Frank Wall Street Reform and Consumer Protection Act. Fourth, the Board can further enhance its diversity and inclusion goals and objectives by finalizing and implementing its diversity strategic plan.

We acknowledge that initiatives and activities that are beyond the scope of our review also contribute to enhancing diversity and inclusion. Therefore, the Board's ability to attract, develop, and retain a diverse and inclusive workforce is affected by other factors not specifically identified in our report.

Recommendations

Our report contains recommendations designed to enhance and promote diversity and inclusion at the Board. In its response to our draft report, the Board concurs with our recommendations and outlines planned, ongoing, and completed activities. The Board has taken steps to improve the collection of applicant demographic data, provide non-EEO statistics, and finalize the diversity and inclusion strategic plan. In addition, the Board plans to enhance certain functions within the Office of Diversity and Inclusion.

Summary of Recommendations, OIG Report No. 2015-MO-B-006

Rec. no.	Report page no.	Recommendation	Responsible office
1	23	Develop and implement an alternative method for collecting the demographic data of economist and research assistant applicants to improve the response rate.	Divisions that recruit economists and research assistants
2	24	Ensure that the demographic data for all internal and external officer applicants are maintained in the Board's centralized applicant database.	Management Division
3	30	Consider conducting annual analyses of the distribution of employee performance ratings to identify whether patterns exist that may indicate unfair or unequal treatment. If the analyses reveal patterns that may indicate unfair or unequal treatment, determine whether any actions are necessary.	Management Division
4	41	Ensure that aggregate non–equal employment opportunity case statistics are provided to all Division Directors and that division-specific statistics are provided to the respective Division Director.	Management Division
5	51	Finalize and implement the Board's diversity and inclusion strategic plan and ensure that a. the plan incorporates the agency's overall diversity and inclusion objectives. b. key elements of the plan are included in the Board's 2016–2019 agency strategic plan.	Office of Diversity and Inclusion
6	52	Formalize the standards the Office of Diversity and Inclusion relies on for equal employment opportunity and the racial, ethnic, and gender diversity of the workforce and the senior management of the agency.	Office of Diversity and Inclusion
7	54	Ensure that No FEAR Act training a. is offered on a regular basis. b. is tailored to the Board and includes equal employment opportunity and diversity and inclusion topics in accordance with the Board's *No FEAR Act Written Training Plan*. c. is evaluated for effectiveness and that any improvements identified are incorporated into the training as needed. d. attendance records are retained.	Office of Diversity and Inclusion
8	56	Document the roles and responsibilities of the Office of Diversity and Inclusion and distribute them to all Board divisions.	Office of Diversity and Inclusion
9	56	Partner with divisions to cooperatively develop strategies and initiatives that will help advance diversity and inclusion throughout the Board.	Office of Diversity and Inclusion
10	56	Work with divisions to finalize and implement the quarterly reporting tool and establish a schedule to communicate the results for each division to the respective Division Director. The quarterly reporting tool should include diversity and inclusion activities for each division with clear objectives and corresponding measures.	Office of Diversity and Inclusion

Rec. no.	Report page no.	Recommendation	Responsible office
11	57	Strengthen internal controls for reporting *Management Directive 715* data, to include a. documenting the methodology for extracting and filtering the appropriate data. b. verifying the accuracy and completeness of the data in the *Management Directive 715* report prior to submission.	Office of Diversity and Inclusion and Management Division

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

March 31, 2015

MEMORANDUM

TO: Distribution List

FROM: Melissa Heist
Associate Inspector General for Audits and Evaluations

SUBJECT: OIG Report No. 2015-MO-B-006: *The Board Can Enhance Its Diversity and Inclusion Efforts*

The Office of Inspector General has completed its final report on the subject audit. We conducted this audit in response to a congressional request for information on the Board of Governors of the Federal Reserve System's (Board) activities related to diversity and inclusion. Our objective was to assess the Board's human resources–related operations and other efforts to provide for equal employment opportunities, including equal opportunity for minorities and women to obtain senior management positions, and increase racial, ethnic, and gender diversity in the workforce.

Our report contains recommendations designed to improve the monitoring and promotion of diversity and inclusion at the Board, as well as strengthen related controls. In the Board's response to our draft report, the Board concurs with our recommendations and indicated progress in addressing the recommendations. We have included the Board's response as appendix I in our report.

We appreciate the cooperation that we received from your offices. In its final form, this report will be added to our public website and will be summarized in our next *Semiannual Report to Congress.* Please contact me if you would like to discuss this report or any related issues.

cc: Michell Clark, Director of the Management Division
Dave Harmon, Chief Human Capital Officer and Deputy Director, Management Division
Sheila Clark, Program Director, Office of Diversity and Inclusion
Lillian Shewmaker, Chief of Administration and Special Projects, Division of Research and Statistics
Scott G. Alvarez, General Counsel
William Mitchell, Chief Financial Officer and Director, Division of Financial Management
J. Anthony Ogden, Deputy Inspector General

Distribution:
Donald Hammond, Chief Operating Officer, Office of the Chief Operating Officer
Steven Kamin, Director, Division of International Finance
Thomas Laubach, Director, Division of Monetary Affairs
Nellie Liang, Director, Office of Financial Stability Policy and Research
David Wilcox, Director, Division of Research and Statistics

Contents

Introduction

Objective

The Office of Inspector General (OIG) conducted an audit in response to a March 24, 2014, congressional request for information on the Board of Governors of the Federal Reserve System's (Board) activities related to diversity and inclusion.[1] We received a similar congressional request for information on activities related to diversity and inclusion at the Consumer Financial Protection Bureau, as did the OIGs of five other federal financial regulatory agencies.[2] We coordinated with the other OIGs to develop a comparable objective and scope to address the congressional requests.

Our resultant objective was to assess the Board's human resources–related functions and other efforts to provide for equal employment opportunities, including equal opportunity for minorities and women to obtain senior management positions, and increase racial, ethnic, and gender diversity in the workforce. To answer our objective, we

- reviewed relevant agency personnel operations, policies, and procedures, (e.g., policies related to performance management and hiring), to determine whether adequate controls are established to prevent and detect bias or discrimination
- analyzed information related to demographic statistics for minority and women employees (e.g., performance management, promotions, and representation at all levels of the agency); informal and formal equal employment opportunity (EEO) complaint statistics; and employee satisfaction survey results to determine whether this information suggests disparities in gender, race/ethnicity, or age
- assessed the Board's efforts to respond to complaints, employee satisfaction survey results, or other potential indications of bias or discrimination and to increase diversity throughout the agency
- evaluated the Office of Minority and Women Inclusion's (OMWI) role and involvement in monitoring the impact of the Board's personnel policies on minorities and women, as well as monitoring the Board's efforts to increase diversity in senior management positions
- identified factors that may impact the Board's ability to increase diversity in senior management positions

1. The congressional request letter is in appendix A.

2. The OIGs that received similar requests are those for the U.S. Department of the Treasury's Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Federal Housing Finance Agency, the National Credit Union Administration, and the U.S. Securities and Exchange Commission.

The scope of our audit included the Board's human resources–related functions affecting diversity and inclusion from 2011 through 2013.[3] We also report on relevant management actions that were undertaken in 2014.

We acknowledge that diversity and inclusion are much broader than the areas covered in our report, and that initiatives and activities that are beyond the scope of our review also contribute to enhancing diversity and inclusion. The U.S. Office of Personnel Management (OPM) defines workforce diversity and inclusion, respectively, as follows:

> [Workforce diversity is] a collection of individual attributes that together help agencies pursue organizational objectives efficiently and effectively. These include, but are not limited to, characteristics such as national origin, language, race, color, disability, ethnicity, gender, age, religion, sexual orientation, gender identity, socioeconomic status, veteran status, and family structures. The concept also encompasses differences among people concerning where they are from and where they have lived and their differences of thought and life experiences.[4]
>
> [Inclusion is] a culture that connects each employee to the organization; encourages collaboration, flexibility, and fairness; and leverages diversity throughout the organization so that all individuals are able to participate and contribute to their full potential.[5]

For the purposes of our review, we focused on aspects of diversity and inclusion as they specifically relate to gender, race/ethnicity, and age. These three aspects of diversity were emphasized as being of particular interest in our discussions with congressional staff. The race/ethnicity categories discussed in this report follow those prescribed by the U.S. Equal Employment Opportunity Commission (EEOC) as defined in its *Equal Employment Opportunity Standard Form 100, Rev. January 2006, Employer Information Report EEO-1 Instruction Booklet*. These categories include White (Not Hispanic or Latino), Black or African American (Not Hispanic or Latino), Hispanic or Latino, and Asian (Not Hispanic or Latino), among others.[6] Details on our scope and methodology are in appendix B.

The U.S. Government Accountability Office (GAO), in its *Diversity Management: Expert-Identified Leading Practices and Agency Examples* report, emphasized that a high-performance organization relies on a dynamic workforce with the requisite talents, multidisciplinary knowledge, and up-to-date skills to ensure that it is equipped to accomplish its mission and

3. The Board generally operates on a calendar-year basis; however its performance management process is on a fiscal-year basis.

4. U.S. Office of Personnel Management, *Government-Wide Diversity and Inclusion Strategic Plan 2011*.

5. U.S. Office of Personnel Management, *Government-Wide Diversity and Inclusion Strategic Plan 2011*.

6. For the purposes of this report, we grouped the following race/ethnicity categories as *Other* due to the small number of individuals typically represented in each of these categories: (1) Native Hawaiian or Other Pacific Islander (Not Hispanic or Latino), (2) American Indian or Alaska Native (Not Hispanic or Latino), (3) Two or More Races/Ethnicities (Not Hispanic or Latino), and (4) Not Specified (i.e., individuals who chose not to disclose demographic data).

achieve its goals.[7] Further, the GAO report states that the approach a high-performance organization takes toward its workforce is inclusive and draws on the strengths of employees at all levels and of all backgrounds. Diversity management creates and maintains a positive work environment where the similarities and differences of individuals are valued, so that all can reach their potential and maximize their contributions to an organization's strategic goals and objectives.

Background

The Federal Reserve Act established the Board of Governors of the Federal Reserve System.[8] The Board is composed of seven Governors appointed by the President of the United States, with the advice and consent of the United States Senate.[9] The Board's mission is to foster the stability, integrity, and efficiency of the nation's monetary, financial, and payment systems. The Board has 14 divisions and an OIG.

Section 10 of the Federal Reserve Act[10] grants the Board broad authority over matters of employment. Specifically, section 10 states that Board employment will be governed "solely" by the provisions of the Federal Reserve Act and rules and regulations of the Board that are not inconsistent with the act. As such, the Board is generally not subject to the personnel provisions of title 5 of the *United States Code*, including those relating to recruiting and hiring, performance management, promotions, and employee satisfaction surveys. However, as part of its employment rules, the Board has adopted EEO laws that prohibit discrimination against an individual on the basis of race, color, religion, sex, national origin, age, disability, or genetic information, and the Board promotes the full realization of equal employment opportunity through a continuing affirmative program. The Board also prohibits discrimination on the basis of any application, membership, or service in the uniformed services. In addition, as a matter of policy and although it is not required by law, the Board prohibits discrimination in employment on the basis of sexual orientation. The Board's employment rules include the provisions of the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (No FEAR Act) that require agencies to report EEO complaint information and to provide training at least every two years to their employees, including managers, regarding the rights and remedies available under the employment discrimination protection laws.

Guidance and Best Practices Related to Diversity and Inclusion

This section highlights guidance and best practices related to diversity and inclusion, including EEOC management directives, GAO's *Standards for Internal Control in the Federal Government*, and diversity management leading practices.

7. U.S. Government Accountability Office, *Diversity Management: Expert-Identified Leading Practices and Agency Examples*, GAO-05-90, January 14, 2005.

8. The Federal Reserve System comprises the Board, the 12 regional Federal Reserve Banks, and the Federal Open Market Committee.

9. 12 U.S.C. § 241.

10. 12 U.S.C. § 244.

The EEOC is responsible for enforcing federal laws that prohibit discrimination against a job applicant or an employee because of the person's race/ethnicity, color, religion, sex, national origin, age (40 or older), disability, or genetic information. Federal law also prohibits discrimination against a person because the person complained about discrimination, filed a charge of discrimination, or participated in an employment discrimination investigation or lawsuit. The EEOC provides leadership and guidance to federal agencies on all aspects of the federal government's EEO program. The EEOC ensures federal agency and department compliance with EEOC regulations, provides technical assistance to federal agencies concerning EEO complaint adjudication, monitors and evaluates federal agencies' affirmative employment programs, develops and distributes federal-sector educational materials and conducts training for stakeholders, and adjudicates appeals from administrative decisions made by federal agencies on EEO complaints.

The EEOC's *Management Directive 715* (MD-715) provides federal agencies policy guidance and standards for establishing and maintaining effective EEO programs. The Board follows the requirements of the MD-715 and annually attests to its commitment to equal opportunity in aspects of employment and fostering diversity and inclusion in the workplace.[11] The MD-715 provides instructions that require agencies, among other things, to report demographic data on their workforce on an annual basis. The MD-715 also provides guidance on establishing and maintaining effective programs of equal employment. The MD-715 defines the following six essential elements of a model EEO program:

- demonstrated commitment from agency leadership
- integration of equal employment opportunity into the agency's strategic mission
- management and program accountability
- proactive prevention of unlawful discrimination
- efficiency (e.g., efficient, fair, and impartial complaint resolution process)
- responsiveness and legal compliance[12]

Establishing appropriate internal controls helps agencies improve organizational effectiveness and accountability. In the context of diversity and inclusion at the Board, internal controls may assist the agency in preventing and detecting bias or discrimination in its human resources–related functions and in ensuring the accurate reporting of diversity information. GAO's *Standards for Internal Control in the Federal Government* contains internal control standards for federal agencies to follow; these standards incorporate elements of the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) internal control framework. COSO's internal control framework is widely used and recognized as a leading framework for designing, implementing, and evaluating the effectiveness of internal control. Similar controls are also prescribed for the accurate reporting of information. The National Institute of Standards and Technology's Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, outlines mandatory information security controls for federal information systems, including data output reconciliation and error correction.

GAO has reported leading practices to guide organizations in diversity management. These practices are intended to help agencies create and maintain a positive work environment where

11. In May 2014, the Board published *The EEO Complaint System and How It Works*, which contains Chair Janet Yellen's attestation to the Board's commitment to providing equal employment to all persons.

12. Equal Employment Opportunity Commission, *Management Directive 715*, October 1, 2003.

the similarities and differences of individuals are valued so that all can reach their potential and maximize their contributions to an organization's strategic goals and objectives. GAO issued *Diversity Management: Expert-Identified Leading Practices and Agency Examples* in response to a congressional request to report on the federal government's performance in managing its diverse workforce. In its report, GAO identifies the following nine leading diversity management practices:

Top leadership commitment—A vision of diversity demonstrated and communicated throughout an organization by top-level management.

Diversity as part of an organization's strategic plan—A diversity strategy and plan that are developed and aligned with the organization's strategic plan.

Diversity linked to performance—The understanding that a more diverse and inclusive work environment can yield greater productivity and help improve individual and organizational performance.

Measurement—A set of quantitative and qualitative measures of the impact of various aspects of an overall diversity program.

Accountability—The means to ensure that leaders are responsible for diversity by linking their performance assessment and compensation to the progress of diversity initiatives.

Succession planning—An ongoing, strategic process for identifying and developing a diverse pool of talent for an organization's potential future leaders.

Recruitment—The process of attracting a supply of qualified, diverse applicants for employment.

Employee involvement—The contribution of employees in driving diversity throughout an organization.

Diversity training—Organizational efforts to inform and educate management and staff about diversity.[13]

The GAO report states that the diversity management experts it spoke with or whose publications it reviewed generally agreed that organizations should consider a combination of these nine leading practices when developing and implementing diversity management.

The Board's Workforce

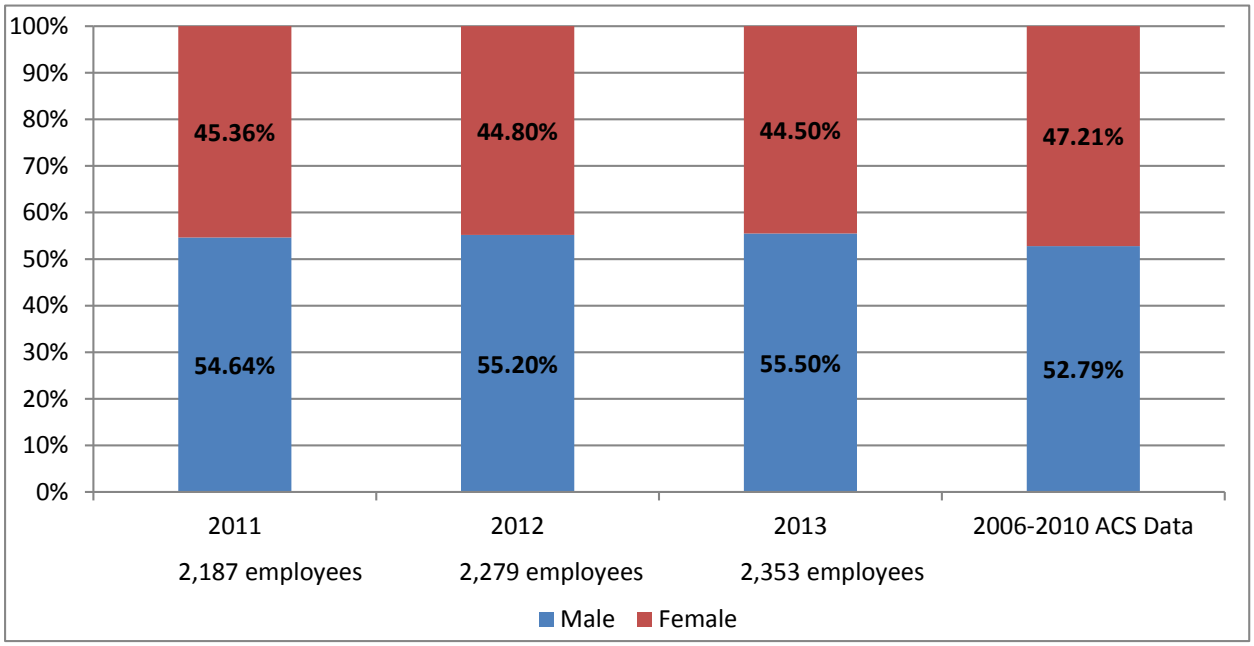
In this section, we provide information about the Board's workforce composition by sex, race/ethnicity, and age. This information provides context for the remainder of the report.

13. U.S. Government Accountability Office, *Diversity Management: Expert-Identified Leading Practices and Agency Examples*, GAO-05-90, January 14, 2005.

Composition of the Workforce

The Board's total workforce was 2,187 in 2011, 2,279 in 2012, and 2,353 in 2013.[14] During this period, as shown in figure 1, female employees accounted for approximately 45 percent of the Board's workforce. According to the U.S. Census Bureau, females accounted for approximately 47 percent of the general workforce, as represented by the most recent five-year American Community Survey (ACS) data.[15]

Figure 1: Permanent Board Employees, 2011–2013, and ACS Data,[a] by Sex



Source: OIG analysis of Board-provided data and the U.S. Census Bureau's ACS data.

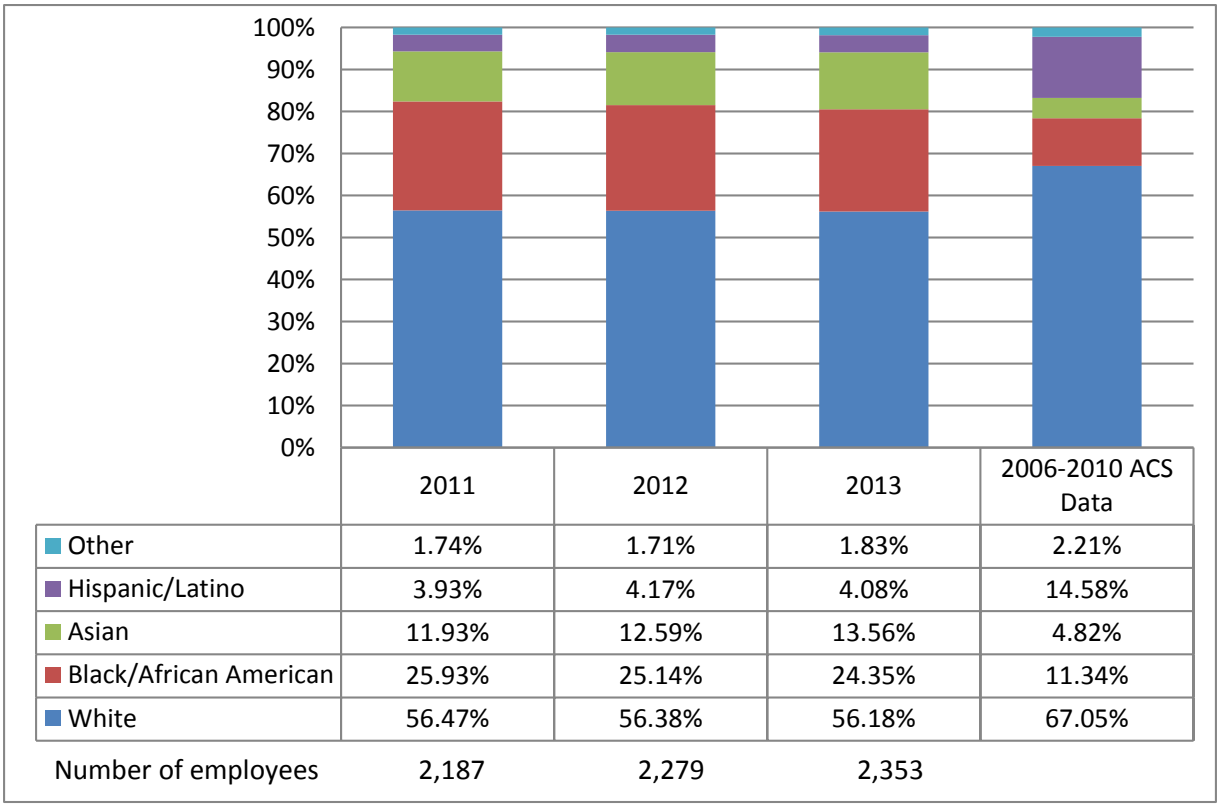
[a]These data are compiled through the survey, which randomly samples around 3.5 million addresses and produces statistics for five-year time periods.

14. The OIG was excluded from this audit to maintain its independence. In addition, the total workforce numbers do not include temporary employees or interns.

15. The U.S. Census Bureau entered into a reimbursable agreement with a consortium of four federal agencies—the EEOC, the U.S. Department of Justice, the Office of Federal Contract Compliance Programs at the U.S. Department of Labor, and OPM—to create a custom tabulation identified as the EEO Tabulation 2006–2010 and referred to as the five-year ACS data. The five-year ACS data serve as the primary benchmark for comparing the race, ethnicity, and sex composition of an organization's workforce with that of the analogous external labor market within a specified geography and job category.

The non-White workforce population averaged 44 percent for all three years under review (figure 2). The Board's workforce is more racially diverse than the workforce represented in the ACS data, which reported a 33 percent non-White workforce for 2006–2010.[16]

Figure 2: Permanent Board Employees, 2011–2013, and ACS Data,[a] by Race/Ethnicity[b]



	2011	2012	2013	2006-2010 ACS Data
Other	1.74%	1.71%	1.83%	2.21%
Hispanic/Latino	3.93%	4.17%	4.08%	14.58%
Asian	11.93%	12.59%	13.56%	4.82%
Black/African American	25.93%	25.14%	24.35%	11.34%
White	56.47%	56.38%	56.18%	67.05%
Number of employees	2,187	2,279	2,353	

Source: OIG analysis of Board-provided data and the Census Bureau's ACS data.

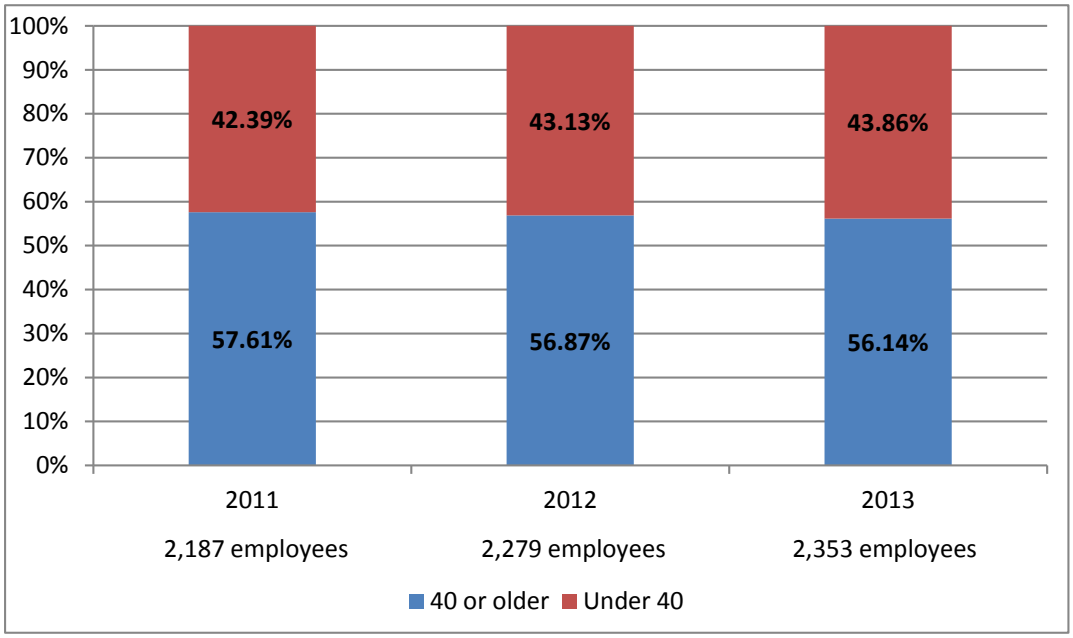
[a]These data are compiled through the survey, which randomly samples around 3.5 million addresses and produces statistics for five-year time periods.

[b]*Other* includes (1) Native Hawaiian or Other Pacific Islander (Not Hispanic or Latino), (2) American Indian or Alaska Native (Not Hispanic or Latino), (3) Two or More Races/Ethnicities (Not Hispanic or Latino), and (4) Not Specified (i.e., individuals who chose not to disclose demographic data).

16. The race/ethnicity categories discussed in this report are the same as those prescribed by the EEOC in its *Equal Employment Opportunity Standard Form 100, Rev. January 2006, Employer Information Report EEO-1 Instruction Booklet*.

To assess age diversity, we looked at two age groups: those under 40 years of age and those 40 years of age or older. We noted that employees 40 years of age or older accounted for approximately 56 to 58 percent of the Board's workforce in 2011, 2012, and 2013 (figure 3). There are no comparable ACS data on age demographics.

Figure 3: Permanent Board Employees, 2011–2013, by Age



Source: OIG analysis of Board-provided data.

Demographics by Pay Grade Category

The Board's pay structure has 22 pay grades.[17] For wage employees, there are seven pay grades, or WE levels, ranging from 41 (lowest) to 47 (highest). The Board also has 14 professional pay grades, or FR levels, ranging from 16 (lowest) to 29 (highest).[18] For executive-level Board staff (known as official staff or officers), the Board has one pay grade, 00, regardless of position title. For the purpose of our analysis, we grouped the wage, professional, and officer grades into the following three categories:

- senior managers and officers (FR-29 and 00)
- mid-level professionals (FR-26 to FR-28)[19]
- all other professional employees and all wage employees (FR-16 to FR-25 and WE-41 to WE-47)

17. The Board's salary structure does not map to the federal government's General Schedule pay structure.

18. In January 2014, the Board added the FR-30 pay grade. This pay grade was not included in our analysis. As of March 2015, there were no incumbents at this pay grade.

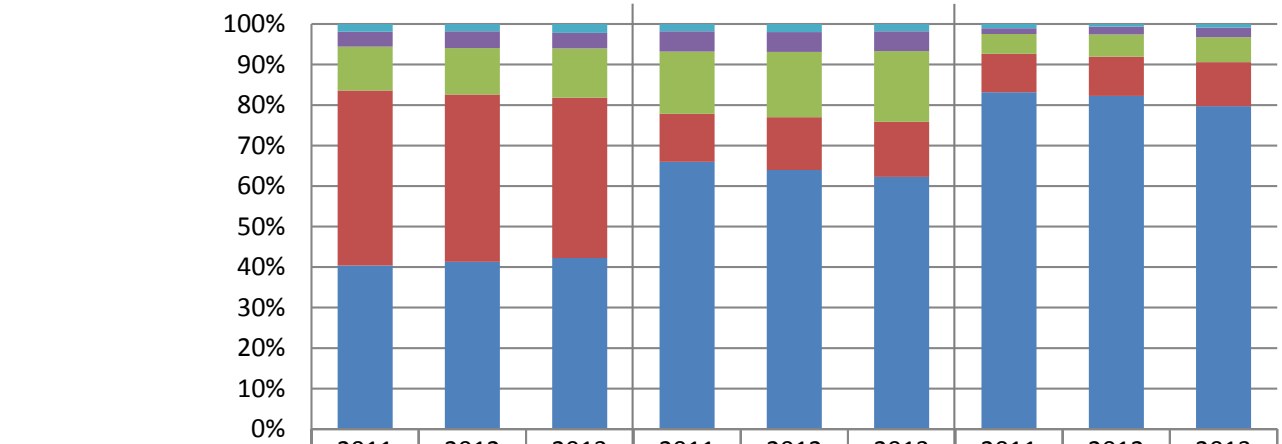
19. *Mid-level professionals* may include supervisors and managers.

Men held more positions than women in each pay grade category. The number of women in the *mid-level professionals* and *senior managers and officers* pay grade categories increased in all three years (appendix C, table C-3).

As illustrated in figure 4, the overall race/ethnicity concentrations within pay grade categories were relatively unchanged from 2011 through 2013. From 2011 through 2013, the Board's workforce was the most diverse in the a*ll other professional employees and all wage employees* category. During that same period, the workforce was the least diverse in the *senior managers and officers* category.

In each year under review, White employees as a percentage of total employees increased in each successively higher grade category. For example, in 2013, White employees accounted for approximately 42 percent of the *all other professional employees and all wage employees* category, 62 percent of the *mid-level professionals* pay grade category, and 80 percent of the *senior managers and officers* pay grade category. Within the *mid-level professionals* and *senior managers and officers* pay grade categories, the percentage of White employees declined while the percentage of non-White employees increased each year.

Figure 4: Workforce Distribution by Race/Ethnicity[a] and Pay Grade Category, 2011–2013



	2011	2012	2013	2011	2012	2013	2011	2012	2013
	All others (FR-16 to FR-25 and WE-41 to WE-47)			Mid-level professionals (FR-26 to FR-28)			Senior managers and officers (FR-29 to 00)		
Other	1.89%	1.78%	2.18%	1.78%	1.99%	1.80%	1.05%	0.65%	0.88%
Hispanic/Latino	3.68%	4.15%	3.86%	5.02%	4.91%	4.89%	1.40%	1.94%	2.35%
Asian	10.85%	11.46%	12.17%	15.38%	16.09%	17.47%	4.91%	5.48%	6.18%
Black/African American	43.18%	41.30%	39.56%	11.82%	13.06%	13.57%	9.47%	9.68%	10.88%
White	40.40%	41.30%	42.24%	66.00%	63.95%	62.28%	83.16%	82.26%	79.71%

Source: OIG analysis of Board-provided data.

Note: Percentages may not total 100 due to rounding.

[a]*Other* includes (1) Native Hawaiian or Other Pacific Islander (Not Hispanic or Latino), (2) American Indian or Alaska Native (Not Hispanic or Latino), (3) Two or More Races/Ethnicities (Not Hispanic or Latino), and (4) Not Specified (i.e., individuals who chose not to disclose demographic data).

Additional workforce distribution data for permanent employees by pay grade category, race/ethnicity, sex, and age are in appendix C.

Human Resource–Related Offices at the Board

Generally, the Board's human resources–related functions are performed by certain sections under the Chief Human Capital Officer within the Management Division as well as the Office of Diversity and Inclusion (OD&I), which is within the Office of the Chief Operating Officer.

Human Resources' Sections in the Management Division

Human Resources' (HR) mission is "to develop human capital strategies and services that align and support the strategic direction of the Board while creating an environment recognized as a 'great place to work' with a high-performing, diverse workforce." The office includes several sections that provide human resources services: Talent Acquisition, Compensation, Employee Relations (ER), and Organizational Development and Learning (OD&L).

Talent Acquisition

Talent Acquisition is responsible for recruiting and hiring. Although Talent Acquisition is involved with the hiring process for all 14 divisions and the OIG, the section does not recruit for certain specialized positions. These specialized positions are legal assistants, attorneys, senior attorneys, counsels, research assistants, and economists. Board divisions that hire research assistants and economists, as well as some specialized legal positions, conduct their own recruiting and applicant screening for those positions, while Talent Acquisition conducts final processing and onboarding for the selected specialized candidates.

Compensation

Compensation conducts analysis and provides recommendations on salary offers and increases for employees based on their qualifications and market conditions. For the performance management process, Compensation ensures that employees' performance ratings are accurately recorded and reconciled before annual merit increases are finalized, as these increases are based on the employees' performance ratings.

Employee Relations

ER provides employee counseling, dispute resolution, and policy assistance, and it also facilitates formal employee relations cases. ER's responsibilities include, but are not limited to, the following:

- identifying and bringing to management's attention emerging employee relations issues and trends that may affect employee morale
- gauging employee morale and assessing the quality of human resources programs and services through outreach

- resolving workplace issues by providing consultation and counseling for management and employees
- administering the Board's grievance and disciplinary actions policies
- collecting employee performance appraisals and managing appeals of employee performance appraisals
- developing and implementing employee relations policies

Organizational Development and Learning

OD&L is responsible for improving the Board's organizational performance and employees' productivity through training and development. The section provides the following services to Board employees:

- Assessments—employee and managerial assessments to identify opportunities for growth and expansion
- Career planning—assessments and development of employee skills that add value to the Board
- Consulting—guidance on organizational transitions, strategy creation, skill-gap analysis, team-need analysis, and creative training options
- Training and classes—guidance on training classes as well as the organization of in-house training for Board employees
- Succession planning—guidance to divisions in identifying and developing staff for career advancement
- Employee engagement surveys—management of the newly adopted, agency-wide process aimed at gaining employees' feedback on the Board's work environment.[20]

Office of Diversity and Inclusion

The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) requires federal financial agencies to establish an OMWI to be responsible for all agency matters related to diversity in management, employment, and business activities. The Board established the OD&I in January 2011 to house in one organization its existing EEO function; its diversity and inclusion programs for minorities, women, and other Board employees; and the Dodd-Frank Act OMWI activities related to financial education, supplier diversity, and regulated entities.

The Board's EEO function follows the regulations set forth in title 12, part 268, of the *Code of Federal Regulations*. These provisions are included in the Board's policy, program, and procedures for providing equal opportunity to Board employees and applicants for employment. In addition, the Board's EEO function manages the Board's EEO complaint process; regulatory reporting, such as that set forth in the MD-715; and EEO training.

20. The Board refers to the employee satisfaction survey as an engagement survey.

In accordance with the Dodd-Frank Act, the Board's OD&I is responsible for the following:

- developing and implementing standards and procedures to ensure, to the maximum extent possible, the fair inclusion and utilization of minorities and women in all activities of the Board

- developing standards for assessing the diversity policies and practices of entities regulated by the Board

- submitting to Congress an annual report regarding actions taken by the Board since the previous report, to include successes achieved and challenges faced by the Board in operating minority and women outreach programs; challenges the Board may face in hiring qualified minority and women employees and contracting with qualified minority-owned and women-owned businesses; and any other information, findings, conclusions, and recommendations for legislative or agency action, as appropriate

The OD&I is also responsible for diversity and inclusion programs that support recruiting and hiring.

Human Resources–Related Functions at the Board

The five human resources–related functions pertaining to diversity and inclusion that are covered in this report and the respective offices with primary or secondary responsibilities for these functions are shown in table 1.

Table 1: Board Offices Responsible for Select Human Resources–Related Functions

Office	Human resources–related functions at the Board				
	Recruiting and hiring	Performance management	Promotions and succession planning	Employee complaints	Employee surveys
Human Resources					
Employee Relations		primary for collecting		primary for non-EEO	primary for exit surveys
Organizational Development and Learning			primary for succession planning		primary for engagement surveys
Talent Acquisition	primary for general professional and wage secondary for officers		secondary for promotions		
Office of Diversity and Inclusion					
Diversity and Inclusion	secondary				
Equal Employment Opportunity				primary for EEO	
All Board divisions					
Divisions	primary for specialized positions and officers	primary for conducting	primary for promotions		

Source: OIG analysis of Board-provided documents and interviews.

The congressional request that initiated our work asked us to examine certain components of the Board's personnel-related functions with respect to diversity and inclusion. We identified these functions to include recruiting and hiring; performance management; promotions and succession planning; complaints; employee satisfaction surveys; and, more generally, the OD&I's overall efforts to enhance diversity and inclusion at the Board. Our findings and recommendations related to each of these activities are discussed in the remaining sections of this report.

Recruiting and Hiring

The Board recognizes that a work environment that attracts top talent is essential. We considered the Board's diversity efforts in its recruiting and hiring as part of our work to address the congressional request to examine the Board's overall human resources–related practices.

This section presents information on the Board's recruiting and hiring processes, including the competitive promotion process. Further, we present demographic statistics on recruiting and hiring. Our findings relate to the Board's processes for gathering and analyzing demographic data on applicants for certain specialized positions and officers.

The Board's Processes

The Board has four distinct processes for recruiting and hiring, depending on position type:

1. professional employees (other than professionals with specialized skills) and wage employees
2. specialized professional employees—legal assistants, attorneys, senior attorneys, and counsels
3. specialized professional employees—economists and research assistants
4. officers

The Board's recruiting and hiring processes for each position type are described below. For each recruitment process, Talent Acquisition assists with the final processing and onboarding of candidates selected for employment.

Recruiting and Hiring for Professional Positions (Other Than Professionals With Specialized Skills) and Wage Positions

The Board has established recruitment practices and uses a variety of methods to attract a broad range of candidates, including job boards, social media, and career fairs. In addition, the Board recruits from colleges and universities. The Board's *Vacant-Position Policy* provides guidance on posting vacancies, selecting the most qualified candidates from a pool of internal and external applicants, and promoting employee awareness of available career opportunities.

Talent Acquisition leads the Board's recruitment efforts and participates in recruiting events with entities such as the National Society of Hispanic MBAs, the National Society of Asian MBAs, and the Thurgood Marshall College Fund. Further, the Board recruits interns through (1) colleges and universities, including historically Black colleges and universities; (2) diversity-focused organizations, such as the Hispanic Association of Colleges and Universities, Washington

Internships for Native Students, the Workforce Recruitment Program,[21] and INROADS;[22] and (3) special-interest publications. OD&I staff members accompany Talent Acquisition representatives at certain recruiting events.

The Board generally provides current employees the first opportunity to apply for open positions;[23] however, the Board may simultaneously advertise open positions to external and internal candidates. Applicants are asked to voluntarily provide their sex and race/ethnicity at the time of application. Talent Acquisition reviews the applications of internal and external candidates to determine whether they meet the position's minimum requirements. Talent Acquisition forwards the applications of qualified internal and external candidates to the hiring manager. The hiring manager identifies candidates to be interviewed. Upon selection of a candidate, the hiring manager informs Talent Acquisition, which then conducts reference and education checks and offers a salary. Applicant information for these professional and wage positions is stored in a centralized applicant database.[24]

Recruiting and Hiring for Specialized Professional Positions—Attorneys

The Legal Division recruits for attorney positions in two ways. For mid-career attorney positions, the division can partner with Talent Acquisition to advertise a vacancy on the Board's public website. In August 2013, Talent Acquisition became involved in recruiting and screening attorney applicants. These applicants are asked to voluntarily provide demographic data at the time of application, and their information is stored in the same centralized applicant database that contains information on other professional and wage position applicants.

For entry-level attorney positions, a Legal Division recruiter recruits second- and third-year students from select law schools, which include schools that have banking law programs. Legal Division applicant information obtained through this process is also stored in the Board's centralized applicant database.

Recruiting and Hiring for Specialized Professional Positions—Economists and Research Assistants

Board divisions that recruit for and hire economists and research assistants have a standard practice for each type of position.[25] According to an economics division official, the Board's

21. The Workforce Recruitment Program is a nationwide recruitment and referral program that connects federal and private-sector employers with highly motivated college students and recent graduates with disabilities.

22. INROADS is the nation's largest nonprofit source of paid internships for undergraduate students of diverse backgrounds.

23. Employees may apply after the internal-only posting period ends, but they are then considered as external applicants and are not guaranteed an interview.

24. Talent Acquisition uses a human resources software application that manages the recruiting and hiring process. Information stored in the software database assists with evaluating candidate qualifications, tracking new hires, and maintaining metrics.

25. Six Board divisions hire economists and research assistants: Research and Statistics, International Finance, Monetary Affairs, Office of Financial Stability Policy and Research, Banking Supervision and Regulation, and Reserve Bank Operations and Payment Systems.

practice derives from universities' practice of posting relevant materials of those pursuing a PhD in economics on their public website. The Board develops its economist candidate pool in four ways:[26]

- A representative for the Board's economics divisions downloads the job market materials of those pursuing a PhD in economics (e.g., curriculum vitae and publications) from select university websites, irrespective of whether the individuals have expressed an interest in working for the Board.

- A committee of Board economists contacts faculty members in economics and finance departments at universities in the United States and abroad to request referrals of individuals expected to be in the job market.

- Candidates can send job market materials to an e-mail address specified on the section of the Board's public website that describes economist positions at the Board.

- Candidates can apply through the American Economic Association's Job Openings for Economists listings.

Board divisions that hire economists contact individuals from this resultant candidate pool to offer them an interview at the American Economic Association's annual meeting in January. A subset of those interviewed are invited for additional interviews at the Board. An individual may be extended multiple interviews and offers, and the economics divisions ultimately choose the candidates to whom they will extend an offer of employment. All economist candidate information is stored in the economics divisions' proprietary database,[27] which is separate from the Board's centralized applicant database.

Research assistants are recruited twice a year through job fairs and outreach to economics and mathematics departments at a number of universities. Applicants for these positions are directed to the Board's website and must submit the required materials (college transcripts and a survey of interest form) to the Board. The materials are reviewed by staff members in several divisions, and qualified candidates are ranked based on credentials. Multiple divisions can interview and extend offers to research assistant candidates. Research assistants at the Board are typically employed for two years; however, their positions can be extended for a year.[28] Research assistant applicant materials are downloaded to a database that is separate from both the database used for economists' applications as well as the Board's centralized applicant database.

Divisions that recruit for economists request demographic data from applicants in the Board's economist database in a mass e-mail that is sent to all the e-mail addresses obtained from curriculum vitae accumulated during the development of the applicant pool, irrespective of whether the individuals have expressed an interest in working for the Board. Divisions that recruit for research assistants request demographic data from applicants after the applicants submit their

26. For the purposes of our review, an economist or research assistant applicant is a candidate whose information is stored in the economics divisions' proprietary database. These individuals may or may not have expressed an interest in working for the Board. An applicant's job market materials are considered by multiple Board divisions.

27. Multiple divisions may consider any candidate in the database for an economist or research assistant position. As a result, individuals were counted multiple times.

28. Research assistants are considered as part of the Board's permanent workforce.

job market materials. The e-mail contains a form that requests research assistant applicants to voluntarily provide their sex and race/ethnicity. Applicants choosing to disclose this information must return the form via e-mail. Data for all individuals being considered for these positions is manually compiled and submitted to HR. HR combines the economist and research assistant demographic data with all other applicant data contained in the Board's centralized applicant database to complete federal reporting requirements.

Hiring officials in the divisions that recruit economists and research assistants acknowledge that diversity within the economics profession is low and that the Board faces challenges in recruiting minorities for these positions. Divisions that hire for these specialized positions recruit at select schools with economist programs. Hiring officials state that they have taken measures to broaden their outreach for economists to underrepresented groups. For example, Board economists serve as program faculty at the American Economic Association Summer Program, which is designed for minority college-level students studying economics.

In addition, outreach is conducted at the high-school level to enhance students' interest in economics prior to college. For example, the FedEd program promotes outreach to underserved high schools in the Washington, DC, metro area and Math x Econ program brings students who are underrepresented in the field of economics, including minorities and women, from underserved high schools to the Board for a one-day program that highlights careers in economics in general and at the Board in particular.

Subsequent to our review, the Board, in partnership with the American Economic Association, hosted the National Summit on Diversity in the Economics Profession. The conference brought together Presidents and Research Directors of the Federal Reserve Banks and Chairs of economics departments from universities around the country to discuss, among other things, the state of diversity in the economics profession.

Recruiting and Hiring for Officers

Board divisions can recruit officers by using the assistance of an external search firm or using the assistance of Talent Acquisition. Divisions can also promote from within. However, officer hirings are managed by, and must be processed through, HR. Each division is charged with developing a detailed justification memorandum to support its officer selection. According to a Board official, Talent Acquisition and the OD&I review the candidate selection justification before it is submitted for approval by either the Oversight Governor for the division or the full Board of Governors.[29]

As of June 2014, both Talent Acquisition and the Director of the OD&I are involved in the early activities of the officer hiring process. These activities include, but are not limited to, discussing the recruitment strategy, identifying the selection panel, and reviewing résumés. Information about the officer applicant pool varied from division to division and was not always captured in the Board's centralized database during the years under review.

29. Internal officer promotions are approved by the division's Oversight Governor and the Administrative Governor. For a newly created officer position, officer vacancies filled with external candidates, or a Board employee who is being considered for an officer position, the members of the Board of Governors must approve the position and the new officer appointment.

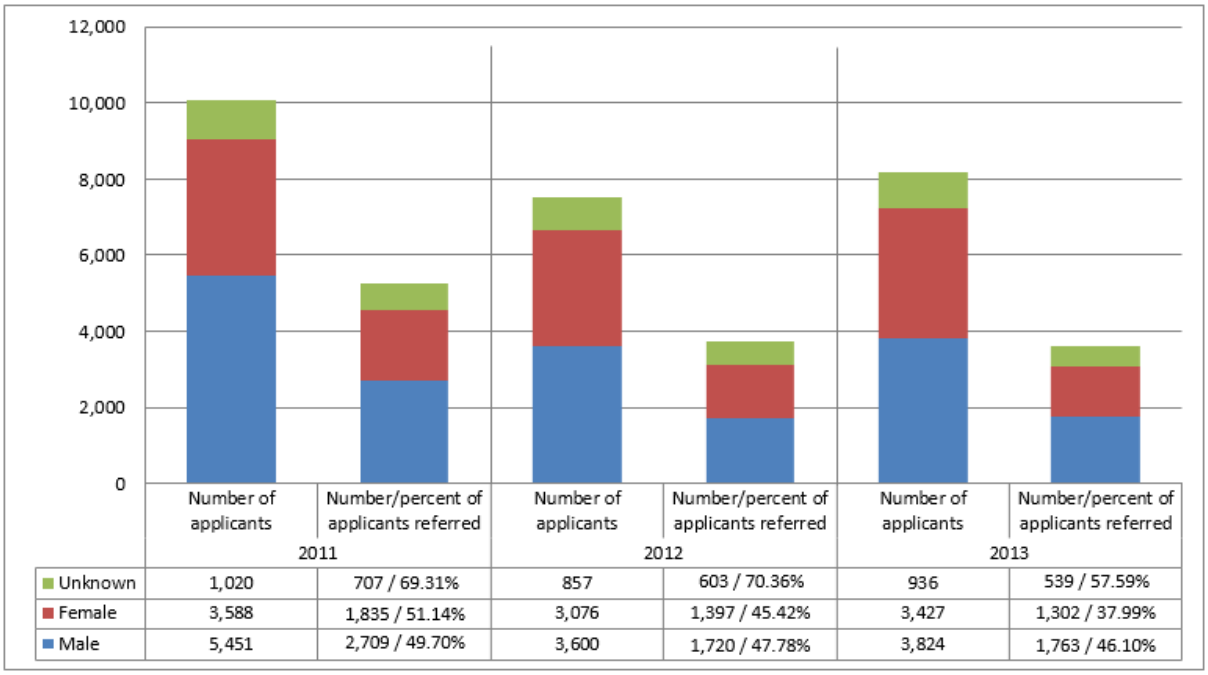
Demographic Statistics

Professional Positions (Other Than Economists and Research Assistants) and Wage Positions

During the application process, applicants for professional positions—including legal assistants, attorneys, senior attorneys, and counsels—and wage positions are prompted to voluntarily provide demographic data, to include sex and race/ethnicity. We analyzed demographic data from the Board's centralized applicant database pertaining to all applicants, to those applicants found to be qualified and referred to the hiring manager, and to those who were ultimately hired. The Board filled 232 professional and wage positions in 2011, 199 positions in 2012, and 154 positions in 2013.

Figure 5 illustrates the number of male and female applicants who applied and the number who were referred to the hiring manager during the period under our review. We found that similar percentages of male and female applicants were referred to the hiring manager. Applicants who did not voluntarily disclose their sex are included in the *Unknown* category.

Figure 5: Professional Position (Other Than Economist and Research Assistant) and Wage Position Applicants, by Sex, 2011–2013



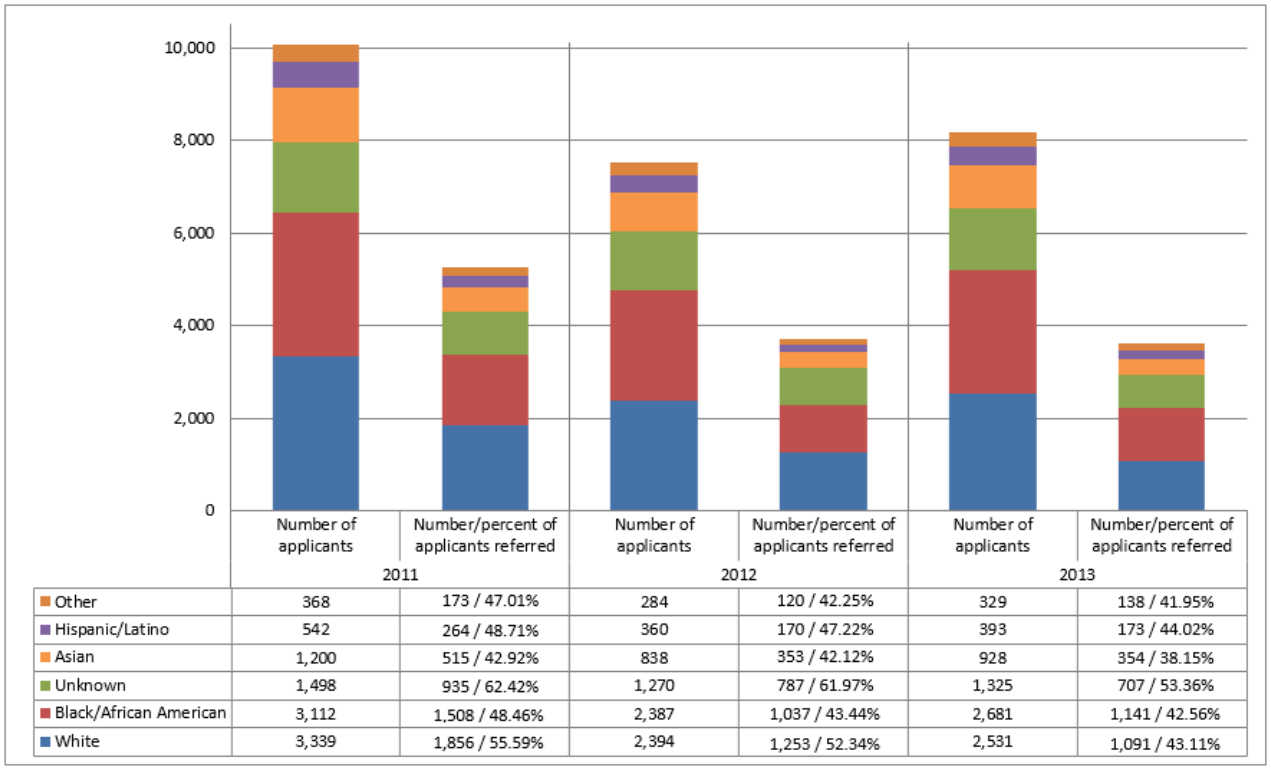
	2011		2012		2013	
	Number of applicants	Number/percent of applicants referred	Number of applicants	Number/percent of applicants referred	Number of applicants	Number/percent of applicants referred
Unknown	1,020	707 / 69.31%	857	603 / 70.36%	936	539 / 57.59%
Female	3,588	1,835 / 51.14%	3,076	1,397 / 45.42%	3,427	1,302 / 37.99%
Male	5,451	2,709 / 49.70%	3,600	1,720 / 47.78%	3,824	1,763 / 46.10%

Source: OIG analysis of Board-provided data.

The total distribution of hires by sex for professional positions (other than economists and research assistants) and wage positions during the three-year period was 339 males, or 57.95 percent of the total hired, and 246 females, or 42.05 percent of the total hired.

Figure 6 illustrates the race/ethnicity composition of applicants who applied and were referred to the hiring manager during the three years we reviewed. Applicants who did not voluntarily disclose their race/ethnicity are included in the *Unknown* category.[30]

Figure 6: Professional Position (Other Than Economist and Research Assistant) and Wage Position Applicants, by Race/Ethnicity,[a] 2011–2013



	2011		2012		2013	
	Number of applicants	Number/percent of applicants referred	Number of applicants	Number/percent of applicants referred	Number of applicants	Number/percent of applicants referred
Other	368	173 / 47.01%	284	120 / 42.25%	329	138 / 41.95%
Hispanic/Latino	542	264 / 48.71%	360	170 / 47.22%	393	173 / 44.02%
Asian	1,200	515 / 42.92%	838	353 / 42.12%	928	354 / 38.15%
Unknown	1,498	935 / 62.42%	1,270	787 / 61.97%	1,325	707 / 53.36%
Black/African American	3,112	1,508 / 48.46%	2,387	1,037 / 43.44%	2,681	1,141 / 42.56%
White	3,339	1,856 / 55.59%	2,394	1,253 / 52.34%	2,531	1,091 / 43.11%

Source: OIG analysis of Board-provided data.

[a]*Other* includes (1) Native Hawaiian or Other Pacific Islander (Not Hispanic or Latino), (2) American Indian or Alaska Native (Not Hispanic or Latino), and (3) Two or More Races/Ethnicities (Not Hispanic or Latino). *Unknown* includes individuals who chose not to disclose their demographic data.

Table 2 illustrates, for the period of our review, the race/ethnicity composition of applicants hired for professional positions (other than economists and research assistants) and wage positions. In the three-year period, approximately 43 percent of all such hires were non-White individuals.

30. Because applicants are not asked to provide a birthdate during the application process, we did not conduct an analysis of the age of applicants and referred applicants.

Table 2: Professional Position (Other Than Economist and Research Assistant) and Wage Position Hires, by Race/Ethnicity, 2011–2013

Race/Ethnicity	Number hired	% of hired
Asian	82	14.02
Black/African American	128	21.88
White	333	56.92
Hispanic/Latino	31	5.30
Other[a]	11	1.88
Total hired	**585**	**100.00**

Source: OIG analysis of Board-provided data.

Note: All hires fully disclosed their race/ethnicity. We were unable to compare the composition of hires to the composition of the applicant pool due to the number of *Unknown* responses in the applicant pool.

[a]*Other* includes (1) Native Hawaiian or Other Pacific Islander (Not Hispanic or Latino), (2) American Indian or Alaska Native (Not Hispanic or Latino), and (3) Two or More Races/Ethnicities (Not Hispanic or Latino).

For more detailed information on the demographics of applicants for professional positions (other than economists and research assistants) and wage positions, see appendix D.

Specialized Positions for Economists and Research Assistants

We attempted to analyze the demographic trends of economist and research assistant applicants as they moved through the recruiting and hiring process; however, we were unable to perform a meaningful analysis due to the large number of applicants who had not voluntarily disclosed their sex or race/ethnicity.[31] The economist database for storing applicant information differs from the database used to store information on research assistant applicants, and both are separate from the Board's centralized applicant database, which is used for other professional and wage position vacancies. As noted above, divisions that recruit for economists and research assistants request demographic data from applicants by sending a form in a separate mass e-mail, and in the case of economist candidates, demographic data is requested irrespective of whether the candidates have expressed an interest in working for the Board. Applicants choosing to disclose this information must return the form via e-mail.

The Board filled 116 economist and research assistant positions in 2011, 85 positions in 2012, and 112 positions in 2013. Upon gaining employment at the Board, all economists and research assistants disclosed their sex for the years under review. The total distribution of economist and research assistant hires by sex during the three-year period was 206 males, or 65.81 percent of the total hired, and 107 females, or 34.19 percent of the total hired.

Table 3 illustrates the total distribution of economist and research assistant hires by race/ethnicity during the period of our review. Approximately 25 percent of economist and research assistant hires during this period were non-White.

31. For the purposes of our review, an economist or research assistant applicant is a candidate whose information is stored in the economics divisions' proprietary database. These individuals may or may not have expressed an interest in working for the Board. An applicant's job market materials are considered by multiple Board divisions.

Table 3: Economist and Research Assistant Hires, by Race/Ethnicity, 2011–2013

Race/Ethnicity	Number hired	% of hired
Asian	61	19.49
Black/African American	2	0.64
White	234	74.76
Hispanic/Latino	10	3.19
Other[a]	6	1.92
Total hired	**313**	**100.00**

Source: OIG analysis of Board-provided data.

Note: All hires fully disclosed their race/ethnicity. We were unable to compare the composition of hires to the composition of the applicant pool due to the number of *Unknown* responses in the applicant pool.

[a]*Other* includes (1) Native Hawaiian or Other Pacific Islander (Not Hispanic or Latino), (2) American Indian or Alaska Native (Not Hispanic or Latino), and (3) Two or More Races/Ethnicities (Not Hispanic or Latino).

For more detailed information on the demographics of applicants for economist and research assistant positions, see appendix D.

The OIG's Analysis of Nondisclosure of Demographic Information

We found that in 2011, approximately 67 percent of individuals considered for economist and research assistant positions did not voluntarily disclose their sex or race/ethnicity, which was considerably higher than the 10 to 15 percent nondisclosure rate of applicants for professional positions (other than economists and research assistants) and wage positions (table 4). In 2012, the nondisclosure rate of economist and research assistant applicants approximated 59 percent, and in 2013, this rate rose to approximately 92 percent. The low response rate may be attributable to the fact that a mass e-mail is sent to the applicant pool for economist positions, irrespective of whether the individuals have expressed an interest in working for the Board. Also, in 2013, according to a Board official, the e-mail was not sent. See appendix D for a distribution of the applicants who voluntarily disclosed their demographic data.

Table 4: Percentage of Applicants Who Did Not Voluntarily Disclose Demographic Information, by Type of Position, 2011–2013

Applicant type	2011	2012	2013
Unknown sex			
Economist and research assistant	67.01	58.96	92.13
Other professional position and wage position	10.14	11.38	11.43
Unknown race/ethnicity			
Economist and research assistant	67.19	59.31	92.26
Other professional position and wage position	14.89	16.86	16.18

Source: OIG analysis based on Board-provided data.

Officers

We attempted to analyze the applicant demographic data for officer positions; however, these data were not consistently tracked by Talent Acquisition and Board divisions. As such, we conducted an analysis of the sex and race/ethnicity of the number of officers selected during the years under our review. The Board filled 30 officer positions in 2011, 26 in 2012, and 18 in 2013 (table 5). Of these 74 officer positions filled through internal promotions and external hires, 41.89 percent were female. The race/ethnicity composition of officers selected over the three-year period was as follows: 8.11 percent were Asian, 8.11 percent were Black/African American, 81.08 percent were White, 1.35 percent were Hispanic/Latino, and 1.35 percent were Other.

Table 5: Officer Selections, by Sex and by Race/Ethnicity, 2011–2013

Demographic group	2011		2012		2013	
	Number selected	% of selected	Number selected	% of selected	Number selected	% of selected
Sex						
Male	13	43.33	19	73.08	11	61.11
Female	17	56.67	7	26.92	7	38.89
Total	**30**	**100.00**	**26**	**100.00**	**18**	**100.00**
Race/Ethnicity						
Asian	1	3.33	5	19.23	0	0.00
Black/African American	3	10.00	3	11.54	0	0.00
White	25	83.33	17	65.38	18	100.00
Hispanic/Latino	1	3.33	0	0.00	0	0.00
Other[a]	0	0.00	1	3.85	0	0.00
Total	**30**	**100.00**	**26**	**100.00**	**18**	**100.00**

Source: OIG analysis based on Board-provided data.

Note: Officer selections include both internal promotions and external hires.

[a]*Other* includes (1) Native Hawaiian or Other Pacific Islander (Not Hispanic or Latino), (2) American Indian or Alaska Native (Not Hispanic or Latino), and (3) Two or More Races/Ethnicities (Not Hispanic or Latino).

Finding: The Board Cannot Fully Assess the Level of Diversity in the Economist and Research Assistant Applicant Pool

We found that in 2011 and 2012, over half the individuals in the economist and research assistant database did not voluntarily disclose their sex and race/ethnicity; this percentage rose to over 90 percent in 2013. We were informed that in 2013, no economist applicants disclosed demographic information. These rates of nondisclosure did not facilitate demographic trend analysis in the economist and research assistant applicant pools.

The EEOC's guidance to federal agencies for MD-715 reporting instructs agencies to report applicant demographic data for prescribed occupational categories. Pursuant to this guidance, the Board reports applicant pool data for occupational categories that include economists and

research assistants. Further, the guidance states that if a particular group has a low participation rate in a particular occupation, the agency should determine whether recruitment efforts are resulting in a diverse pool of applicants. The Board cannot assess the degree to which the economist and research assistant applicant pool is diverse because the Board's process to collect demographic data for these applicants has resulted in high nondisclosure rates.

Divisions request demographic data from individuals considered for economist and research assistant positions in an additional step in the recruitment process by sending a mass e-mail that contains a form requesting the individual to voluntarily provide his or her sex and race/ethnicity. In the case of economist applicants, this e-mail is sent irrespective of whether the individuals have expressed an interest in working for the Board. Research assistant applicants are asked after their expression of interest in employment. If the individual chooses to disclose this information, he or she must return the form via e-mail. In contrast, professional and wage applicants are asked to voluntarily disclose their demographic data at the time they apply for a position on the Board's website, and the information is stored in the Board's centralized applicant database. In 2013, according to an official, the mass e-mail to request economists' demographic data was never released due to an administrative error.

We found that the method used to obtain demographic data from economist and research assistant applicants did not result in a response rate that enabled the agency to identify diversity trends in its economist and research assistant applicant pool. This method is less effective than the method used for professional positions (other than economists and research assistants) and wage positions, which yields a higher percentage of applicants disclosing demographic data.

Management Actions

According to an official, the Board implemented a new process for economist candidates in 2014 in which the Board automatically requests self-disclosure of demographic information within 24 hours of the Board obtaining an economist applicant's e-mail address. This process eliminates the administrator's role of releasing the mass e-mail.

Recommendation

We recommend that the Directors of the divisions that recruit economists and research assistants

1. Develop and implement an alternative method for collecting the demographic data of economist and research assistant applicants to improve the response rate.

Management's Response

The Board concurs with our recommendation. In its response, the Board notes that management began implementing a new process to automatically request self-disclosure of demographic information within 24 hours of obtaining an economist applicant's e-mail address. The Board will assess whether this change provides a significant improvement in response rates for economist and research assistant applicants and, if not, will consider other changes in order to obtain demographic data for economist and research assistant applicants.

OIG Comment

The actions described by the Board are generally responsive to our recommendation. We plan to follow up on the Board's actions to ensure that the recommendation is fully addressed.

Finding: The Board Did Not Consistently Track Officer Applicant Demographic Data

We found that the Board's method for recruiting and hiring officers did not produce information that shows the diversity of the applicant pool. Demographic information for the officer applicant pool was not consistently tracked by Talent Acquisition, the hiring division, or the executive search firms used by divisions. We also noted that during 2011–2013, two officer positions were tracked in the Board's centralized applicant database.

The MD-715 guidance requires agencies to report applicant demographic data for occupational categories, including senior-level positions. Further, the guidance states that if a particular group has a low participation rate in the applicant pool, the agency should determine whether recruitment efforts are resulting in a diverse pool of applicants.

Historically, the Board's divisions have operated autonomously in establishing their management processes, including those for recruiting and hiring officers. A division may fill an officer vacancy by promoting from within the division, using an executive search firm, or posting a vacancy announcement through the Board's centralized applicant database. Because the Board has several methods to recruit and hire officers and does not consistently collect voluntary demographic data for officer applicants, the Board cannot assess the diversity of the applicant pool for officer-level positions. By establishing a standardized formal process to ensure that officer applicant demographic data are captured, the Board can better assess whether its officer recruitment efforts are resulting in a diverse pool of applicants.

Management Actions

In June 2013, the Board began a more standardized process to recruit for officer positions. Further, all officer positions will be tracked through the centralized applicant database. This standardized process may allow Talent Acquisition to accumulate demographic data and measure trends in diversity at the officer-applicant level. While these efforts will provide the Board with better information to assess the diversity of its officer applicant pool, we note that there may be gaps in the demographic data when divisions use an executive search firm to recruit officer candidates.

Recommendation

We recommend that the Chief Human Capital Officer

2. Ensure that the demographic data for all internal and external officer applicants are maintained in the Board's centralized applicant database.

Management's Response

The Board concurs with our recommendation. In its response, the Board notes that management began to implement processes to track officer positions, which it believes will allow it to accumulate demographic data and measure trends in diversity at the officer-applicant level.

OIG Comment

The actions described by the Board are generally responsive to our recommendation. We plan to follow up on the Board's actions to ensure that the recommendation is fully addressed.

Performance Management

The purpose of the Board's Performance Management Program is (1) to continuously improve individual and organizational performance, (2) to develop and motivate employees to become top performers and help the Board achieve its mission and purpose, and (3) to inform various employment decisions.

This section presents information on performance management for the period of our review, including a summary of the Board's process and trend statistics based on the independent analysis performed by an external consulting firm. The consulting firm's analysis indicated statistically significant differences in performance ratings among certain demographic groups on an agency-wide basis. When these demographic groups' performance ratings were evaluated by pay grade category, however, in most cases there was no trend of statistically significant differences.[32] The agency-wide differences do not necessarily indicate discrimination and could be due to actual differences in employee performance or other factors. Further analysis of performance ratings may help the Board identify any patterns that may indicate potential unfair or unequal treatment. The Board piloted a new performance management system in 2014; performance management data associated with the new rating system are not reflected in our analysis.

The Board's Process

The Board's *Performance Management Program* policy describes the Board's Performance Management Program, which provides the framework for an employee's annual performance assessment and rating during the period of our review. The Board's performance periods follow a fiscal year (October 1 through September 30) schedule. Supervisors are responsible for creating performance standards, monitoring performance, and providing employees with feedback on their performance. Supervisors are required to conduct an annual, written review of an employee's performance, which should be reviewed by the supervisors' manager before issuance to the employee. In the fiscal year (FY) 2011, FY 2012, and FY 2013 rating periods, employees were assigned one of five possible ratings: *extraordinary*, *outstanding*, *commendable*, *marginal*, and *unsatisfactory*.[33]

According to the Board's policy, the reviewing manager should attempt to resolve any disagreement between an employee and his or her supervisor with respect to the employee's performance rating. Further, Board employees other than a Division Director, an Office Director, or the Chief Operating Officer can, within a certain time frame, appeal their performance rating

32. The external consulting firm we used refers to this as *job level* rather than pay grade category.

33. Economists were on a seven-tier system: *extraordinary*, *outstanding plus*, *outstanding*, *commendable plus*, *commendable*, *marginal*, and *unsatisfactory*.

with the Director of the division or office.[34] ER will assist in facilitating this process. However, if the appeal is based on sex, race/ethnicity, or age, the employee must file a separate complaint with the OD&I.[35]

Annual performance ratings are the basis for determining merit salary increases, which are administered by Compensation, and the ratings may also be considered when determining variable pay, eligibility for additional incentive programs, and promotions.[36] Employees with a rating of *marginal* or *unsatisfactory* are not eligible for merit increases or other types of performance-based pay.

Demographic Statistics

Results From an External Consulting Firm's Analysis Performed for the OIG

We used an external consulting firm to conduct an independent analysis of the Board's FY 2011, FY 2012, and FY 2013 employee performance ratings. The consulting firm conducted tests of statistical significance and practical significance to evaluate group differences.[37] For analysis purposes, the consulting firm analyzed gender and age differences, as well as race/ethnicity differences among the White, Black/African American, Hispanic/Latino, Asian, and Other groups.[38] The consulting firm evaluated performance data for three pay grade categories: *senior managers and officers* (FR-29 and 00), *mid-level professionals* (FR-26 to FR-28), and *all others*[39] (FR-16 to FR-25 and WE-41 to WE-47).

The external consulting firm's analysis revealed that overall during the three-year period, approximately 99 percent of Board employees received ratings of *commendable* or above (table 6).[40]

34. The Chief Human Capital Officer will review appeals if the Division Director is the supervisor or the reviewing manager. If the Chief Human Capital Officer is the supervisor or the reviewing manager, the Board's General Counsel will appoint an appeals officer.

35. The OD&I and ER ensure that the appropriate office handles an employee's complaint, depending on the basis. Gender, race/ethnicity, age, or disability discrimination claims are handled by the OD&I; other workplace complaints are handled by ER.

36. During the review period, variable pay was generally targeted toward officers and employees in designated job families that (1) are critical to the execution of the Board's core mission, (2) require skills that are in high demand in the marketplace, (3) have salaries well below prevailing market levels, and (4) experience recruiting difficulties and high rates of turnover. Compensation reviews new variable pay requests for additional job families and makes a recommendation to the Chair of the Committee on Board Affairs, who makes the final determination.

37. A test for statistical significance indicates the probability that the group difference could have been due to chance. In contrast, measures of practical significance provide an indication of the size of the difference.

38. *Other* includes American Indian/Alaskan Native, Native Hawaiian/Pacific Islander, individuals identifying themselves as belonging to two or more races, and individuals who chose not to disclose demographic data.

39. In this section of the report, the external consulting firm's use of the term *all others* equates to our use of the term *all other professional employees and all wage employees* elsewhere in the report.

40. Economists who were rated *outstanding plus* are shown as *outstanding* and those rated as *commendable plus* are shown as *commendable*.

Table 6: Distribution of Performance Ratings for All Employees, FY 2011–FY 2013

Performance ratings	FY 2011		FY 2012		FY 2013	
	Number of rated employees	% of total rated employees	Number of rated employees	% of total rated employees	Number of rated employees	% of total rated employees
1—*extraordinary*	378	19.13	429	20.27	480	22.39
2—*outstanding*	712	36.03	848	40.08	956	44.59
3—*commendable*	882	44.64	829	39.18	696	32.46
4—*marginal*	4	0.20	10	0.47	12	0.56
5—*unsatisfactory*	0	N/A	0	N/A	0	N/A
Total	**1,976**	**100.00**	**2,116**	**100.00**	**2,144**	**100.00**

Source: External consulting firm analysis based on Board-provided data.

The results of the consulting firm's analysis of the Board's FY 2011, FY 2012, and FY 2013 performance ratings indicated statistically significant differences among Board employees across certain demographic groups on an agency-wide basis. However, when these demographic groups' performance ratings were evaluated by pay grade category, in most cases, there was no trend of statistically significant differences. These statistically significant differences do not necessarily indicate discrimination and could be due to a variety of factors either individually or in combination, such as actual differences in employee performance. A statistically significant result does not imply that a difference is good or bad or that it is large or small; it indicates that the observed difference is probably not due to chance.

The external consulting firm did not find statistically significant differences in the gender category. However, the consulting firm found statistically significant differences in the following race/ethnicity and age categories:

- In all three years, on an agency-wide basis, White employees received higher performance ratings compared with Asian employees; however, there were no significant differences in performance ratings when analyzed at the job levels.

- In all three years, on an agency-wide basis, White employees received higher performance ratings compared with Black/African American employees. In 2012 and 2013, there were no statistically significant differences in performance ratings when analyzed at the job levels. In 2011, there was a statistically significant difference between the average ratings of White employees and Black/African American employees for the *all others* employee job level.

- In 2013, in the *senior managers and officers* category, Hispanic/Latino employees received higher performance ratings as compared with White employees. The comparison included 247 White employees and only 7 Hispanic/Latino employees; therefore, these results should be interpreted with caution.[41]

41. According to the external consulting firm, small sample results are often nonrepresentative and unstable and can change substantially with small changes in the data.

- In 2012, on an agency-wide basis, White employees received higher performance ratings compared with Hispanic/Latino employees; however, there were no significant differences in performance ratings when analyzed at the job levels.

- In 2012, on an agency-wide basis, employees 40 years of age or older received higher performance ratings than employees under 40 years of age; however, there were no significant differences in ratings for employees under 40 years of age and employees 40 years of age or older within the *senior managers and officers* job level and within the *all others* employee job level.

- In all three years, in the *mid-level professionals* category, employees under 40 years of age received higher performance ratings than employees 40 years of age or older.

The consulting firm's full report on the Board's employee performance ratings is included as appendix E.

The OIG's Analysis

In addition to the external consulting firm's statistical analysis of performance ratings for the entire Board, we analyzed performance ratings by division to determine average performance ratings for FY 2011, FY 2012, and FY 2013 by race/ethnicity. We did not evaluate these averages for statistical significance, and we did not conduct analyses by pay grade category.

The results of our analysis by division were similar to the external consulting firm's agency-wide findings discussed above.[42] These observations do not necessarily indicate discrimination and could be due to a variety of factors. Appendix F contains our analysis of performance management data by divisions.

Finding: The Board Has Not Conducted Analyses of Employee Performance Reviews on an Annual Basis

According to a Board official, the Board does not consistently conduct a review of the distribution of performance ratings to ascertain how the ratings are distributed across sex, race, or people 40 years of age or older. The Board has periodically analyzed aggregate performance ratings distributions by divisions. Further, in 2012, the Board surveyed employees on the Performance Management Program. The final results report indicates survey participant concerns with effectiveness, fairness, and rater bias.

One government best practice suggests that organizations should gather and analyze statistics on the distribution of performance ratings.[43] Uneven ratings distributions across gender and race/ethnicity might raise questions about fairness. If differing treatment is found within the performance appraisal process, efforts should be made to determine whether appraisal design

42. The external consulting firm reversed the order of the Board's performance management rating system so that higher ratings reflected better performance. However, our analysis reflects the Board's ordering of performance ratings, in which a lower rating number reflected higher performance (e.g., *extraordinary* is represented by a rating of 1).

43. U.S. Office of Personnel Management, *Evaluating Performance Appraisal Programs: An Overview*, PMD-09, January 1999.

features are causing the lack of balance in the ratings or whether other issues at the organization may be responsible.

As previously noted, the external consulting firm found statistically significant differences in performance ratings among certain demographic groups on an agency-wide basis. When these demographic groups' performance ratings were evaluated by pay grade category, however, in most cases there was no trend of statistically significant differences. Additional analyses of employee performance ratings will allow the Board to better determine whether its performance management system supports the development and retention of a diverse workforce.

Management Actions

The Board acknowledged challenges with the performance management system in place during the review period. In discussions about the performance management framework, employees were in favor of a framework that (1) focused on growth, (2) included ongoing conversations between managers and employees, (3) created a partnership between managers and employees, and (4) potentially had a more effective method to rate performance. The Board decided to adopt a new performance rating system.

The new performance management process was piloted in five divisions and the OIG for performance year 2013–2014, with full implementation in all Board divisions in the 2014–2015 performance year. The purpose of the new process is to align staff to the work of the Board, provide greater accountability, support the growth of staff, improve the value of time spent, and increase the fairness of the process. In addition, the new process involves frequent conversations between employees and their managers that are designed to develop and grow employees' capabilities. The Board contracted for the necessary expertise to assist with the program's implementation, which includes information sessions, tools and guides, training, and other support.

Recommendation

We recommend that the Chief Human Capital Officer

3. Consider conducting annual analyses of the distribution of employee performance ratings to identify whether patterns exist that may indicate unfair or unequal treatment. If the analyses reveal patterns that may indicate unfair or unequal treatment, determine whether any actions are necessary.

Management's Response

The Board concurs with our recommendation. In its response, the Board notes that a periodic analysis focused on areas in which management has potential concerns may be useful. Management will consider the feasibility of conducting additional analyses on a periodic basis.

OIG Comment

The actions described by the Board are generally responsive to our recommendation. We plan to follow up with the Board to determine its final decision in considering our recommendation.

Promotions and Succession Planning

In the OIG's September 2014 *Major Management Challenges for the Board of Governors of the Federal Reserve System*, we reported on the Board's risk associated with staff retirement and turnover, as well as challenges the Board faces in replacing employees with specialized knowledge and skill sets. One way to address such challenges is through succession planning. GAO states that succession planning is a comprehensive ongoing process that provides for forecasting senior leadership needs, identifying and developing candidates with the potential to fill future leadership position openings, and selecting individuals from a diverse pool of qualified candidates to meet executive resource needs. Similarly, promotions can also be a vehicle for increasing agency diversity.

This section presents information on the Board's career-ladder promotions process as well as demographic statistics on promotions. We found that the Board started a formal succession planning process in late 2012, but it has not yet been fully implemented across all Board divisions.

The Board's Processes

Promotions

Promotions at the Board may be made in a competitive manner or through career-ladder progression. A competitive promotion is a grade increase that results when an employee applies for a vacant position in a higher grade level than the current employee's grade level, competes from a pool of applicants, and is hired for the position. Competitive promotions are addressed in the Board's *Vacant-Position Posting* policy. Information on competitive promotions is included in the Recruiting and Hiring section of this report.

A career-ladder promotion is available to both wage and professional employees in positions that allow for the employee to be promoted to one or more sequentially higher pay grades within the career ladder for his or her position. Employees in such positions may become eligible for a career-ladder promotion once they complete any required time within the grade and have proven their ability to perform satisfactorily at the next-higher pay grade. An employee's manager or supervisor recommends an employee for a career-ladder promotion by preparing a written justification. Once the recommendation is approved within the respective division, Talent Acquisition processes the personnel action.

Succession Planning

According to GAO, agencies with effective succession planning and management efforts determine the critical skills and competencies that will be needed to achieve current and future program results; develop strategies tailored to address gaps in human capital approaches for enabling and sustaining the contributions of all critical skills and competencies; and address

specific human capital challenges, such as diversity.[44] In addition, succession planning is one of GAO's nine leading diversity management practices. In that context, GAO describes strategic planning as an ongoing, strategic process for identifying and developing a diverse pool of talent for an organization's potential future leaders.

The Board developed a two-phase, formal agency-wide succession planning program in late 2012 to help identify a diverse pool of candidates for senior management positions throughout the Board. The Board's program will identify development opportunities for employees to prepare them for potential advancement. Both phases entail planning discussions with Board senior management focusing on three elements: (1) employee performance, (2) learning agility, and (3) readiness.

Phase 1 discussions are held with Division Directors and Deputy Directors regarding their direct reports at the officer level. Phase 2 of the Board's succession planning program will involve discussions with officers regarding their managers. The Board currently does not have a formal plan for Board employees in nonsupervisory roles; however, divisions have engaged in informal succession planning practices that are separate from the Board's formal succession planning program.

Demographic Statistics

We conducted an analysis of career-ladder promotions for all three pay grade categories at the Board. For the purpose of this report, our analysis focuses on career-ladder promotions by race/ethnicity in 2011, 2012, and 2013 (figure 7). We did not conduct an analysis of the eligibility requirements based on time in grade for career-ladder promotions because these requirements vary by division and position type. In addition, an employee's performance rating may also factor into his or her eligibility. Therefore, the results of our trend analysis do not necessarily indicate discrimination or bias and could be due to a variety of factors.

In 2011 through 2013, the Board awarded a total of 610 career-ladder promotions. Of these 610 promotions,

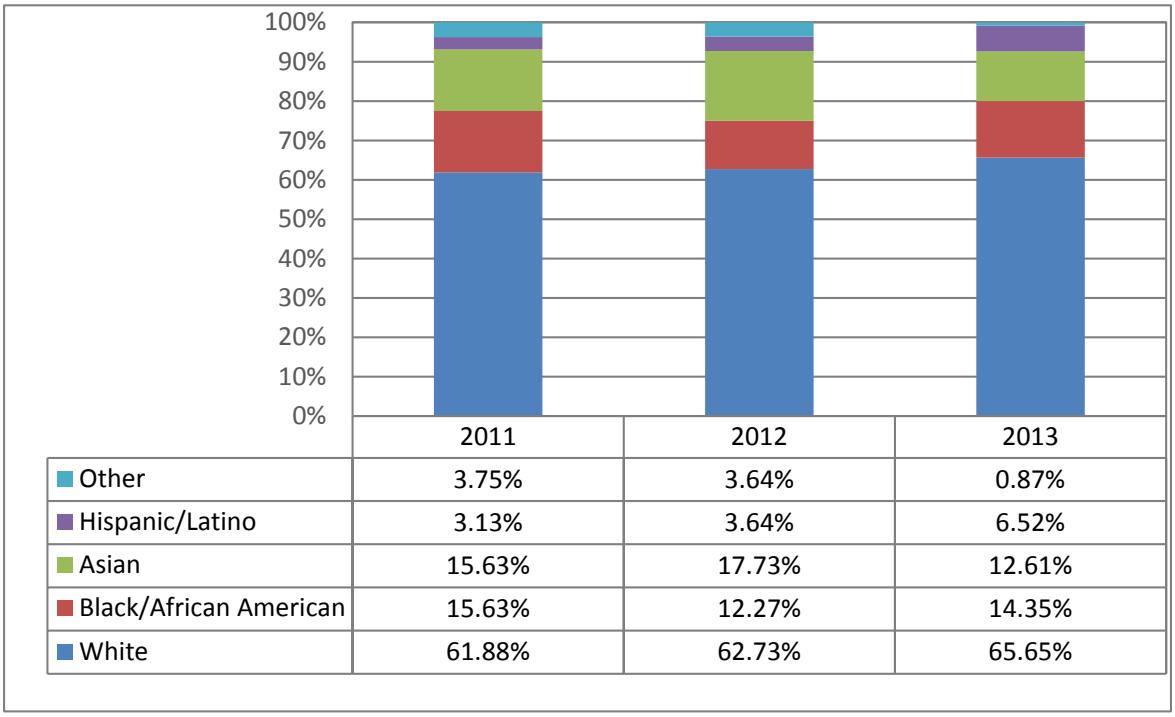
- 460 occurred in the *all other professional employees and all wage employees* category (FR-16 to FR-25 and WE-41 to WE-47)
- 144 occurred in the *mid-level professionals* category (FR-26–FR-28)
- 6 occurred in the *senior managers and officers* category (FR-29–00)[45]

As a percentage of the overall workforce during 2011–2013, female employees accounted for 44.89 percent of the workforce and received 42.13 percent of the career-ladder promotions. Male employees accounted for 55.11 percent of the workforce and received 57.87 percent of the career-ladder promotions.

44. U.S. Government Accountability Office, *Human Capital: Selected Agencies Have Opportunities to Enhance Existing Succession Planning and Management Efforts*, GAO-05-585, June 2005.

45. All six promotions were from FR-28 to FR-29.

Figure 7: Career-Ladder Promotions Awarded, by Race/Ethnicity, 2011–2013[a]



	2011	2012	2013
Other	3.75%	3.64%	0.87%
Hispanic/Latino	3.13%	3.64%	6.52%
Asian	15.63%	17.73%	12.61%
Black/African American	15.63%	12.27%	14.35%
White	61.88%	62.73%	65.65%

Source: OIG analysis of Board-provided data.

[a]*Other* includes (1) Native Hawaiian or Other Pacific Islander (Not Hispanic or Latino), (2) American Indian or Alaska Native (Not Hispanic or Latino), (3) Two or More Races/Ethnicities (Not Hispanic or Latino), and (4) Not Specified (i.e., individuals who chose not to disclose demographic data).

For additional information on the 2011–2013 career-ladder promotions by sex, race/ethnicity, and age within each pay grade category, refer to appendix G.

The Board Is in the Process of Implementing Its Formal Succession Planning Process

The Board developed a two-phase, formal agency-wide succession planning program in late 2012 to help identify a diverse pool of candidates for senior management positions throughout the Board. Phase 1 of the Board's process has been implemented in 8 of the 14 divisions and the OIG. The Board anticipates implementing phase 1 in the remaining 6 divisions by 2016. Phase 2 will begin by the end of 2015. Both phases are scheduled for full implementation by 2017.

GAO's *Diversity Management: Expert-Identified Leading Practices and Agency Examples* defines succession planning as

> a comprehensive, ongoing strategic process that provides for forecasting an organization's senior leadership needs; identifying and developing candidates who have the potential to be future leaders; and selecting individuals from among a diverse pool of qualified candidates to meet executive resource needs. . . . Succession planning and management can help an organization become what it needs to be, rather than simply recreate the existing organization.[46]

In addition, GAO reports that succession planning is also tied to the federal government's "opportunity to change" the diversity of its executives through new appointments.

Board officials informed the OIG that most divisions have performed some form of succession planning. For example, one Board division is developing a process to meet with every officer, manager, and supervisor to determine the developmental requirements for preparing a qualified replacement. Further, the division is developing key competencies for each pay grade and plans to identify training to complement these competencies. These steps are designed to guide staff members as they progress through the division's career ladder. Another division offers a robust staff development program that focuses on technical training and soft skills.[47] Aside from the Board's formal succession planning program, Board divisions have taken actions to develop staff members.

Succession planning is associated with opportunities to change diversity at the executive level.[48] Therefore, the establishment within the Board of a formal succession program may help the Board in its efforts to reach diversity and inclusion goals.

46. U.S. Government Accountability Office, *Diversity Management: Expert-Identified Leading Practices and Agency Examples*, GAO-05-90, January 14, 2005.

47. Soft skills include, but are not limited to, communication, self-awareness, motivation, social skills, and empathy.

48. U.S. Government Accountability Office, *Diversity Management: Expert-Identified Leading Practices and Agency Examples*, GAO-05-90, January 14, 2005.

Employee Complaints

Employees can raise grievances through the EEO and non-EEO processes. The Board has a defined EEO complaint process for applicants and Board employees who believe that they have been a victim of discrimination. The non-EEO process includes providing opportunities for employees to file and resolve grievances related to unfavorable performance ratings, unfair treatment, harassment, relationships with coworkers, and disciplinary actions.

This section provides a summary of the Board's processes and statistics related to EEO and non-EEO case data. We noted an opportunity for the Board to better communicate non-EEO case statistics to all divisions.

Related Laws and Regulations

Although not required by law, the Board follows several laws and regulations related to the EEOC and the processing of EEO complaints. In particular, the Board follows the requirements of the MD-715, which provides guidance and standards for establishing and maintaining effective EEO programs that ensure that all employees have equal opportunity without regard to race/ethnicity, color, religion, national origin, age, sex, or disability.[49]

The Board has also adopted, as part of its employment rules, EEO laws that prohibit discrimination, including the provisions of the No FEAR Act that require the Board to report and provide training on compliance with EEO laws and to post on its public website on a quarterly basis certain summary statistical data relating to EEO complaints.

The Board's Process for EEO Complaints

The Board's *Equal Employment Opportunity Policy*, revised May 13, 2013, provides for equal opportunity in employment for all persons and applies to, among other human resources–related functions, the EEO complaint process. The Board prohibits discrimination in employment on the basis of race/ethnicity, color, religion, sex, national origin, age, disability, or genetic information, and promotes the full realization of EEO through a continuing affirmative program. The Board also prohibits discrimination on the basis of any application, membership, or service in the uniformed services. In addition, as a matter of policy and although it is not required by law, the Board prohibits discrimination in employment on the basis of sexual orientation. An applicant or Board employee who believes that he or she has been discriminated against should consult with the OD&I within 45 days of becoming aware of the alleged discriminatory act or personnel action.

49. These programs are under of title VII, section 717, of the Civil Rights Act of 1964 and section 501 of the Rehabilitation Act of 1973.

Informal EEO Complaints

The informal process begins when an EEO counselor is assigned to conduct an initial counseling session with the complainant to obtain information about the alleged complaint. The EEO counselor then has 30 calendar days to make inquiries, attempt to resolve the matter, and advise the employee on the process to file a formal complaint. On a case-by-case basis, the EEO counselor may offer the complainant the right to engage in the alternative dispute resolution process. If counseling sessions or the alternative dispute resolution process cannot resolve the matter, or if a complaint in mediation is not resolved by the 90th day, the EEO counselor will issue a written notice to the complainant stating that it is the complainant's right to file a formal complaint within 15 days of receipt of the notice.

Formal EEO Complaints

If a formal complaint is filed, an EEO counselor will review the complaint and determine the issues that will be accepted for investigation. During the investigation stage, an independent investigator will be contracted to investigate the issues accepted in the complaint. At the close of the investigation, the OD&I will provide the complainant with an investigative report. On receipt of the investigative report, the complainant has 30 days to take one of the following courses of action:

- Request from the OD&I a final Board decision without a hearing; the Board has 60 calendar days to render a decision.

- Request a hearing and decision from an EEOC Administrative Judge, followed by a final decision by the Board.[50]

If a complainant does not agree with the final decision that has been rendered by the Board, the complainant may take the following courses of action:

- Appeal to the EEOC upon the Board's dismissal of, or its final decision on, a formal complaint within 30 calendar days of receipt of the Board's dismissal or final decision.

- File a civil action in U.S. district court within 90 calendar days of the Board's final decision or the EEOC's decision on appeal.

- If 180 days have elapsed since the filing of the formal complaint, request a hearing from an EEOC Administrative Judge.

- If 180 days have elapsed since the filing of the formal complaint or since the filing of an appeal with the EEOC, file a civil action in U.S. district court.

50. Employees who request a hearing before an EEOC Administrative Judge must notify the OD&I. The EEOC will appoint an EEOC Administrative Judge to hold the hearing. The Administrative Judge will make findings of fact and conclusions of law and will issue a decision. The Board will have 40 calendar days from the date it receives the Administrative Judge's decision to issue a final order informing the complainant of whether it will implement the decision. If the Board does not implement the Administrative Judge's decision, the complainant can file an appeal with the EEOC simultaneously with the issuance of the Board's final order.

Statistics

Informal EEO Complaints

From FY 2011 through FY 2013, the OD&I conducted 166 counseling sessions.[51] A counseling session is a conversation between an EEO staff member and a complainant. The number of counseling sessions for FY 2011–FY 2013 remained relatively steady. Specifically, there were 58 counseling sessions in FY 2011 and 54 counseling sessions each year in FY 2012 and FY 2013.[52]

Formal EEO Complaints

Overall, the total number of new formal EEO complaints was 8 in FY 2011, 11 in FY 2012, and 2 in FY 2013.[53] Of the 21 new complaints filed during FY 2011–FY 2013, the most common EEO issues were as follows:

- **Retaliation.** Federal law prohibits the removal, demotion, harassment, or otherwise retaliatory activity against employees because they filed a charge of discrimination or because they complained to their employer about discrimination on the job.

- **Hostile work environment/harassment.** Hostile work environment or harassment is created by unwelcome conduct that is based on race, color, religion, sex, national origin, age, disability, or genetic information.[54]

- **Disparate treatment.** This prohibited treatment is apparent when an individual of a protected group is shown to have been singled out and treated less favorably than others who are similarly situated based on race, color, religion, sex, national origin, age, disability, or genetic information.

A complainant may file multiple issues in a single complaint.

51. The Board operates on a calendar-year basis; however, EEOC reporting requirements are based on a fiscal-year basis. Therefore, the OD&I reports counseling session data and EEO cases filed on a fiscal-year basis. Counseling sessions are counted, but to preserve anonymity, complainant identification data are not collected. As a result, the counseling session counts may include OIG personnel who are otherwise excluded from the data in this report.

52. Complainants may receive multiple counseling sessions; therefore, the number of counseling sessions per fiscal year may be greater than the number of complainants who sought counseling.

53. The OIG was excluded from this audit; therefore, we excluded OIG complaints. During this period, we noted that for the 21 complaints filed, there were 21 complainants.

54. Harassment becomes unlawful when (1) enduring the offensive conduct becomes a condition of continued employment or (2) the conduct is severe or pervasive enough to create a work environment that a reasonable person would consider intimidating, hostile, or abusive.

EEO Processing Time

The Board reports EEO complaint processing times as part of its No FEAR Act reporting. Investigations must be completed within 270 days, including extension, of the filing date of an individual complaint.[55] We noted that during FY 2011–FY 2013, the average number of days complaints were in the investigation stage rose sharply in FY 2013; however, the Board's average remained below the 270-day requirement. In addition, the average number of days that complaints were in the final action stage rose in FY 2012 and then declined in FY 2013 (table 7).[56]

Table 7: EEO Complaint Processing Times, FY 2011–FY 2013[a]

Complaint phase	Average number of days, FY 2011	Average number of days, FY 2012	Average number of days, FY 2013
Investigation	151	133	228
Final action	36	53	26

Source: The Board's *No FEAR Act Report*, September 18, 2014.

[a]Complaint processing times include data from all EEO complaints filed during FY 2011–FY 2013, including EEO complaints filed by the OIG.

The Board's Process for Non-EEO Matters

The Board's non-EEO process is initiated when a Board employee or an employee's supervisor contacts ER for advice or guidance. ER categorizes non-EEO matters into 21 categories that include performance, leave, attendance, or other workplace issues (such as perceived unfair or unprofessional treatment, concerns about promotions, or relationships with coworkers), and disciplinary actions.[57]

ER will provide one or more counseling sessions to help resolve a non-EEO issue. At any time during this counseling process, a Board employee or supervisor can choose to file a non-EEO case, which requires ER to take action aside from counseling, such as mediation. When this occurs, ER documents the action as a non-EEO case. Cases include employee complaints and adverse actions taken by the Board against an employee.

ER recorded 711 active non-EEO cases during 2011–2013, excluding the OIG. The majority of the cases were concentrated in four categories related to performance, work, leave, and disciplinary actions, which are defined as follows:

55. This requirement derives from *Management Directive 110*, which provides federal agencies with EEOC policies, procedures, and guidance relating to the processing of employment discrimination complaints governed by the EEOC's regulations in title 29, part 1614, of the *Code of Federal Regulations*.

56. When an Administrative Law Judge renders a decision, final action is required within 40 days of receipt of the hearing file and the Administrative Law Judge's decision. The Board's *Rules Regarding Equal Opportunity* delineates time frames for other circumstances and particular complaints.

57. For purposes of this report, performance issues include performance, performance management, and performance improvement. Categories that garnered fewer complaints include adverse action, disability, fit for duty, garnishment, harassment, Americans with Disabilities Act, selection, suitability, and other/miscellaneous.

- Performance issues include matters related to an employee's performance under the Board's performance management system.

- Work issues include employee complaints or questions regarding unfair treatment on the basis of conduct or reasons that do not adversely affect the employee's performance and that are not covered under existing laws regarding discrimination.

- Leave issues include an employee's failing to follow leave procedures, being tardy, and making false statements related to a leave request. Other leave complaints may include leave administration matters such as Family and Medical Leave Act requests.

- Disciplinary actions document oral counseling, a written warning, or a suspension of 14 calendar days or less. Disciplinary actions only address conduct-related problems and provide for disciplinary measures that are less severe than those outlined in the Board's *Adverse Action Policy* and associated procedures.

In general, ER works to resolve all non-EEO matters informally through counseling sessions or formally as a case between the employee and management within four to six weeks. Resolution time frames vary, however, based on the type of case.

The Board maintains non-EEO case data on a calendar-year basis. Overall, we noted that the number of active non-EEO cases as of year-end 2011, 2012, and 2013 were 232, 229, and 250, respectively.[58] We found that in 2011, the average processing time was 147 days; in 2012, 153 days; and in 2013, 155 days. In general, resolution time frames vary based on the type of case.

Finding: Non-EEO Case Statistics Were Not Provided to Divisions on a Regular Basis

We found that during 2011–2013, ER provided non-EEO case statistics to Board divisions only on request. According to ER, if it detected a pattern of non-EEO cases (i.e., three or more) in a specific division, it would typically address the issue by offering counseling or training to division officials to prevent future occurrences. We also noted that the HR division compiled aggregate statistics in an internal report each year; however, only the report containing 2013 data was distributed to the divisions in May 2014.[59]

One of ER's objectives is to identify emerging employee relations issues and trends that may affect employee morale and notify management of such issues in advance of any impact. ER's practice is to collect non-EEO case data, conduct trend analysis, and submit this information to Management Division officials and to divisions that specifically request this information. While we acknowledge that ER collected this information, this information was not disseminated to all Board divisions. Further, according to a Board official, there was no systematic process in place to distribute the annual HR report that contained aggregate non-EEO statistics to all divisions in the Board in 2011 and 2012.

58. Formal non-EEO cases are tracked in a centralized database by ER; one employee may have more than one formal case.

59. The Management Division publishes an annual internal HR operations report. This report includes the number of new hires, employee benefits, separations, and employee exit interview data, among other types of information.

Disclosure of non-EEO case statistics to all Board divisions will help the divisions to identify barriers and other issues related to harassment, unfair treatment, relationships with coworkers, disciplinary action, and unfavorable performance ratings that may relate to diversity and inclusion. In addition, sharing information with division officials may assist them in identifying any patterns. Communicating non-EEO case data to all divisions can help to mitigate similar occurrences and assist in developing improvement strategies.

Management Actions

ER provided Division Directors with a more detailed non-EEO trend statistics report in October 2014 with the intent of obtaining their feedback and suggestions for an ongoing information exchange. This was the first detailed report to be distributed to all Division Directors. ER intends to distribute non-EEO trend statistics on at least a quarterly basis.

Recommendation

We recommend that the Chief Human Capital Officer

4. Ensure that aggregate non-EEO case statistics are provided to all Division Directors and that division-specific statistics are provided to the respective Division Director.

Management's Response

The Board concurs with our recommendation. In its response, the Board notes that management began providing Division Directors with non-EEO trend statistics and plans to continue this practice on a quarterly basis.

OIG Comment

The actions described by the Board are responsive to our recommendation. We plan to follow up on the Board's actions to ensure that the recommendation is fully addressed.

Employee Surveys

According to GAO, involving employees in diversity management efforts helps drive diversity throughout an organization. Employee surveys provide an opportunity for employees to share with management their perceptions of the agency's diversity and inclusion, culture, and work environment.[60]

This section presents information on the Board's efforts to obtain employee feedback. Specifically, we provide the Board's practices on satisfaction and exit surveys as well as demographic information regarding separations from the Board during the 2011–2013 period.

The Board's Process

The Board did not conduct agency-wide employee satisfaction surveys during the 2011–2013 period. On September 4, 2014, an external consulting firm administered the Board's first agency-wide engagement survey. Eighty-seven percent, or 2,147 employees, responded to the survey in its entirety. The survey included the three questions below, which were designed to gather data specifically related to employee perceptions of diversity and inclusion. Employees were asked to rate their responses as *strongly agree*, *agree*, *neutral*, *disagree*, or *strongly disagree*. As detailed below, 64 percent to 75 percent of respondents answered either or *strongly agree* or *agree* to the three questions.

Diversity and inclusion question	% responding *strongly agree* or *agree*
My organization's policies promote fair treatment of employees regardless of their different diversity characteristics.	75
My organization values employees with varied backgrounds and experiences.	67
My organization is committed to promoting diversity and inclusion.	64

The Board is continuing to assess the results of the 2014 survey and will determine what, if any, action plans are needed. These action plans will help to determine the timing of the next survey. We were also informed that the Board may consider conducting a diversity and inclusion survey once the agency-wide survey results have been thoroughly analyzed. These efforts will allow for trend analyses on the success of diversity initiatives as well as workplace inclusion.

60. U.S. Government Accountability Office, *Diversity Management: Expert-Identified Leading Practices and Agency Examples*, GAO-05-90, January 14, 2005.

We also noted that in 2013, two divisions independently conducted employee satisfaction surveys to obtain their employees' perspective on the particular division's work environment. Each survey contained one question specifically related to diversity and inclusion.

Although the Board did not conduct an agency-wide employee satisfaction survey in 2011, 2012, or 2013, ER offered separating employees the opportunity to voluntarily complete an electronic exit survey and participate in a face-to-face exit interview. ER collected the data and interview responses and prepared aggregate separation information for reporting in the HR section's internal annual report.

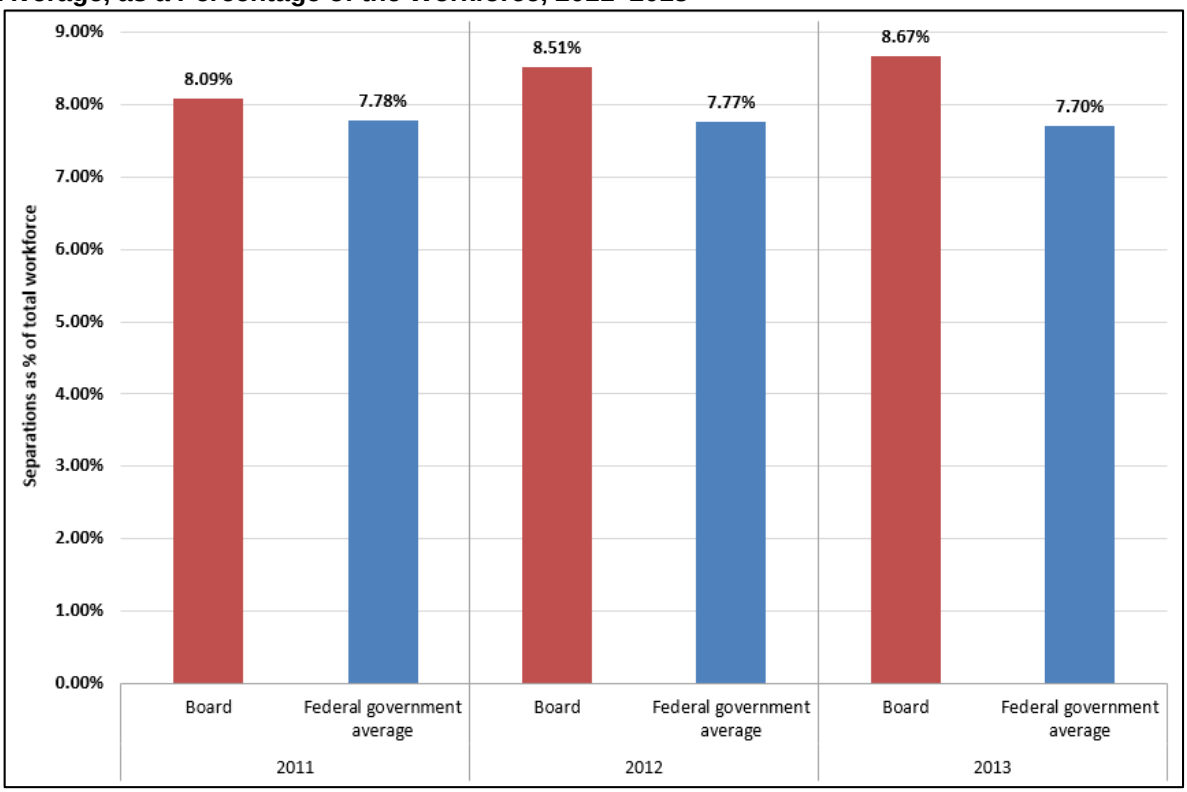
Demographic Statistics

Separations

We reviewed data for employees leaving the Board. Generally, the rate at which employees left Board employment was consistent with federal executive agencies during 2011–2013 (figure 8).[61]

61. The federal government average for separations was obtained from OPM's FedScope, which is a database that includes information on permanent employees who left the federal executive service (excluding the U.S. Postal Service). FedScope data are recorded on a fiscal-year basis; however, Board separation data are captured on a calendar-year basis. Therefore, an exact comparison could not be made. FedScope can be found at http://www.fedscope.opm.gov.

Figure 8: Separations (Including Retirements) From the Board and the Federal Government Average, as a Percentage of the Workforce, 2011–2013[a]



Source: OIG analysis of Board-provided data and OPM's FedScope data.

[a]OPM's FedScope data, which we used as a benchmark, are recorded on a fiscal-year basis; however, Board separation data are captured on a calendar-year basis rather than a fiscal-year basis. Both FedScope and Board separation data include retirements.

We analyzed the demographics of employees leaving Board service for reasons other than retirement. In 2011, 117 Board employees, or approximately 5 percent of the workforce, separated for reasons other than retirement. In 2012 and 2013, there were 139 and 138 nonretirement separations, respectively, accounting for approximately 6 percent of the workforce in both years.

Research assistants are considered permanent employees during their two-year tenure at the Board. Excluding research assistant separations, the Board's annual separation rate decreases by an average of 1.71 percent over the three years.

From 2011 through 2013, the number and percentage of female employees leaving Board service for reasons other than retirement remained relatively steady. Fifty-three female employees left the Board in 2011 and again in 2012, and 49 female employees left the Board in 2013. These separations represented 4.68 percent to 5.34 percent of the total female workforce.

With respect to race/ethnicity:

- In 2011, 12 Black/African American employees separated; in 2012, 20 Black/African American employees separated; and in 2013, 12 Black/African American employees separated. These separations represented 2.09 percent to 3.49 percent of the Black/African American workforce.

- In 2011, 16 Asian employees separated; in 2012, 13 Asian employees separated; and in 2013, 14 Asian employees separated. These separations represented 4.39 percent to 6.13 percent of the Asian workforce.

- In 2011, 4 Hispanic/Latino employees separated; in 2012, 5 Hispanic/Latino employees separated; and in 2013, 9 Hispanic/Latino employees separated. These separations represented 4.65 percent to 9.38 percent of the Hispanic/Latino workforce.

- In 2011, 83 White employees separated; in 2012, 98 White employees separated; and in 2013, 99 White employees separated. These separations represented 6.72 percent to 7.63 percent of the total White workforce.

Additional information on nonretirement separations by sex, race/ethnicity, and age can be found in appendix H.

The Board Has Begun Providing Employee Exit Survey Statistics to Divisions

Employees who separated from the Board are given the opportunity to voluntarily complete an exit survey and, separately, to participate in an exit interview. HR reported aggregate employee exit data for employees who separated in 2011 and 2012 in its 2013 annual report for its internal use; the aggregate data were provided to divisions only on request. For employees who separated in 2013, the aggregate employee exit data in HR's annual report were distributed to Board divisions in May 2014. The 2015 publication that will reflect 2014 aggregate employee exit data was being compiled at the time of our audit.

GAO's *Diversity Management: Expert-Identified Leading Practices and Agency Examples* suggests that one leading practice is to use quantitative and qualitative data derived from interviews, focus groups, and surveys to identify employee perceptions of the work environment and culture. Over time, trends in responses can help an organization assess progress in achieving organizational goals and objectives.

We noted that specific diversity and inclusion issues did not emerge in HR's annual reports; however, exit interview narratives documented that the most favorable aspects of working at the Board were colleagues, employee benefits, and work schedules. Interviewees indicated that the least favorable aspects included workload pressures, dissatisfaction with management, and frustration with having several layers of review of work and not being able to make decisions at lower levels of the organization. Board divisions can benefit from having access to agency-wide employee exit statistics and exit interview responses regardless of whether the division had

employees who separated, as that information may help inform the Board's continued efforts related to diversity and inclusion.

The Office of Diversity and Inclusion

The OD&I's mission is to ensure equal opportunity for all persons and to promote diversity relating to the Board's initiatives to employ, manage, and retain its human capital. This section discusses the OD&I's compliance with applicable provisions of the Dodd-Frank Act, the Board's application of the EEOC's MD-715 requirements, and the Board's compliance with provisions of the No FEAR Act as set forth in the Board's employment rules. It also presents the OD&I's organizational structure.

We found that the Board could benefit from finalizing its diversity strategic plan. We also found that the Board should formalize standards for equal employment opportunity and racial, ethnic, and gender diversity of the workforce and the senior management of the agency and ensure that No FEAR Act training is offered on a regular basis. In addition, we noted that the OD&I could enhance its communication to divisions on EEO matters and diversity initiatives. Finally, the OD&I should strengthen its internal controls for data collection and processing for MD-715 reporting.

Related Laws and Regulations

The Dodd-Frank Act required the Board to establish an OMWI. To satisfy this requirement, the Board established the OD&I in January 2011. The OD&I houses the preexisting EEO function; the Diversity and Inclusion section, which is responsible for programs for minorities, women, and other employees at the Board; and OMWI, which is responsible for implementing the applicable provisions of the Dodd-Frank Act related to financial education, supplier diversity, and regulated entities. The Director of the OD&I reports to the Board's Administrative Governor and to the Chief Operating Officer.[62]

The Board follows the EEOC's MD-715, which includes general reporting requirements that help an agency identify and eliminate any barriers that impede free and open competition in the workplace and prevent individuals of any racial or national origin group or either sex from realizing their full potential. As part of its annual MD-715 reporting, the Board reports its identification of barriers to equal employment opportunity and its plans to eliminate such barriers.

In addition, the Board has adopted provisions of the No FEAR Act and its implementing regulations[63] that require agencies to (1) post quarterly, on their public website, certain summary statistical data relating to EEO complaints filed under title 29, part 1614, of the *Code of Federal Regulations* and (2) notify current and former employees and applicants for federal employment of their rights and protections against discrimination. The No FEAR Act also requires each agency to develop a written plan for training all its employees, including supervisors and

62. The Federal Reserve Act authorizes the Board to delegate any of its functions, other than those pertaining to rulemaking or pertaining principally to monetary and credit policies, to members or employees of the Board, among others. As such, the Chairman delegated the responsibility for the OD&I to the Chief Operating Officer, who in turn delegated it to the Director of the OD&I.

63. 5 C.F.R. part 724.

managers. In response to the No FEAR Act's requirements, the Board developed the *No FEAR Act Written Training Plan*, which outlines how the Board will satisfy the No FEAR Act requirements. The plan includes, but is not limited to, providing training to all new Board employees within 90 days of employment and refresher training to Board employees.

The EEOC produces an *Annual Report on the Federal Workforce* that includes, among other data, information on federal EEO complaints and alternative dispute resolution activities. Similar to other federal agencies, the Board reports this information on the EEOC's Annual Federal Equal Employment Opportunity Statistical Report of Discrimination Complaints. Federal agency administrators upload data into the EEOC's Federal Sector EEO Portal, which is only accessible to authorized federal agency administrators.

Structure of the OD&I

An OD&I official explained that the OD&I's structure is based on its three functions:

- **Diversity and Inclusion—**OD&I staff members are responsible for the diversity and inclusion aspects of certain programs, such as recruiting, and for generating workforce trend data and providing this information to 13 of the 15 Board divisions.[64] In addition, a Diversity and Inclusion staff member is assigned as an official liaison to 12 Board divisions.[65] This section of the OD&I fulfills the Dodd-Frank Act requirements concerning minorities and women.

- **Equal Employment Opportunity—**OD&I staff members are responsible for handling the Board's EEO complaints and relevant reporting requirements, such as the annual MD-715 and No FEAR Act reports and the EEOC's Annual Federal Equal Employment Opportunity Statistical Report of Discrimination Complaints. In addition to EEO responsibilities, EEO staff members assist the Diversity and Inclusion section with generating workforce trend data and providing the data to the remaining two Board divisions, as well as assisting with diversity and inclusion programs. In addition, an EEO staff member is assigned as an official liaison to these two Board divisions.

- **OMWI—**OD&I staff members are responsible for activities related to the financial education of the community, such as minority and youth groups; the diversity of the Board's suppliers; and the standards for assessing the policies and practices of the entities supervised by the Federal Reserve Banks under delegated authority from the Board. These specific practices do not directly relate to diversity within the Board and are not addressed in this report.

Compliance With Dodd-Frank Act Requirements

We assessed the OD&I's activities for compliance with 10 requirements of section 342 of the Dodd-Frank Act that pertain to our audit objective. We found that the OD&I complies with 9 of the 10 requirements and partially complies with 1 requirement, as shown in table 8.

64. The OIG is included in the 15 divisions.

65. The OD&I does not provide a liaison to the Office of the Chief Operating Officer because the OD&I is part of that division.

Table 8: The Board's Compliance With Relevant OMWI Requirements of Section 342 of the Dodd-Frank Act[a]

Relevant[a] OMWI requirements applicable to the Board	Fully satisfies	Partially satisfies
The Director of each Office shall be appointed by, and shall report to, the agency administrator.	✓	
Each Director shall develop standards for equal employment opportunity and the racial, ethnic, and gender diversity of the workforce and senior management of the agency:		✓
Each Office shall submit to Congress an annual report regarding the actions taken by the agency and the Office pursuant to this section, which shall include		
the successes achieved and challenges faced by the agency in operating minority and women outreach programs	✓	
the challenges the agency may face in hiring qualified minority and women employees and contracting with qualified minority-owned and women-owned businesses; and	✓	
any other information, findings, conclusions, and recommendations for legislative or agency action, as the Director determines appropriate.	✓	
Each agency shall take affirmative steps to seek diversity in the workforce of the agency at all levels of the agency in a manner consistent with applicable law. Such steps shall include		
recruiting at historically black colleges and universities, Hispanic-serving institutions, women's colleges, and colleges that typically serve majority minority populations;	✓	
sponsoring and recruiting at job fairs in urban communities;	✓	
placing employment advertisements in newspapers and magazines oriented toward minorities and women;	✓	
partnering with organizations that are focused on developing opportunities for minorities and women to place talented young minorities and women in industry internships, summer employment, and full-time positions;	✓	
any other mass media communications that the Office determines necessary.	✓	

Source: OIG analysis of the Board's *Annual Report to Congress on OMWI*, OIG interviews with OMWI officials, Board policies and procedures, and section 342 of the Dodd-Frank Act (12 U.S.C. § 5452).

[a]We only analyzed the Dodd-Frank Act requirements that pertained to the scope of our audit.

The OD&I submitted annual reports to Congress for 2011, 2012, and 2013, which outlined its activities, successes, and challenges. The OD&I focused on agency diversity issues by partnering

with the six Board employee advisory committees that deal with gender, race/ethnicity, and diversity.[66]

In addition, Board officials indicated that the OD&I participates in divisions' recruiting efforts and in national diversity recruiting events by sharing the costs associated with career fairs and attending affinity group[67] engagements hosted by professional minority organizations. We also noted that the OD&I is involved with the hiring of Board officers, as detailed in the Recruiting and Hiring section of this report. However, the Director of the OD&I has not formalized standards for equal employment opportunity and the racial, ethnic, and gender diversity of the workforce and the senior management of the agency.

Finding: The Board Needs to Finalize Its Diversity and Inclusion Strategic Plan

We found that the Board has not finalized its diversity and inclusion strategic plan. Board officials, including those within the OD&I, were in the process of developing this plan during our audit. The Board's *Strategic Framework 2012–15* states,

> OD&I is working with Human Resources and Procurement staff at the Board to (1) ensure a commitment to recruit and retain a staff that is diverse and inclusive and (2) develop standards and procedures to ensure, to the extent possible, the fair inclusion and utilization of minority and women-owned businesses in the Board's procurements.

The Board is developing its 2016–2019 strategic plan, which will include a component on diversity.

GAO's *Diversity Management: Expert-Identified Leading Practices and Agencies Examples* states that an agency's diversity strategy and plan should be developed and aligned with the organization's overall strategic plan. Further, GAO reports that one expert suggests that organizations link diversity to their overall strategic plan to ensure that diversity initiatives are not viewed as extras that could be vulnerable to cuts, for example, when funds are tight. An agency that incorporates diversity as part of its strategic plan can translate its diversity aspirations into a tangible practice and can foster a culture change that supports and values differences.

Implementation of a diversity and inclusion strategic plan tied to the Board's strategic plan would promote a culture of diversity and inclusion in achieving the Board's goals. The plan can also provide a base from which progress can be measured on the Board's diversity and inclusion objectives.

66. The six employee advisory groups are (1) Advisory Committee for People with Disabilities; (2) African American Employees Advisory Committee; (3) Asian Employees Advisory Committee; (4) FRB Woman's Program Advisory Committee; (5) Hispanic Employees Advisory Committee; and (6) Lesbian, Gay, Bisexual, Transgender, and Allies Employees Advisory Committee.

67. An *affinity group* is a group formed around a shared interest or common goal, to which individuals formally or informally belong.

Recommendation

We recommend the Director of the OD&I

5. Finalize and implement the Board's diversity and inclusion strategic plan and ensure that

    a. the plan incorporates the agency's overall diversity and inclusion objectives.

    b. key elements of the plan are included in the Board's 2016–2019 agency strategic plan.

Management's Response

The Board concurs with our recommendation. In its response, the Board states that it will finalize the diversity and inclusion strategic plan. In addition, the Director of OMWI is a member of the Board's 2016–2019 strategic plan workgroup and is ensuring that the key elements of the diversity and inclusion plan are included.

OIG Comment

The actions described by the Board appear to be responsive to our recommendation. We plan to follow up on the Board's actions to ensure that the recommendation is fully addressed.

Finding: The Board's Standards for Equal Employment Opportunity and Racial, Ethnic, and Gender Diversity Have Not Been Formalized

We found that the Director of the OD&I has not formalized the OD&I's standards for equal employment opportunity and racial, ethnic, and gender diversity of the workforce and the senior management of the agency, as required by section 342(b)(2)(A) of the Dodd-Frank Act. Although the OD&I's diversity efforts are guided by federal government EEO requirements, it has not formalized a set of standards as required by the Dodd-Frank Act.

As a benchmarking exercise, we reviewed the standards of another financial regulatory agency's OMWI that were documented in the agency's overall diversity and inclusion strategic plan. In developing standards, the OMWI used the agency's strategic plan, annual performance budget information, the *Federal Equal Employment Opportunity Recruitment Plan*,[68] and the MD-715. Following best practices, the financial regulatory agency's diversity and inclusion strategic plan contains standards that include the agency's attestation of, commitment to, and definition of diversity and inclusion, as well as the agency's goals, implementation measures, priorities, and actions to satisfy Dodd-Frank Act requirements and to enhance diversity and inclusion within the agency.

68. The *Federal Equal Employment Opportunity Recruitment Plan* provides statistical data on employment in the federal workforce and highlights human capital practices that federal agencies are using to recruit, develop, and retain talent.

Since 1995 and prior to the creation of the OD&I, the Board sponsored EEO and affirmative action programs that included promoting diversity in its employment practices. The OD&I considers elements of these legacy programs, as well as the EEOC guidance used for MD-715 reporting, as its Dodd-Frank Act–required standards.

Formalizing standards can increase the transparency of the OD&I's diversity processes and practices and the way in which it plans to meet its internal objectives, monitor its progress, and meet its long-term goals. Without formalized standards, the Board is only partially compliant with the Dodd-Frank Act and may be limited in its ability to evaluate its effectiveness in promoting equal employment opportunity and diversity within its workforce and senior management.

Recommendation

We recommend that the Director of the OD&I

6. Formalize the standards the OD&I relies on for equal employment opportunity and the racial, ethnic, and gender diversity of the workforce and the senior management of the agency.

Management's Response

The Board concurs with our recommendation. In its response, the Board states that it plans to formalize the standards the OD&I relies on for equal employment opportunity and the racial, ethnic, and gender diversity of the workforce and the senior management of the agency, which will be included in the diversity and inclusion strategic plan.

OIG Comment

The actions described by the Board appear to be responsive to our recommendation. We plan to follow up on the Board's actions to ensure that the recommendation is fully addressed.

Finding: The Board's EEO and Diversity Training Is Not Provided on a Regular Basis

We found that the OD&I does not provide training related to EEO and diversity to all employees on a regular basis. No FEAR Act training is required every two years. The Board provided No FEAR Act training in 2011; however, the OD&I did not retain any records pertaining to this training. No FEAR Act training, as described in the Board's *No FEAR Act Written Training Plan*, was not provided in 2013.

The OD&I is responsible for providing EEO, No FEAR Act, and diversity training. Internal and external guidance related to administering these trainings includes the following:

- The EEOC's MD-715 instructions identify the basic elements necessary to create and maintain a model EEO program. One element in the guidance advocates that all employees receive information about the EEO program through training on the EEO process and the protections afforded to employees, related policy statements, and reasonable accommodation procedures.

- GAO's *Diversity Management: Expert-Identified Leading Practices and Agencies Examples* states that diversity training can help an organization's employees increase their awareness and understanding of diversity as well as help employees develop skills to promote communication and increase productivity. Such training can provide employees with an awareness of individual differences—including cultural, work style, and personal presentation—and an understanding of how diverse perspectives can improve organizational performance. The GAO report also states that the effectiveness of diversity training efforts should be evaluated to help decisionmakers manage resources and help agencies improve results.

- The Board's *No FEAR Act Written Training Plan*, developed in response to OPM's July 2006 final rule implementing the No FEAR Act training requirements, outlines how the Board will satisfy the No FEAR Act requirements. The act requires federal agencies to train all new employees within 90 days of hire and provide training to all employees every two years. Training must inform employees of their rights and remedies under the federal antidiscrimination laws.

An OD&I official informed us that both EEO and diversity training were included in the No FEAR Act training that was required for all Board employees in 2014. In addition, the OD&I official indicated that the office provided customized EEO and diversity training based on trends or issues observed in particular divisions. Division officials we spoke with expressed an interest in having more guidance on the EEO complaint handling process.

In 2011, a Board contractor provided No FEAR Act training. According to an OD&I official, the vendor retained records of attendance using its own identification system and OD&I officials verified employees' completion of the training by matching Board employee identification numbers to those in the vendor's identification system. However, the OD&I did not retain records of this verification or of the training modules that were taught. The contract ended in 2011, and similar training was not offered Boardwide in 2013.

Providing No FEAR Act training—which includes both EEO and diversity and inclusion elements—on a regular basis can benefit the Board. For example, training on equal employment opportunity can inform employees who may wish to file EEO complaints and managers who handle such complaints, and it can assist the Board in establishing a model EEO program. Further, training on diversity and inclusion can help employees to understand how diverse perspectives can improve organizational performance. To ensure that the training accomplishes these goals, the Board will need to evaluate the effectiveness of the training offered and take steps to make improvements, as needed.

Management Actions

On October 27, 2014, the OD&I offered a web-based No FEAR Act training that was mandatory for all employees. Additional training modules were provided for supervisors, managers, and officers.

Recommendation

We recommend that the Director of the OD&I

7. Ensure that No FEAR Act training

    a. is offered on a regular basis.

    b. is tailored to the Board and includes EEO and diversity and inclusion topics in accordance with the Board's *No FEAR Act Written Training Plan.*

    c. is evaluated for effectiveness and that any improvements identified are incorporated into the training as needed.

    d. attendance records are retained.

Management's Response

The Board concurs with our recommendation. In its response, the Board states that it will continue to provide No FEAR Act training on a regular basis. In addition, it will explore methods to evaluate the training for effectiveness and to incorporate improvements as needed. Further, the Board will consider including provisions in its contract for the training that would require the vendor to provide the Board with evidence of employees' completion of the training.

OIG Comment

The actions described by the Board are generally responsive to our recommendation. While the Board will explore methods to evaluate the No FEAR Act training for effectiveness, we encourage the Board to tailor the program to the Board's workplace needs, as necessary. We also encourage the Board to retain evidence of employees' completion of the No FEAR Act training. We plan to follow up on the Board's actions to ensure that the recommendation is fully addressed.

Finding: The OD&I Can Improve Its Communication to Divisions on EEO Matters and Diversity Initiatives

Board division officials reported that they experienced varying levels of interaction with and guidance from the OD&I. Specifically, four divisions reported positive experiences with the

OD&I in regard to its EEO function and its diversity and inclusion activities. However, the remaining divisions communicated a variety of concerns that indicate perceived limits to the OD&I's value and impact, including not understanding the function of components within OD&I, the limited assistance available to managers and officers with respect to the EEO complaint process, and the OD&I's minimal involvement during the recruiting and hiring of specialized positions.

Further, one division expressed that it would like the OD&I to address developmental issues for women and minorities. Additionally, another division stated that it would like the OD&I to hold annual or biannual meetings with division management to, among other things,

- discuss Boardwide expectations and any planned diversity initiatives
- educate managers and officers on the Board's EEO program and expectations
- discuss how EEO counselors can assist managers and officers

The OD&I's objectives are to provide guidance to Division Directors, managers, and supervisors to help them resolve EEO matters as they arise and to participate in planning and implementing the divisions' EEO and diversity programs, including talent management, employee coaching, career development, recruitment, outreach, intern programs, and leadership development. However, these objectives do not fully address OD&I's roles and responsibilities, which will assist divisions in understanding the function of components within the OD&I.

According to an OD&I official, prior to the Dodd-Frank Act enactment, the EEO section and the Diversity and Inclusion section conducted outreach to the divisions. Although the Board established the OD&I to include an OMWI function in response to the Dodd-Frank Act requirements, according to the OD&I official, the OD&I has not significantly modified its approach because these activities were already being covered prior to the enactment of the Dodd-Frank Act.

We believe that the OD&I can further its objectives by enhancing communications with all Board divisions on EEO and diversity and inclusion efforts. This approach can also assist the OD&I in aligning its efforts to its objectives and better enable the office to ensure equal opportunity for all persons and to promote diversity relating to the Board's initiatives to employ, manage, and retain its human capital.

Management Actions

We were informed that the OD&I is developing a quarterly reporting tool for each division. The tool's purpose is to support the Board's strategic objectives and commitment to attract, hire, develop, promote, and retain a highly diverse workforce and to show each division's progress. The OD&I plans to implement this tool during the second quarter of 2015. The sharing and discussion of the quarterly reporting tool results with the divisions will provide the OD&I with an opportunity to clarify its roles and responsibilities and provide guidance and assistance to divisions.

Recommendations

We recommend that the Director of the OD&I

8. Document the roles and responsibilities of the OD&I and distribute them to all Board divisions.

9. Partner with divisions to cooperatively develop strategies and initiatives that will help advance diversity and inclusion throughout the Board.

10. Work with divisions to finalize and implement the quarterly reporting tool and establish a schedule to communicate the results for each division to the respective Division Director. The quarterly reporting tool should include diversity and inclusion activities for each division with clear objectives and corresponding measures.

Management's Response

The Board concurs with our recommendations. In its response, the Board states that it will take steps to increase the divisions' awareness of the OD&I's roles and responsibilities. In addition, the Board plans to implement a new quarterly reporting tool for divisions that will establish specific diversity and inclusion strategies and initiatives.

OIG Comment

The actions described by the Board are generally responsive to our recommendations. While we acknowledge that the OD&I's objectives are updated annually as part of the Board's budget process, the stated objectives do not fully address the OD&I's roles and responsibilities. A more comprehensive document may assist divisions in understanding the functions of the components within the OD&I. We plan to follow up on the Board's actions to ensure that the recommendations are fully addressed.

Finding: The OD&I's Controls for MD-715 Data Collection Should Be Strengthened

We analyzed the workforce data in the Board's human resources database and had difficulty reconciling the annual aggregated data to the information reported on the MD-715. We determined that the OD&I's process to filter the data used for the MD-715 report resulted in a limited overstatement of the number of promotions, separations, and new hires. Specifically, we found 20 duplicate entries, representing less than 1 percent of the 2,600 total entries in the promotions, separations, and new hires data in the Board's MD-715 report for 2011, 2012, and 2013. Although we identified a small number of errors in the MD-715 reporting, additional controls would help reduce the risk of significant errors occurring in the future.

Establishing appropriate internal controls helps agencies improve organizational effectiveness and accountability. GAO's *Standards for Internal Controls in the Federal Government* states that effective communications within the organization are needed to carry out internal controls and

other responsibilities. In addition to internal communications, agencies should ensure that there are adequate means of communicating with, and obtaining information from, stakeholders. Moreover, effective information management is critical to achieving useful and reliable communication of information.

Further, National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, outlines mandatory information security controls for federal information systems, including in the areas of data output reconciliation and error correction.

The OD&I's process for reporting certain data in the MD-715 report consists of querying, downloading, and filtering data provided by HR. During the 2011–2013 period, we found that the data collected were not validated against the employee electronic records stored in HR. We believe that the duplicate entries resulted from the lack of mutual understanding between the OD&I and HR of the underlying data needed to complete a line item in the MD-715 report and the lack of internal controls in the OD&I to validate the data. We noted fewer duplicate entries in 2013 due to better collaboration between the OD&I and HR.

While we understand that the error rate was less than 1 percent, a documented data gathering methodology can facilitate consistent reporting and reduce the risk of reporting errors, such as the duplicate entries noted in our analysis. During our audit, we were informed that the OD&I will hire a data specialist to assist with the MD-715 reporting process.

Recommendation

We recommend that the Director of the OD&I and the Director of the Management Division

11. Strengthen internal controls for reporting MD-715 data, to include

    a. documenting the methodology for extracting and filtering the appropriate data.

    b. verifying the accuracy and completeness of the data in the MD-715 report prior to submission.

Management's Response

The Board concurs with our recommendation. In its response, the Board states that it agrees that it is always useful to take steps to ensure that data are reported as completely and accurately as possible, and the Board states that it will take the recommended steps to enhance the data reporting process.

OIG Comment

The actions described by the Board are generally responsive to our recommendation. We plan to follow up on the Board's actions to ensure that the recommendation is fully addressed.

According to GAO, an agency with a diverse workforce that includes minorities and women in key positions benefits from multidisciplinary knowledge and skills that can help the organization better accomplish its mission and goals and increase innovation.[69] An agency that effectively manages its employees provides for equal opportunities, which is essential to attracting, developing, and retaining the most qualified workforce. GAO further states that when an organization's top leaders demonstrate the importance of diversity and inclusion initiatives, a clear message is sent about the organization's commitment to diversity management.

Prior to the enactment of the Dodd-Frank Act, which required the Board to establish an OMWI, the Board had established diversity and inclusion practices, followed the requirements of the EEOC's MD-715, and adopted provisions of the No FEAR Act. After the period under review, we noted that the Board took actions to change certain practices, including, but not limited to, adopting a more standardized process for recruiting officer positions; sharing a non-EEO trend statistics report with all divisions; providing mandatory, web-based No FEAR Act training; and developing a quarterly reporting tool to show each division's progress in supporting the Board's strategic objectives and commitment to attract, hire, develop, promote, and retain a highly diverse workforce.

Our audit results identified several opportunities for the Board to enhance its diversity and inclusion efforts. Such improvements may enable the Board to further realize the benefits of a diverse workforce and reaffirm its commitment to diversity and inclusion in the workplace. Our recommendations address issues in the following four areas:

Data Analysis and Reporting—The Board can enhance its efforts to monitor and analyze certain types of workforce data that can be used to identify diversity and inclusion trends. For example, the Board could more effectively collect demographic data on applicants for economist, research assistant, and officer positions to gain a better understanding of the diversity within applicant pools for these professions. Additionally, there is an opportunity for the Board to conduct additional analysis of its employees' performance ratings to identify any patterns that may relate to diversity and inclusion or to identify any differences that may indicate bias. We also noted that in areas with available statistics, such as non-EEO matters, the Board can provide this information on a regular basis to all divisions. Further, the Board can strengthen its controls for MD-715 data collection.

Communication and Training—The Board can benefit from communicating the roles and responsibilities for carrying out EEO and diversity and inclusion activities. The Board is developing a quarterly reporting tool to evaluate each division's progress toward achieving the Board's diversity and inclusion goals. This tool could be used to enhance communication between the divisions and the OD&I as well as the divisions' understanding of the OD&I's

69. U.S. Government Accountability Office, *Diversity Management: Trends and Practices in the Financial Services Industry and Agencies after the Recent Financial Crisis*, GAO-13-238, April 2013.

functions. The Board can also benefit from requiring No FEAR Act training on a regular basis, include both EEO and diversity components in the training, and maintain internal records of employee's completion of training. No FEAR Act training should be tailored to the agency and evaluated to determine its effectiveness. Moreover, regular, mandatory training can be used to increase organizational efforts to inform and educate management and staff and provide employees with an understanding of how diverse perspectives can improve organizational performance. Further, regular No FEAR Act training can facilitate the appropriate handling of EEO matters by management and staff.

Full Compliance With Relevant Dodd-Frank Act Requirements—The Board believes that elements of its legacy EEO program satisfy section 342(b)(2)(A) of the Dodd-Frank Act—which requires agencies to develop standards for equal employment opportunity and racial, ethnic, and gender diversity of the workforce and the senior management of the agency—and therefore has not formalized these standards. Formalizing standards can increase the transparency of the Board's diversity processes and practices and the way in which it plans to meet its internal objectives, monitor its progress, and meet its long-term goals. Additionally, with formalized standards, the Board can be in full compliance with the Dodd-Frank Act requirements.

Diversity Strategic Planning—The Board should finalize its diversity strategic plan and ensure that the Board's diversity and inclusion objectives are incorporated into the agency's broader strategic plan. As indicated by best practices, incorporating diversity and inclusion objectives into the agency-wide strategic plan will assist in ensuring that diversity and inclusion are viewed as essential to meeting the Board's strategic goals. Implementation of a diversity and inclusion strategic plan tied to the Board's strategic plan would promote a culture of diversity and inclusion in achieving the Board's goals. The plan can also provide a base from which progress can be measured on the Board's diversity and inclusion objectives.

It is important to note that while our report focuses on the Board's specific diversity and inclusion initiatives and human resources–related activities, initiatives and activities that are beyond the scope of our review also contribute to enhancing diversity and inclusion principles.

Appendix A
Congressional Request Letter

JEB HENSARLING, TX, CHAIRMAN

United States House of Representatives
Committee on Financial Services
Washington, D.C. 20515

MAXINE WATERS, CA, RANKING MEMBER

March 24, 2014

Inspector General Mark Bialek
Board of Governors of the Federal Reserve System
Office of Inspector General
20th and C Streets N.W.
Mail Stop 300
Washington, DC 20551

Dear Inspector General Bialek:

We write to request that the Office of the Inspector General (OIG) for the Board of Governors of the Federal Reserve System (FRS) review the agency's internal operations to determine whether any personnel practices have created a discriminatory workplace or otherwise systematically disadvantaged minorities from obtaining senior management positions.

Section 342 of the Dodd-Frank Wall Street Reform and Consumer Protection Act established an Office of Minority and Women Inclusion (OMWI) at most of the federal financial regulatory agencies, responsible for matters relating to diversity in management, employment, and business activities. Despite this statutory mandate, the Government Accountability Office (GAO) concluded in a report released last year that management-level representation of minorities and women among federal financial agencies and Federal Reserve Banks has not changed substantially from 2007 through 2011. In fact, across all federal financial regulators, agency representation of minorities was as low as 6 percent and dropped as low as zero percent at one of the Reserve Banks. In light of these findings and the concerns raised by employee performance evaluations at the Consumer Financial Protection Bureau (CFPB), we believe the OIG should work in cooperation with Federal Reserve System's OMWI Director to assess current personnel practices and make recommendations necessary to ensure full compliance with the law.

The 2013 GAO report, entitled "Trends and Practices in the Financial Industry and Agencies after the Recent Financial Crisis," documented the extremely poor representation of women and minorities in leadership positions within the financial services industry and among federal financial regulators. According to GAO, industry representation of minorities in 2011 was higher in lower-level management positions – approximately 20 percent – as compared to about 11 percent of senior-level manager positions.

While public attention is currently and justifiably focused on the CFPB, the most recent OMWI reports suggest the disparities impeding internal upward mobility for minorities may be endemic throughout all the agencies regulating the financial services industry. According to the Treasury Department's 2013 OMWI report, among its senior executive management, 86 percent are white men, compared to 7 percent Black men, 4 percent Hispanic men, and 3 percent Asian men. Among the agency's GS-15 employees, which serves as a pipeline to senior level management, white men are once again overrepresented at 86 percent, compared to 6 percent Black men, 2 percent Hispanic men, and 6 percent Asian men.

At the Federal Reserve, white men represent 50 percent of executive senior level managers, compared to just 28.7 percent represented by white women. Along ethnic categories, black and Hispanic men represent, respectively, roughly 5 percent and 1 percent of executive senior level managers. Black women represent roughly 6 percent and Hispanic women represent nearly 2 percent of senior managers.

According to the most recent information from the GAO, at the National Credit Union Administration (NCUA), whites represent 88 percent of senior level management positions, compared to 4 percent represented by blacks and 4 percent by Hispanics. At the Office of the Comptroller of the Currency (OCC), whites represent 82 percent of senior level managers, compared to 9 percent black and 5 percent Hispanic. Whites represent 89 percent of senior level management positions at the Securities and Exchange Commission, compared to 2 percent black and 5 percent Hispanic. Minorities appear to fair best at the Federal Housing Finance Agency, where whites represent 76 percent of senior level management positions, compared to 16 percent black and 8 percent Hispanic. However, more comprehensive analysis is still needed from the agency to fully assess the racial and gender employment of minorities in senior positions beyond the GAO's limited information.

Accordingly, we request that the OIG examine any employee complaints, formal or informal, related to personnel practices, workplace policies and the findings from any employee satisfaction surveys, whether conducted by the Federal Reserve System or an outside entity. If the OIG identifies any individuals or groups of individuals who have exhibited discriminatory behaviors or patterns of unfair or unequal treatment, we ask that the OIG provide recommendations about appropriate actions, including remedial training or removal from employment with the agency. Furthermore, we request that the OIG assess the agency's OMWI operations, and ensure corrective actions are taken within the agency with regard to employee compensation, rating systems, retention, and promotion of women and minorities.

Sincerely,

Appendix B
Scope and Methodology

The overall objective for this audit was to assess the Board's human resources–related functions and other efforts to provide for equal employment opportunities, including equal opportunity for minorities and women to obtain senior management positions, and for racial, ethnic, and gender diversity in the workforce. The scope of our audit included the Board's human resources–related operations affecting diversity and inclusion from January 2011 through December 2013. We also considered any changes that occurred during 2014.

We gained an understanding of the Board's human resources–related functions within our scope, which include recruiting and hiring, performance management, promotions and succession planning, complaints, and employee satisfaction surveys, by reviewing relevant Board policies and procedures and interviewing Board divisions responsible for performing these functions. Specifically, we met with officials from the OD&I and HR, as well as representatives from the economics-related divisions and the Legal Division, to discuss topics such as key personnel, roles and responsibilities, systems and applications, and policies and procedures.

We identified Board policies and procedures related to recruiting and hiring, employee complaints, and performance management, as well as guidance and best practices related to diversity and inclusion. We reviewed relevant Board policies and procedures to identify internal controls that may prevent or detect bias or discrimination. The Board has a limited number of policies related to its human resources–related functions. As a result, we selected two internal controls related to preventing or detecting discrimination or bias in the performance management process to conduct compliance testing with policies and procedures.

We collected and analyzed data from HR to identify trend statistics related to the Board's workforce, recruiting and hiring, performance management, promotions, and separations. In addition, we analyzed data related to informal and formal EEO complaints and non-EEO complaints. We assessed the reliability of all the data we obtained to ensure that they were sufficiently reliable for the purposes of our analysis. As part of our data reliability evaluation, we observed the Board extract the data it provided us from the Board's centralized database of record for all of the human resources–related activities except for EEO complaints. We also obtained screenshots of the queries it used to extract the data. In the case of EEO complaints, we did not verify this information, as the Board informed us of the potential for privacy issues associated with the OIG's extracting or observing the extraction of these data; however, officials provided us with the summary data, and we attempted to use publicly available sources to verify the cases the Board provided us. After we determined that the data were reliable for the purposes of our audit, we analyzed the data based on sex, race/ethnicity, and age, where possible.

We examined workforce demographics agency-wide and by pay grade category. We also compared the workforce demographics data to the data from the ACS published by the U.S. Census Bureau, which serves as the primary external benchmark for comparing the sex and race/ethnicity composition of an organization's workforce. We examined the demographics of the applicants processed during each phase of the Board's hiring process.

For performance management, we coordinated with the four other federal financial regulatory agency OIGs that had received a similar congressional request to use the services of an external consulting firm. The external consulting firm analyzed, on an agency-wide basis, the Board's FY 2011, FY 2012, and FY 2013 performance ratings by gender, race/ethnicity, and age. The external consulting firm's analysis is provided in its entirety in appendix E of this report. In addition, we conducted an internal analysis of the performance ratings by division.

We analyzed data for career-ladder promotions, exit survey results, EEO complaints, non-EEO complaints, and Board separations. We assessed the Board's efforts (1) to respond to complaints or other potential indications of bias and (2) to increase diversity in management.

We evaluated the OD&I's role and involvement in monitoring (1) the impact of the Board's human resources–related policies on minorities and women and (2) the agency's efforts to increase diversity in senior management positions and within the agency. We reviewed documents and conducted interviews with OD&I officials to assess its efforts to respond to EEO complaints. We also reviewed documents, conducted interviews, and applied best practices to evaluate the OD&I's efforts as they relate to diversity and inclusion and the provision of training to management and staff. In addition, we reviewed Board documents and conducted interviews with OD&I officials to evaluate compliance with applicable sections of the Dodd-Frank Act.

Finally, we interviewed Board division officials to gain an understanding of the Board's challenges in achieving diversity throughout the agency and within senior management. Through these interviews, we sought to gain management's perspective on

- diversity challenges and strategies to enhance diversity and succession planning efforts for critical management positions
- division interactions with the OD&I
- the OD&I's role and involvement in monitoring the effect of the Board's human resources–related policies on minorities and women

We conducted our audit fieldwork from May 2014 to November 2014. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our finding and conclusions based on our audit objective.

Appendix C
Workforce Data

The tables below provide a breakdown of permanent employees based on sex, race/ethnicity, and age for 2011, 2012, and 2013.

Table C-1: Permanent Employees, by Sex, Race/Ethnicity, and Age, 2011–2013, and Demographic Breakdown of ACS Data, 2006–2010

Permanent workforce demographics	2011		2012		2013		ACS data
	Number	% of total workforce	Number	% of total workforce	Number	% of total workforce	% of total
Total permanent workforce	**2,187**	**100.00**	**2,279**	**100.00**	**2,353**	**100.00**	**100.00**
Sex							
Female	992	45.36	1,021	44.80	1,047	44.50	47.21
Male	1,195	54.64	1,258	55.20	1,306	55.50	52.79
Race/Ethnicity							
White	1,235	56.47	1,285	56.38	1,322	56.18	67.05
Black/African American	567	25.93	573	25.14	573	24.35	11.34
Asian	261	11.93	287	12.59	319	13.56	4.82
Hispanic/Latino	86	3.93	95	4.17	96	4.08	14.58
Other[a]	38	1.74	39	1.71	43	1.83	2.21
Age							
Under 40	927	42.39	983	43.13	1,032	43.86	N/A
40 or older	1,260	57.61	1,296	56.87	1,321	56.14	N/A

Source: OIG analysis of Board-provided data and the Census Bureau's ACS data.

Note: Percentages may not total 100 due to rounding.

[a]*Other* includes (1) Native Hawaiian or Other Pacific Islander (Not Hispanic or Latino), (2) American Indian or Alaska Native (Not Hispanic or Latino), (3) Two or More Races/Ethnicities (Not Hispanic or Latino), and (4) Not Specified (i.e., individuals who chose not to disclose demographic data).

Table C-2: Permanent Employees, Race/Ethnicity Distribution by Pay Grade Category, 2011–2013

Workforce by race/ethnicity and pay grade category	2011		2012		2013	
	Number	% of total workforce	Number	% of total workforce	Number	% of total workforce
Total permanent workforce	**2,187**	**100.00**	**2,279**	**100.00**	**2,353**	**100.00**
All others (FR-16–FR-25 and WE-41–WE-47)						
Asian	109	4.98	116	5.09	123	5.23
Black/African American	434	19.84	418	18.34	400	17.00
White	406	18.56	418	18.34	427	18.15
Hispanic/Latino	37	1.69	42	1.84	39	1.66
Other[a]	19	0.87	18	0.79	22	0.93
Total	**1,005**	**45.95**	**1,012**	**44.41**	**1,011**	**42.97**
Mid-level professionals (FR-26–FR-28)						
Asian	138	6.31	154	6.76	175	7.44
Black/African American	106	4.85	125	5.48	136	5.78
White	592	27.07	612	26.85	624	26.52
Hispanic/Latino	45	2.06	47	2.06	49	2.08
Other[a]	16	0.73	19	0.83	18	0.76
Total	**897**	**41.02**	**957**	**41.99**	**1,002**	**42.58**
Senior managers and officers (FR-29–00)						
Asian	14	0.64	17	0.75	21	0.89
Black/African American	27	1.23	30	1.32	37	1.57
White	237	10.84	255	11.19	271	11.52
Hispanic/Latino	4	0.18	6	0.26	8	0.34
Other[a]	3	0.14	2	0.09	3	0.13
Total	**285**	**13.03**	**310**	**13.60**	**340**	**14.45**

Source: OIG analysis of Board-provided data.

[a]*Other* includes (1) Native Hawaiian or Other Pacific Islander (Not Hispanic or Latino), (2) American Indian or Alaska Native (Not Hispanic or Latino), (3) Two or More Races/Ethnicities (Not Hispanic or Latino), and (4) Not Specified (i.e., individuals who chose not to disclose demographic data).

Table C-3: Permanent Employees, Sex Distribution by Pay Grade Category, 2011–2013

Workforce by sex and pay grade category	2011		2012		2013	
	Number	% of total workforce	Number	% of total workforce	Number	% of total workforce
Total permanent workforce	**2,187**	**100.00**	**2,279**	**100.00**	**2,353**	**100.00**
All others (FR-16–FR-25 and WE-41–WE-47)						
Female	497	22.73	490	21.50	488	20.74
Male	508	23.23	522	22.90	523	22.23
Total	**1,005**	**45.95**	**1,012**	**44.41**	**1,011**	**42.97**
Mid-level professionals (FR-26–FR-28)						
Female	380	17.38	409	17.95	424	18.02
Male	517	23.64	548	24.05	578	24.56
Total	**897**	**41.02**	**957**	**41.99**	**1,002**	**42.58**
Senior managers and officers (FR-29–00)						
Female	115	5.26	122	5.35	135	5.74
Male	170	7.77	188	8.25	205	8.71
Total	**285**	**13.03**	**310**	**13.60**	**340**	**14.45**

Source: OIG analysis of Board-provided data.

Table C-4: Permanent Employees, Age Distribution by Pay Grade Category, 2011–2013

Workforce by age and pay grade category	2011		2012		2013	
	Number	% of total workforce	Number	% of total workforce	Number	% of total workforce
Total permanent workforce	**2,187**	**100.00**	**2,279**	**100.00**	**2,353**	**100.00**
All others (FR-16–FR-25 and WE-41–WE-47)						
Under 40	529	24.19	541	23.74	559	23.76
40 or older	476	21.76	471	20.67	452	19.21
Total	**1,005**	**45.95**	**1,012**	**44.41**	**1,011**	**42.97**
Mid-level professionals (FR-26–FR-28)						
Under 40	366	16.74	409	17.95	441	18.74
40 or older	531	24.28	548	24.05	561	23.84
Total	**897**	**41.02**	**957**	**41.99**	**1,002**	**42.58**
Senior managers and officers (FR-29–00)						
Under 40	32	1.46	33	1.45	32	1.36
40 or older	253	11.57	277	12.15	308	13.09
Total	**285**	**13.03**	**310**	**13.60**	**340**	**14.45**

Source: OIG analysis of Board-provided data.

Appendix D
Recruiting and Hiring Data

Tables D-1 through D-4 provide the complete distribution of applicants based on sex and race/ethnicity for professional and wage employee and specialized positions of research assistants and economist. For each category under the candidate dispositions, the table provides the number and percentage of applicants that were referred and hired.

Table D-1: Recruiting and Hiring for Professional and Wage Positions, by Sex, 2011–2013

Candidate disposition by sex	2011		2012		2013	
	Number	% of applicants	Number	% of applicants	Number	% of applicants
Applicants						
Female	3,588	35.67	3,076	40.83	3,427	41.86
Male	5,413	54.19	3,600	47.79	3,824	46.71
Unknown	1,020	10.14	857	11.38	936	11.43
Total applicants	**10,059**	**100.00**	**7,533**	**100.00**	**8,187**	**100.00**
Referred						
Female	1,835	51.14	1,397	45.42	1,302	37.99
Male	2,709	49.70	1,720	47.78	1,763	46.10
Unknown	707	69.31	603	70.36	539	57.59
Total referred	**5,251**	**52.20**	**3,720**	**49.38**	**3,604**	**44.02**
Hired[a]						
Female	92	2.56	89	2.89	65	1.90
Male	140	2.57	110	3.06	89	2.33
Unknown	0	0.00	0	0.00	0	0.00
Total hired	**232**	**2.31**	**199**	**2.64**	**154**	**1.88**

Source: OIG analysis of Board-provided data.

[a]All individuals who were hired provided demographic data.

Table D-2: Recruiting and Hiring Distribution for Professional and Wage Positions, by Race/Ethnicity, 2011–2013

Candidate disposition by race/ethnicity	2011		2012		2013	
	Number	% of applicants	Number	% of applicants	Number	% of applicants
Applicants						
Asian	1,200	11.93	838	11.12	928	11.34
Black/African American	3,112	30.94	2,387	31.69	2,681	32.75
White	3,339	33.19	2,394	31.78	2,531	30.91
Hispanic/Latino	542	5.39	360	4.78	393	4.80
Other[a]	368	3.66	284	3.77	329	4.02
Unknown[b]	1,498	14.89	1,270	16.86	1,325	16.18
Total applicants	**10,059**	**100.00**	**7,533**	**100.00**	**8,187**	**100.00**
Referred						
Asian	515	42.92	353	42.12	354	38.15
Black/African American	1,508	48.46	1,037	43.44	1,141	42.56
White	1,856	55.59	1,253	52.34	1,091	43.11
Hispanic/Latino	264	48.71	170	47.22	173	44.02
Other[a]	173	47.01	120	42.25	138	41.95
Unknown[b]	935	62.42	787	61.97	707	53.36
Total referred	**5,251**	**52.20**	**3,720**	**49.38**	**3,604**	**44.02**
Hired[c]						
Asian	32	2.67	26	3.10	24	2.59
Black/African American	49	1.57	45	1.89	34	1.27
White	138	4.13	108	4.51	87	3.44
Hispanic/Latino	10	1.85	15	4.17	6	1.53
Other[a]	3	0.82	5	1.76	3	0.91
Unknown[b]	0	0.00	0	0.00	0	0.00
Total hired	**232**	**2.31**	**199**	**2.64**	**154**	**1.88**

Source: OIG analysis of Board-provided data.

[a]*Other* includes (1) Native Hawaiian or Other Pacific Islander (Not Hispanic or Latino), (2) American Indian or Alaska Native (Not Hispanic or Latino), and (3) Two or More Races/Ethnicities (Not Hispanic or Latino).

[b]*Unknown* includes individuals who chose not to disclose their demographic data.

[c]All individuals who were hired provided demographic data.

Table D-3: Recruiting and Hiring for Economists and Research Assistants, by Sex, 2011–2013

Candidate disposition by sex	2011		2012		2013	
	Number	% of applicants	Number	% of applicants	Number	% of applicants
Applicants[a]						
Female	525	10.67	830	13.04	149	2.73
Male	1,099	22.33	1,783	28.00	280	5.13
Unknown	3,298	67.01	3,754	58.96	5,024	92.13
Total applicants	**4,922**	**100.00**	**6,367**	**100.00**	**5,453**	**100.00**
Referred[b]						
Female	524	99.81	725	87.35	138	92.62
Male	1,096	99.73	1,547	86.76	253	90.36
Unknown	3,297	99.97	3,314	88.28	5,020	99.92
Total referred	**4,917**	**99.90**	**5,586**	**87.73**	**5,411**	**99.23**
Hired[c]						
Female	42	8.00	27	3.25	38	25.50
Male	74	6.73	58	3.25	74	26.43
Unknown	0	0.00	0	0.00	0	0.00
Total hired	**116**	**2.36**	**85**	**1.34**	**112**	**2.05**

Source: OIG analysis of Board-provided data.

[a]For the purposes of our review, multiple divisions may consider any candidate in the database for an economist or research assistant position. As a result, individuals were counted multiple times.

[b]An economist applicant is automatically referred to a hiring manager in all divisions that hire economists. Research assistants can be referred to a hiring manager in multiple divisions, once considered qualified.

[c]All individuals who were hired provided demographic data.

Table D-4: Recruiting and Hiring for Economists and Research Assistants, by Race/Ethnicity, 2011–2013

Candidate disposition by race/ethnicity	2011		2012		2013	
	Number	% of applicants	Number	% of applicants	Number	% of applicants
Applicants[a]						
Asian	429	8.72	695	10.92	61	1.12
Black/African American	63	1.28	97	1.52	26	0.48
White	974	19.79	1,451	22.79	301	5.52
Hispanic/Latino	128	2.60	303	4.76	19	0.35
Other[b]	21	0.43	45	0.71	15	0.28
Unknown[c]	3,307	67.19	3,776	59.31	5,031	92.26
Total applicants	**4,922**	**100.00**	**6,367**	**100.00**	**5,453**	**100.00**
Referred[d]						
Asian	429	100.00	604	86.91	54	88.52
Black/African American	61	96.83	81	83.51	19	73.08
White	972	99.79	1,257	86.63	283	94.02
Hispanic/Latino	128	100.00	275	90.76	17	89.47
Other[b]	21	100.00	39	86.67	13	86.67
Unknown[c]	3,306	99.97	3,330	88.19	5,025	99.88
Total referred	**4,917**	**99.90**	**5,586**	**87.73**	**5,411**	**99.23**
Hired[e]						
Asian	21	4.90	16	2.30	24	39.34
Black/African American	0	0.00	2	2.06	0	0.00
White	88	9.03	66	4.55	80	26.58
Hispanic/Latino	4	3.13	1	0.33	5	26.32
Other[b]	3	14.29	0	0.00	3	20.00
Unknown[c]	0	0.00	0	0.00	0	0.00
Total hired	**116**	**2.36**	**85**	**1.34**	**112**	**2.05**

Source: OIG analysis of Board-provided data.

[a]For the purposes of our review, multiple divisions may consider any candidate in the database for an economist or research assistant position. As a result, individuals were counted multiple times.

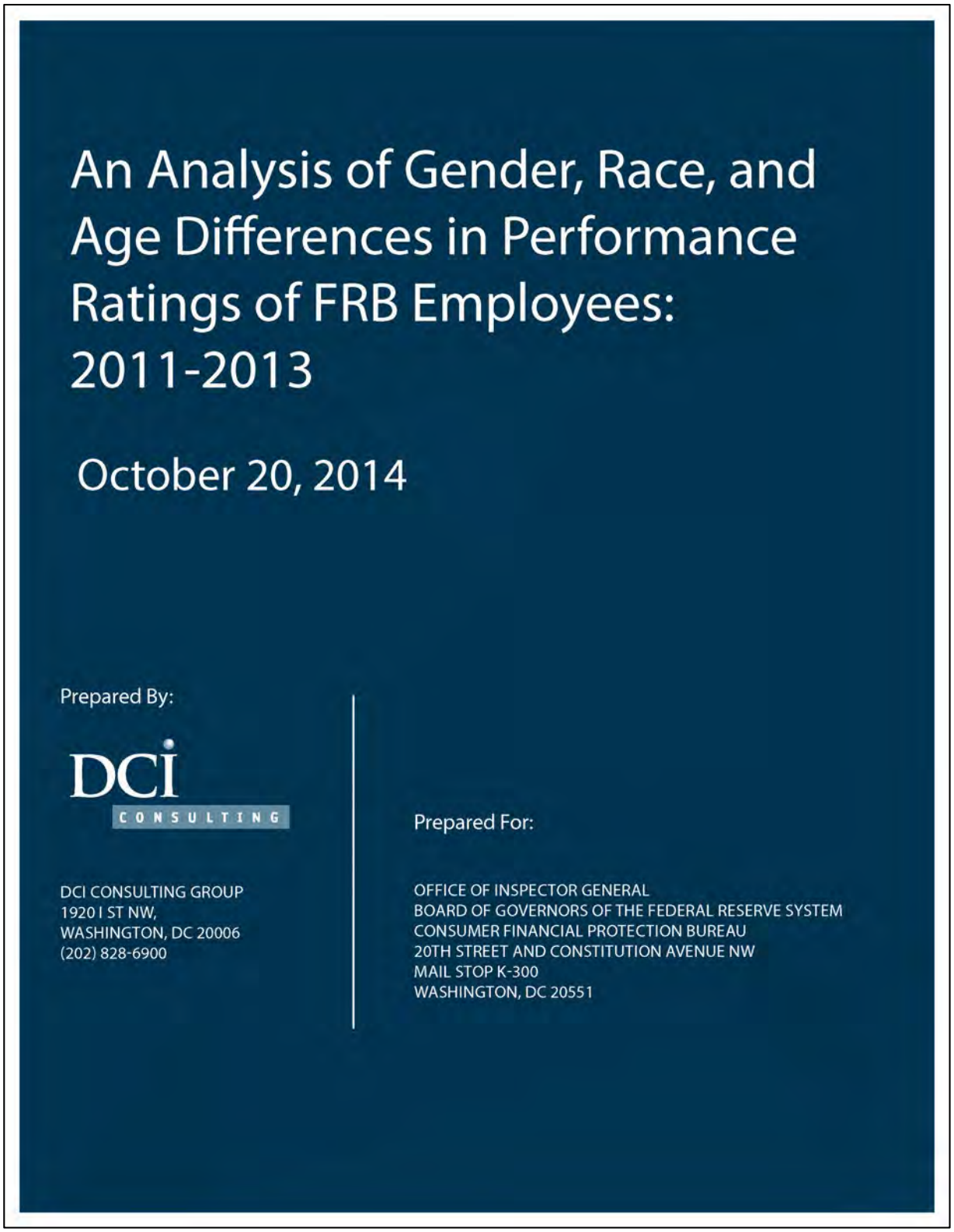
[b]*Other* includes (1) Native Hawaiian or Other Pacific Islander (Not Hispanic or Latino), (2) American Indian or Alaska Native (Not Hispanic or Latino), and (3) Two or More Races/Ethnicities (Not Hispanic or Latino).

[c]*Unknown* includes individuals who chose not to disclose their demographic data.

[d]An economist applicant is automatically referred to a hiring manager in all divisions that hire economists. Research assistants can be referred to a hiring manager in multiple divisions, once considered qualified.

[e]All individuals who were hired provided demographic data.

Appendix E
External Consulting Firm's Statistical Analysis of the Board's FY 2011, FY 2012, and FY 2013 Performance Ratings



An Analysis of Gender, Race, and Age Differences in Performance Ratings of FRB Employees: 2011-2013

October 20, 2014

Prepared By:

DCI CONSULTING

DCI CONSULTING GROUP
1920 I ST NW,
WASHINGTON, DC 20006
(202) 828-6900

Prepared For:

OFFICE OF INSPECTOR GENERAL
BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU
20TH STREET AND CONSTITUTION AVENUE NW
MAIL STOP K-300
WASHINGTON, DC 20551

Table of Contents

Executive Summary

On March 24, 2014, members of the United States House of Representatives Committee on Financial Services sent letters requesting that the Offices of Inspector Generals (OIGs) for seven financial regulatory agencies perform work to determine whether agency internal operations and personnel practices are systematically disadvantaging minorities and women from obtaining senior management positions. The Federal Reserve Board (FRB) was one of these agencies.

The OIGs initiated individual assignments with a general overall objective to assess agency personnel operations and other efforts to provide for equal employment opportunities, including equal opportunity for minorities and women to obtain senior management positions, and increase racial, ethnic and gender diversity in the workforce. One element of the work was for each OIG to assemble agency wide performance appraisal data to identify performance ratings distributions by gender, race/ethnicity, age and bargaining unit status (where applicable). This report presents the methodology and results of the analyses conducted for the OIG for the Board of Governors of the Federal Reserve System (FRB).

Separate analyses were conducted on overall performance ratings administered in 2011, 2012, and 2013. These analyses were conducted to detect potential performance rating differences based on gender, race/ethnicity and age. Analyses were conducted at a number of different job levels. Both statistical significance tests (e.g., t-tests) and effect sizes (e.g., d-scores) were evaluated to determine whether differences were meaningful. Standard social science criteria (e.g., alpha = .05) were used to interpret statistical significance, and effect sizes were compared to typical results found in the personnel selection research literature.

For gender data, males and females did not differ significantly in performance ratings at any level of analysis in any of the three years.

For the agency wide race/ethnicity data, Whites were rated significantly higher than African Americans and Asians in all three years, and were rated significantly higher than Hispanics in 2012 but not 2011 and 2013.

Lastly, for age data, younger workers were rated significantly higher than older workers at the mid-level jobs for all three years.

Statistically significant group differences do not necessarily indicate discrimination by themselves. Differences in performance ratings could be due to a wide variety of explanations. This report concludes with a number of measures that an agency can take to assess performance rating system content and process.

Introduction

Project Background

On March 24, 2014, members of the United States House of Representatives Committee on Financial Services sent letters requesting that the Offices of Inspector Generals (OIGs) for seven financial regulatory agencies perform work to determine whether agency internal operations and personnel practices are systematically disadvantaging minorities and women from obtaining senior management positions.[1] The agencies include the following:

- Federal Deposit Insurance Corporation (FDIC)
- Board of Governors of the Federal Reserve System (FRB)
- Consumer Financial Protection Bureau (CFPB)
- Office of the Comptroller of the Currency (OCC)
- Federal Housing Finance Agency (FHFA)
- National Credit Union Administration (NCUA)
- Securities and Exchange Commission (SEC)

The OIGs initiated individual assignments with a general overall objective to assess agency personnel operations and other efforts to provide for equal employment opportunities, including equal opportunity for minorities and women to obtain senior management positions, and increase racial, ethnic and gender diversity in the workplace. One element of the work was for each OIG to assemble agency wide performance appraisal data to identify performance ratings distributions by gender, race/ethnicity, age and bargaining unit status (applicable to all agencies except the FRB and FHFA). The FDIC Office of Inspector General (FDIC OIG) offered to engage and fund an independent contractor to perform statistical analyses of the performance appraisal results for each agency to determine whether there are statistically significant differences between groups of interest. DCI Consulting Group was selected to conduct these analyses for each of the agencies except for the Securities and Exchange Commission (SEC).

This report presents the methodology and results of the analyses conducted for the OIG for the Board of Governors of the Federal Reserve System (FRB).[2]

The FRB Performance Rating System

The performance management program at FRB serves as the basis for determining "pay-for-performance" amounts provided to employees. These increases take the form of *merit increases*, which affect employees' base salary and growth over time. Performance ratings may also be considered when determining variable pay or eligibility for additional incentive programs. Employees who receive lower ratings (i.e., unsatisfactory or marginal) may not be eligible for such increases.

---

[1] See the Appendix for a copy of this letter.
[2] DCI staff conducted all analyses and authored this report. Nothing in the report should be construed as representing the views of FRB OIG.

The distribution of performance ratings for 2011, 2012, and 2013 are depicted in Table 1. As presented, the lower the rating the better the performance. For purposes of exposition and consistency across agencies, these codes were reverse ordered so that higher ratings reflected better performance in the results section below. For example, a rating of 5 represents extraordinary performance in the results summarized in this report.

Table 1. Distribution of Performance Ratings

	Count			Percent		
Rating	2011	2012	2013	2011	2012	2013
1 – Extraordinary	378	429	480	19.13	20.27	22.39
2 – Outstanding	712	848	956	36.03	40.08	44.59
3 – Commendable	882	829	696	44.64	39.18	32.46
4 – Marginal	4	10	12	0.20	0.47	0.56
5 – Unsatisfactory	0	0	0	0.00	0.00	0.00

Method

Initial Dataset

FRB OIG provided DCI with data for 2011, 2012 and 2013. The performance time period covered for each year was from October 1st through September 30th. Relevant information for each year included:

- Performance Year
- EEO1 Category
- Job Function
- Job Level
- Salary Plan
- Overall Rating
- Rating Description
- Age
- Race/National origin
- Gender
- Whether the employee was 40 years of age or Older

The dataset for each year included all employees who were eligible for performance ratings. Although OIG employees are rated using the FRB system, they were not included in the dataset. Neither employee name nor employee number was included in the dataset.

Data Cleaning

The first step in the data cleaning process was to remove employees in the dataset who had not been with the agency long enough (90 days) to receive a performance rating. As it turned out, no employees were removed in any of the three years.

Race/Ethnicity Grouping

FRB OIG provided race/ethnicity grouping for analysis. Their coding scheme is presented in Table 2. If employees listed only one race/ethnicity (e.g., White, Asian), they were placed into that race/ethnicity category. If employees listed more than one race/ethnicity (e.g., Asian and White) were placed into the category of "Two or more".[3] Employees who did not identify their

[3] As shown in Table 2, the exception to this was that any employees identifying themselves as Hispanic, regardless of whether they listed any other races, were counted as Hispanic rather than "Two or More." There were no employees categorized as "Two or more" races. Note that employees self-identifying as "two or more" races or "other" are typically not included in any analysis, because those classifications could mean many different things, particularly due to the number of possible race combinations.

race/ethnicity were included in the gender and age analyses but were omitted from the race/ethnicity analyses.

Table 2. Race/Ethnicity From Dataset and Race/Ethnicity Analysis Groups

Analysis Grouping	Race/Ethnicity Categories in Dataset
White, Non-Hispanic (White)	• White • White, not of Hispanic origin • Not Hispanic in Puerto Rico
Asian (Asian)	• Asian
Black or African American (African American)	• Black or African American • Black, not of Hispanic Origin
Hispanic or Latino (Hispanic)	• Hispanic • Hispanic or Latino • Hispanic or Latino, American Indian or Alaska Native • Hispanic or Latino, Black or African American • Hispanic or Latino, Black or African American, White • Hispanic or Latino, White
Native Hawaiian or Other Pacific Islander (Native Hawaiian)	• Native Hawaiian • Other Pacific Islander
American Indian or Alaska Native (American Indian)	• American Indian • Alaska Native • American Indian/Alaska Native
Other	• Unknown

Age Grouping

FRB OIG also provided age groupings for analysis. Employees were placed into one of two categories: under 40 or 40+. These categories were chosen to be consistent with the Age Discrimination in Employment Act (ADEA). The category placement was based on the employee's age on the first day of the performance period for each of the three years. Table 3 depicts the race/ethnicity, gender, and age breakdown for each of the three years.

Table 3. Number of Employees by Gender, Race/Ethnicity, and Age

	Year		
Demographic Group	2011	2012	2013
TOTAL	1,976	2,116	2,144
Gender			
Female	917	960	973
Male	1,059	1,156	1,171
Race/Ethnicity			
White	1,087	1,184	1,185
Black or African American	546	550	554
Asian	229	259	280
Not Specified	3	2	2
Hispanic/Latino	79	87	88
American Indian/Alaskan Native	2	2	2
Native Hawaiian/Pacific Islander	1	2	0
Other (Unknown)	29	30	33
Age			
Under 40	778	881	893
40+	1,198	1,235	1,251

Data Integrity

To ensure the integrity of the data, two consultants reviewed the initial dataset. To ensure the accuracy of the statistical analyses, the analyses were conducted twice by separate consultants using different analysis programs (i.e., SAS, SPSS, Excel, HR Equator). These separate analyses yielded identical results.

Data Analysis Methodology

The OIGs for each agency agreed that the analyses would be conducted at two levels for all agencies: Overall and by bargaining unit status (where applicable). However, bargaining status was not a factor in the FRB data. Each agency then determined other levels of analysis that made sense for the agency. FRB OIG asked that analyses also be conducted by job level (senior managers, mid-level employees, and all other employees).

To compare the differences in the mean performance ratings across gender, race/ethnicity and age groups, tests of both statistical significance and practical significance were used.[4] Tests of

[4] Statistical analyses were only conducted when comparisons included 5 or more employees in each group. This decision was based on professional judgment. Small sample results are often non-representative, unstable and can change substantially with small changes in the data. Samples too small for analyses are labeled n/a in results tables.

statistical significance indicate the probability that the group difference could have been due to chance. A statistically significant result does not imply that a difference is good or bad or that it is large or small. Instead it simply indicates that the observed difference is probably not due to chance. In contrast, measures of practical significance provide an indication of the size of the difference.

To determine if the group differences were statistically significant, t-tests were used.[5] To assess statistical significance, DCI used two-tailed tests, which assess rating differences in both directions (e.g., differences that favor males as well as differences that favor females) and an alpha level of .05. Both standards are common in social science research. An alpha level of .05 indicates that the probability of a false positive (i.e., a statistically significant result that is incorrect) is 5 percent. This threshold for identifying a statistically significant difference generally corresponds to a t-value of 1.96 (although this value may vary slightly depending on sample size). Any t-value highlighted in the results tables was statistically significant at an alpha level of .05.

To determine practical significance, two measures were used: the percent differences between the two groups and d-scores. A d-score indicates the size of the difference in terms of standard deviations. That is, a d of 1.0 indicates that the two groups differed by a full standard deviation (a large effect) whereas a d of 0.10 indicates that the two groups differed by a tenth of a standard deviation (a small effect).

Table 4 will be helpful in interpreting the d-scores observed for FRB. The table summarizes a combination of d-scores obtained in a meta-analysis[6] by Roth, Huffcutt, and Bobko (2003)[7] on racial differences, a meta-analysis by McKay and McDaniel (2006)[8] on Black-White differences, a meta-analysis by Roth, Purvis, and Bobko (2012)[9] on gender differences, as well as internal research conducted by DCI. Thus, Table 4 represents the gender and race/ethnicity differences that are "typically found" in studies of performance appraisal differences. There have been no meta-analyses comparing performance ratings of employees over and under 40.

---

[5] For each comparison, we tested the assumption of equal variances between the two groups. If this test indicated unequal variances, a *t*-test for unequal variances was used (Welch's *t*-test). If the Welch's *t*-test changed the significance interpretation from that of the initial Student's *t*-test, the Welch's *t*-test value was listed in the table.

[6] A meta-analysis is a study that statistically combines the results of all previous studies conducted on a topic. These studies combine data over time (e.g., some source studies date back to the 1960s) and from a variety of jobs (e.g., blue collar and white collar) in different settings (e.g., private, public and military) to identify "typical" findings. In this context, the results of a meta-analysis are a series of effect sizes (d-scores) that provide a single source summary of previous research. Interested readers should refer to the references below for more information related to specific studies.

[7] Roth, P. L., Huffcutt, A. I., & Bobko, P. (2003). Ethnic group differences in measures of job performance: A meta-analysis. *Journal of Applied Psychology, 88*(4), 694-706.

[8] McKay, P. F., & McDaniel, M. A. (2006). A reexamination of Black-White mean differences in work performance: More data, more moderators. *Journal of Applied Psychology, 91*(3), 538-554.

[9] Roth, P. L., Purvis, K. L., & Bobko, P. (2012). A meta-analysis of gender group differences for measures of job performance in field studies. *Journal of Management, 38*(2), 719-739.

Table 4. "Typical" D-Scores Found in Performance Rating Studies

Comparison	Level of Analysis	
	Company Wide	By Title
Male – Female	-0.07	-0.08
White – Black	0.34	0.22
White – Hispanic	0.14	0.07
White – Asian	0.08	0.00

Note: Negative d-scores indicate females have higher ratings than men. D-scores computed by title reflect average performance differences between protected class subgroups within specific titles, rather than company-wide. Thus, analyses conducted by title are conducted at a finer level of analysis than are analyses conducted company wide, such that employees are more similar to one another in each cross-section of employees that are analyzed.

Analysis Results

Gender

Table 5 presents the results of gender analyses. There were no statistically significant gender differences in average performance ratings either agency wide or within the three job levels. This pattern was observed for all three years.

Race/Ethnicity

White to African-American Comparison

As depicted in Table 6, for 2013 the average performance ratings for Whites were higher than the average performance ratings for African Americans, at a statistically significant level, when evaluating ratings agency wide. However, when the data were analyzed by job level, there were no statistically significant White-African American differences in ratings. The effect size for the agency wide difference in 2013 (d= 0.23) was smaller than the value normally found for company-wide White-African American comparisons (which is d= 0.34).

In terms of statistically significant findings at the agency wide level, the pattern for 2012 and 2011 was identical to that of 2013: the average performance ratings for Whites were higher than the average performance ratings for African Americans, at a statistically significant level. The effect size for 2012 was d= 0.32 and for 2011 was d= 0.27, which is similar to the magnitude of differences reported in the research literature. The results for 2012 were also similar to those for 2013 in that there were no statistically significant differences once the data were analyzed by job level. In 2011, however, there was a statistically significant difference between average ratings of Whites and African Americans for the all other employee job level (d= 0.15).[10]

White to Hispanic Comparison

As depicted in Table 7, there were two statistically significant differences in the average performance ratings of Whites and Hispanics across all years and comparisons. In 2013, there was a statistically significant difference in favor of Hispanics at the senior manager level. This effect was in the opposite direction of what is typically found in the literature and was large (d=-0.77). However, it should be noted that this latter comparison included 247 Whites and only 7 Hispanics, and results should be interpreted with caution.

[10] One pattern that we were not asked to formally evaluate using statistics, but which is clear simply by evaluating the average ratings across the different job levels, is that employees at higher levels tend to receive higher performance ratings.

Table 5. Analysis Results - Gender Comparison

	Count		Avg Rating		Statistics		
Year/Unit of Analysis	M	F	M	F	t-value	% diff	d
2013							
Overall	1171	973	3.89	3.88	0.47	0.4	0.02
Level							
Sr Mgmt	186	127	4.32	4.42	-1.36	-2.3	-0.16
Mid-Level	529	399	3.91	3.90	0.26	0.3	0.02
Other	456	447	3.70	3.71	-0.15	-0.2	-0.01
2012							
Overall	1156	960	3.82	3.78	1.12	1.0	0.05
Level							
Sr Mgmt	178	115	4.38	4.33	0.58	1.1	0.07
Mid-Level	519	394	3.84	3.80	0.79	1.0	0.05
Other	459	451	3.58	3.62	-0.95	-1.3	-0.06
2011							
Overall	1059	917	3.74	3.74	0.20	0.2	0.01
Level							
Sr Mgmt	161	108	4.26	4.34	-0.96	-1.9	-0.12
Mid-Level	462	351	3.68	3.77	-1.85	-2.5	-0.13
Other	436	458	3.62	3.57	1.14	1.6	0.08

Note: Negative t-values indicate women received higher ratings than men

t-values highlighted in orange indicate that the t-value is statistically significant favoring women

t-values highlighted in gray indicate that the t-value is statistically significant favoring men

Table 6. Analysis Results - Race: White to African American Comparison

		Count		Avg Rating		Statistics		
	Year/Unit of Analysis	W	AA	W	AA	t-value	% diff	d
2013								
	Overall	1185	554	3.96	3.79	4.48	4.6	0.23
	Level							
	Sr Mgmt	247	37	4.37	4.27	0.86	2.3	0.15
	Mid-Level	584	129	3.95	3.86	1.20	2.2	0.12
	Other	354	388	3.71	3.72	-0.23	-0.3	-0.02
2012								
	Overall	1184	550	3.89	3.65	6.21	6.6	0.32
	Level							
	Sr Mgmt	243	27	4.37	4.37	0.03	0.1	0.01
	Mid-Level	584	119	3.84	3.79	0.73	1.4	0.07
	Other	357	404	3.65	3.56	1.66	2.5	0.12
2011								
	Overall	1087	546	3.82	3.62	5.13	5.6	0.27
	Level							
	Sr Mgmt	223	26	4.30	4.31	-0.08	-0.3	-0.02
	Mid-Level	533	103	3.73	3.75	-0.25	-0.5	-0.03
	Other	331	417	3.66	3.54	2.09	3.2	0.15

Note: Negative t-values indicate African Americans received higher ratings than Whites

t-values highlighted in orange indicate that the t-value is statistically significant favoring African Americans

t-values highlighted in gray indicate that the t-value is statistically significant favoring Whites

Table 7. Analysis Results - Race: White to Hispanic Comparison

Year/Unit of Analysis	Count W	Count H	Avg Rating W	Avg Rating H	Statistics t-value	Statistics % diff	Statistics d
2013							
Overall	1185	88	3.96	3.81	1.87	4.1	0.21
Level							
Sr Mgmt	247	7	4.37	4.86	-2.00	-10.1	-0.77
Mid-Level	584	43	3.95	3.77	1.54	4.8	0.24
Other	354	38	3.71	3.66	0.40	1.4	0.07
2012							
Overall	1184	87	3.89	3.71	2.15	4.9	0.24
Level							
Sr Mgmt	243	6	4.37	4.50	-0.45	-2.8	-0.19
Mid-Level	584	45	3.84	3.69	1.37	4.2	0.21
Other	357	36	3.65	3.61	0.32	1.2	0.06
2011							
Overall	1087	79	3.82	3.67	1.69	4.2	0.20
Level							
Sr Mgmt	223	4	4.30	n/a	n/a	n/a	n/a
Mid-Level	533	39	3.73	3.54	1.57	5.4	0.26
Other	331	36	3.66	3.67	-0.06	-0.2	-0.01

Note: Negative t-values indicate Hispanics received higher ratings than Whites

t-values highlighted in orange indicate that the t-value is statistically significant favoring Hispanics

t-values highlighted in gray indicate that the t-value is statistically significant favoring Whites

At the agency wide level in 2012, Whites received significantly higher performance ratings than Hispanics and the effect size exceeded what would be expected based on the research literature (d=0.24). However, there were no significant differences in performance ratings within any of the three job levels.

For 2011, there were no significant differences in performance ratings for Whites versus Hispanics at an agency wide level, and for either mid-level employees or all other employees. There were too few Hispanic senior managers (N=4) to make a comparison between White and Hispanic at the senior manager level.

White to Asian Comparison

As depicted in Table 8, Whites received significantly higher performance ratings than Asians at the agency wide level in 2013, and the effect size (d=0.22) was larger than the value normally found for company-wide White-Asian differences (d= 0.08). However, there were no significant differences in performance ratings within any of the three job levels.

This pattern was repeated for both 2012 and 2011, where Whites received significantly higher performance ratings than Asians (d= 0.22). However, as in 2013, there were no significant differences in performance ratings within any of the three job levels in either 2012 or 2011.

Age

As depicted in Table 9, there were no statistically significant differences in performance ratings between older and younger employees in 2013 at an agency wide level, for senior managers, or for all other employees. However, there was a significant difference in favor of younger employees for mid-level employees (d= 0.21).

In 2012, there was a statistically significant overall difference in performance ratings favoring older employees (d= -0.11). However, there were no significant differences in ratings for younger and older employees when looking at the senior manager or all other employee job level. Younger employees received significantly higher ratings than older employees for mid-level employees (d =0.13). This flip in the direction of the difference across unit of analysis is likely what statisticians refer to as a Simpson's paradox. This phenomenon occurs when aggregating data across levels while ignoring the distributions at particular levels produce misleading results (i.e., that older workers are significantly favored in the aggregate). In this case, a larger percentage of older workers were in senior executive roles compared to younger workers, where ratings were much higher than other job levels. As such the larger percentage of older workers at this level may be driving aggregate results.

For 2011, there were no significant differences in performance ratings between older and younger employees at an agency wide level, and the same was true for senior managers and all

other employees. However, there was a significant difference in favor of the younger employees for mid-level employees (d= 0.20).

Table 8. Analysis Results - Race: White to Asian Comparison

	Count		Avg Rating		Statistics		
Year/Unit of Analysis	W	A	W	A	t-value	% diff	d
2013							
Overall	1185	280	3.96	3.80	3.36	4.4	0.22
Level							
Sr Mgmt	247	20	4.37	4.25	0.80	2.8	0.19
Mid-Level	584	156	3.95	3.83	1.73	3.0	0.16
Other	354	104	3.71	3.65	0.67	1.5	0.07
2012							
Overall	1184	259	3.89	3.73	3.24	4.5	0.22
Level							
Sr Mgmt	243	15	4.37	4.07	1.73	7.6	0.46
Mid-Level	584	148	3.84	3.80	0.57	1.0	0.05
Other	357	96	3.65	3.55	1.19	2.8	0.14
2011							
Overall	1087	229	3.82	3.66	3.02	4.6	0.22
Level							
Sr Mgmt	223	13	4.30	4.15	0.73	3.4	0.21
Mid-Level	533	122	3.73	3.70	0.31	0.6	0.03
Other	331	94	3.66	3.52	1.56	3.9	0.18

Note: Negative t-values indicate Asians received higher ratings than Whites

t-values highlighted in orange indicate that the t-value is statistically significant favoring Asians

t-values highlighted in gray indicate that the t-value is statistically significant favoring Whites

Table 9. Analysis Results - Age Comparison

	Count		Avg Rating		Statistics		
Year/Unit of Analysis	<40	40+	<40	40+	t-value	% diff	d
2013							
Overall	893	1251	3.86	3.90	-1.23	-1.0	-0.05
Level							
Sr Mgmt	34	279	4.38	4.35	0.24	0.6	0.04
Mid-Level	394	534	4.00	3.84	3.18	4.0	0.21
Other	465	438	3.71	3.69	0.46	0.6	0.03
2012							
Overall	881	1235	3.75	3.84	-2.57	-2.2	-0.11
Level							
Sr Mgmt	34	259	4.47	4.34	1.05	2.9	0.19
Mid-Level	388	525	3.88	3.78	1.99	2.5	0.13
Other	459	451	3.59	3.61	-0.40	-0.5	-0.03
2011							
Overall	778	1198	3.72	3.75	-0.87	-0.8	-0.04
Level							
Sr Mgmt	34	235	4.32	4.29	0.27	0.8	0.05
Mid-Level	304	509	3.81	3.67	2.79	4.0	0.20
Other	440	454	3.61	3.57	0.83	1.1	0.06

Note: Negative t-values indicate those 40 years of age or older received higher ratings than those younger than 40 years of age
t-values highlighted in orange indicate that the t-value is statistically significant favoring those 40 years of age or older
t-values highlighted in gray indicate that the t-value is statistically significant favoring those younger than 40 years of age

Conclusions and Discussion

This report summarized the methodology and results of analyses related to subgroup differences on overall performance ratings administered in 2011, 2012, and 2013 at FRB. These analyses were conducted to detect potential performance rating differences based on gender, race/ethnicity and age. Analyses were conducted at a variety of levels of analysis. Both statistical significance tests (e.g., t-tests) and effect sizes (e.g., d-scores) were evaluated to determine whether differences were meaningful. Standard social science criteria (e.g., alpha = .05) were used to interpret statistical significance, and effect sizes were compared to typical results found in the personnel selection research literature.

The agency wide results across years indicate no pattern of statistically significant differences in average performance ratings between (a) women and men, (b) Hispanics and Whites, or (c) those age 40 or older and those younger than 40. In fact, there were no statistically significant gender differences, regardless of the level of analysis (i.e., overall or by organizational level). There were two statistically significant differences in average performance ratings between Hispanics and Whites, but they were not (a) at the same level of analysis (one was at the agency wide level and the other at the senior management level) or (b) in the same direction (one indicated higher average ratings for Hispanics and the other for Whites). Thus, in general, the overall results indicated no systematic differences in performance ratings for gender or White-Hispanic comparisons. With respect to age, a consistent pattern across years emerged at the mid-level jobs. The average performance ratings for employees younger than 40 were higher than those for employees age 40 or older, at a statistically significant level, but the effect sizes were not large.

With respect to agency wide performance differences between White employees and both Asian and African American employees, there is a trend of statistically significant differences in average ratings. In all three years, the average performance ratings for Whites were higher than those for Asians, at a statistically significant level. Similarly, in all three years, the average performance ratings for Whites were higher than those for African Americans, at a statistically significant level. The White-Asian differences were higher than that which is typically reported in the research literature, whereas the White-African American differences were lower than that which is typically reported in the research literature. It is notable that in the case of both White-Asian comparisons and White-African American comparisons, there is not a trend of statistically significant differences in performance ratings once the data are evaluated by job level.

Interpreting Statistically Significant Findings

It is important to understand that a statistically significant difference in ratings based on gender, race/ethnicity, or age does not necessarily indicate that discrimination is occurring. Such group differences could be due to actual differences in performance, regional differences in ratings, job family differences in ratings (i.e., supervisors in certain fields are more strict or lenient than supervisors in other fields) or some combination of all these factors.

To investigate whether any group differences are due to actual differences in performance or other factors rather than to discrimination, a number of measures could be taken to assess an agency's performance rating system process and content. These include verification that:

- The performance appraisal dimensions are job related;
- The performance appraisal system is adequately structured;
- Supervisors making the performance evaluations receive training;
- There is a system in place for management to review supervisor's performance ratings to determine if there are any patterns (e.g., racial or gender differences) that need to be reviewed;
- There is an appeal process for employees who believe their performance ratings are not accurate;
- There is a standardized, objective system for making employment decisions (e.g., merit increases, promotions) on the basis of the performance ratings;
- There is a well-developed feedback system through which employees can receive information about their performance that will promote their future development and enable them to improve job performance.

Potential Future Analyses

As described above, in cases where statistically significant differences exist, we generally recommend that the performance appraisal system be evaluated along the dimensions described above. In addition, a number of follow up analyses may be useful for interpreting results and gaining a clearer understanding of what factors may be driving those findings.

First, the analyses for this report were conducted at three job levels: senior managers, mid-level employees, and all other employees. It might be useful to conduct further analyses by such strata as salary band, region or location, and job title. In some instances, job level results may be further explained by more nuanced analyses and more granular levels.

Second, examining the interaction between the race/ethnicity and gender of the employee and the race/ethnicity and gender of the supervisor might also provide some insight into the statistically significant group differences. In some instances rater-ratee interactions may further explain results.

Third, because the analyses in this report focused on the overall rating, it might be informative to look at group differences in the initial element ratings, to determine whether a particular element could be driving results.

Fourth, it may be useful to analyze tangible employment outcomes that are directly or indirectly linked to performance ratings. For example, merit raises, bonuses and promotion decisions could

all be analyzed across the protected groups discussed in this report. This set of analyses could provide a broader perspective on equal employment opportunity outcomes across groups.

Note: We did not include appendix I of the external consultant's report, which is a copy of the congressional request letter. We include that letter as appendix A of this report.

Appendix F
Performance Management Data

In addition to the consultant's analysis on performance management data, we conducted our own analysis to determine the average performance ratings for each division by race/ethnicity (tables F-1 and F-2).

Table F-1: Average Performance Ratings, Race/Ethnicity Distribution by Division, 2011–2013

Average performance ratings by race/ethnicity	Division						
	Office of the Chief Operating Officer	Division of Financial Management	Division of Information Technology	Legal Division	Management Division	Office of the Staff Director	Office of the Secretary
2011							
Asian	[a]	[a]	2.35	2.29	2.29	N/A	N/A
Black/African American	[a]	[a]	2.33	2.62	2.34	2.32	2.39
White	[a]	[a]	2.24	2.22	2.14	2.08	2.25
Hispanic/Latino	[a]	[a]	2.17	N/A	2.50	N/A	2.50
Other[b]	[a]	[a]	1.83	N/A	2.25	N/A	N/A
2012							
Asian	[a]	1.88	2.29	2.29	2.18	[c]	N/A
Black/African American	[a]	2.57	2.38	2.43	2.35	[c]	2.32
White	[a]	2.04	2.29	2.10	2.17	[c]	2.00
Hispanic/Latino	[a]	N/A	2.17	N/A	2.41	[c]	N/A
Other[b]	[a]	N/A	2.33	N/A	2.25	[c]	N/A
2013							
Asian	N/A	2.25	2.15	2.38	2.13	[c]	N/A
Black/African American	2.30	2.43	2.38	2.33	2.13	[c]	2.36
White	2.00	2.12	2.16	2.07	2.04	[c]	2.00
Hispanic/Latino	N/A	N/A	2.00	N/A	2.00	[c]	2.33
Other[b]	N/A	N/A	2.17	N/A	2.11	[c]	N/A

Source: OIG analysis of Board-provided data.

Note: Analyses were only conducted when comparisons included more than five employees in each group. This decision was based on professional judgment; samples too small for analysis are labeled *N/A,* unless otherwise noted. The lower the average number, the higher the performance rating.

[a]The Office of the Chief Operating Officer and the Division of Financial Management were not established until 2012. Only two members of the Office of the Chief Operating Officer received a performance rating in 2012; therefore, the sample was too small for analysis.

[b]*Other* includes (1) Native Hawaiian or Other Pacific Islander (Not Hispanic or Latino), (2) American Indian or Alaska Native (Not Hispanic or Latino), (3) Two or More Races/Ethnicities (Not Hispanic or Latino), and (4) Not Specified (i.e., individuals who chose not to disclose demographic data).

[c]The Office of the Staff Director was not an established division in 2012 and 2013; therefore, performance rating results were not captured for those years.

Table F-2: Average Performance Ratings, Race/Ethnicity Distribution by Divisions With Economist Positions, 2011–2013

Race/Ethnicity and year	Division							
	Office of Board Members	Division of Banking Supervision and Regulation	Division of Consumer and Community Affairs	Division of International Finance	Division of Monetary Affairs	Office of Financial Stability Policy and Research	Division of Research and Statistics	Division of Reserve Bank Operations and Payment Systems
2011								
Asian	N/A	2.42	N/A	2.22	2.29	[a]	2.38	2.27
Black/African American	2.35	2.43	2.43	2.38	N/A	[a]	2.68	2.57
White	1.88	2.27	2.08	2.21	1.92	[a]	2.21	2.21
Hispanic/Latino	2.17	2.64	1.71	N/A	N/A	[a]	2.33	N/A
Other[b]	N/A	N/A	N/A	N/A	N/A	[a]	N/A	N/A
2012								
Asian	2.33	2.28	N/A	2.55	2.25	N/A	2.26	2.22
Black/African American	2.17	2.19	2.52	2.50	2.17	N/A	2.63	2.20
White	1.74	2.11	2.10	2.19	1.96	1.91	2.12	2.06
Hispanic/Latino	2.33	2.50	2.13	2.13	N/A	N/A	2.13	N/A
Other[b]	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
2013								
Asian	N/A	2.09	2.17	2.50	2.25	N/A	2.32	2.37
Black/African American	2.07	2.07	2.41	2.20	2.29	N/A	2.50	2.00
White	1.69	1.96	2.10	2.27	1.94	2.36	2.04	2.04
Hispanic/Latino	2.17	2.57	1.63	2.14	N/A	N/A	N/A	2.17
Other[b]	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Source: OIG analysis of Board-provided data.

Note: Analyses were only conducted when comparisons included more than five employees in each group. This decision was based on professional judgment; samples too small for analysis are labeled *N/A,* unless otherwise noted. The lower the average number, the higher the performance rating.

[a]The Office of Financial Stability Policy and Resarch was established in 2011. Only five staff members received performance ratings in 2011. Therefore, the sample was too small for analysis.

[b]*Other* includes (1) Native Hawaiian or Other Pacific Islander (Not Hispanic or Latino), (2) American Indian or Alaska Native (Not Hispanic or Latino), (3) Two or More Races/Ethnicities (Not Hispanic or Latino), and (4) Not Specified (i.e., individuals who chose not to disclose demographic data).

Appendix G
Career-Ladder Promotions Data

Tables G-1 through G-3 depict career-ladder promotions by grade based on sex, race/ethnicity, and age for 2011, 2012, and 2013. The tables do not include the pay grade category from which the employee was promoted.

Table G-1: Career-Ladder Promotions, Sex Distribution by Pay Grade Category, 2011–2013

Sex and pay grade category	2011		2012		2013	
	Number	% of promotions	Number	% of promotions	Number	% of promotions
All others (FR-16–FR-25 and WE-41–WE-47)						
Female	54	41.86	75	44.91	66	40.24
Male	75	58.14	92	55.09	98	59.76
Total	**129**	**100.00**	**167**	**100.00**	**164**	**100.00**
Mid-level professionals (FR-26–FR-28)						
Female	9	29.03	24	50.00	28	43.08
Male	22	70.97	24	50.00	37	56.92
Total	**31**	**100.00**	**48**	**100.00**	**65**	**100.00**
Senior managers and officers (FR-29–00)						
Female	0	0.00	1	20.00	0	0.00
Male	0	0.00	4	80.00	1	100.00
Total	**0**	**0.00**	**5**	**100.00**	**1**	**100.00**

Source: OIG analysis of Board-provided data.

Table G-2: Career-Ladder Promotions, Race/Ethnicity Distribution by Pay Grade Category, 2011–2013

Race/Ethnicity and pay grade category	2011		2012		2013	
	Number	% of promotions	Number	% of promotions	Number	% of promotions
All others (FR-16–FR-25 and WE-41–WE-47)						
Asian	21	16.28	32	19.16	20	12.20
Black/African American	25	19.38	22	13.17	24	14.63
White	74	57.36	103	61.68	110	67.07
Hispanic/Latino	5	3.88	5	2.99	9	5.49
Other[a]	4	3.10	5	2.99	1	0.61
Total	**129**	**100.00**	**167**	**100.00**	**164**	**100.00**
Mid-level professionals (FR-26–FR-28)						
Asian	4	12.90	7	14.58	9	13.85
Black/African American	0	0.00	5	10.42	9	13.85
White	25	80.65	30	62.50	40	61.54
Hispanic/Latino	0	0.00	3	6.25	6	9.23
Other[a]	2	6.45	3	6.25	1	1.54
Total	**31**	**100.00**	**48**	**100.00**	**65**	**100.00**
Senior managers and officers (FR-29–00)						
Asian	0	0.00	0	0.00	N/A	0.00
Black/African American	0	0.00	0	0.00	N/A	0.00
White	0	0.00	5	100.00	1	100.00
Hispanic/Latino	0	0.00	0	0.00	N/A	0.00
Other[a]	0	0.00	0	0.00	N/A	0.00
Total	**0**	**0.00**	**5**	**100.00**	**1**	**100.00**

Source: OIG analysis of Board-provided data.

[a]*Other* includes (1) Native Hawaiian or Other Pacific Islander (Not Hispanic or Latino), (2) American Indian or Alaska Native (Not Hispanic or Latino), (3) Two or More Races/Ethnicities (Not Hispanic or Latino), and (4) Not Specified (i.e., individuals who chose not to disclose demographic data).

Table G-3: Career-Ladder Promotions, Age Distribution by Pay Grade Category, 2011–2013

Age and pay grade category	2011		2012		2013	
	Number	% of promotions	Number	% of promotions	Number	% of promotions
All others (FR-16–FR-25 and WE-41–WE-47)						
Under 40	107	82.95	143	85.63	147	89.63
40 or older	22	17.05	24	14.37	17	10.37
Total	**129**	**100.00**	**167**	**100.00**	**164**	**100.00**
Mid-level professionals (FR-26–FR-28)						
Under 40	25	80.65	41	85.42	53	81.54
40 or older	6	19.35	7	14.58	12	18.46
Total	**31**	**100.00**	**48**	**100.00**	**65**	**100.00**
Senior managers and officers (FR-29–00)						
Under 40	0	0.00	1	20.00	1	100.00
40 or older	0	0.00	4	80.00	0	0.00
Total	**0**	**0.00**	**5**	**100.00**	**1**	**100.00**

Source: OIG analysis of Board-provided data.

Appendix H
Separations Data

Table H-1 illustrates separations, other than retirements, by sex, race/ethnicity, and age for 2011–2013.

Table H-1: Nonretirement Separations, by Sex, Race/Ethnicity, and Age, 2011–2013

Sex, race/ethnicity, and age	2011		2012		2013	
	Number	% of total workforce[a]	Number	% of total workforce[a]	Number	% of total workforce[a]
Total separations	**117**	**5.35**	**139**	**6.10**	**138**	**5.86**
Gender						
Female	53	5.34	53	5.19	49	4.68
Male	64	5.36	86	6.84	89	6.81
Race/Ethnicity						
Asian	16	6.13	13	4.53	14	4.39
Black/African American	12	2.12	20	3.49	12	2.09
White	83	6.72	98	7.63	99	7.49
Hispanic/Latino	4	4.65	5	5.26	9	9.38
Other[b]	2	5.26	3	7.69	4	9.30
Age						
Under 40	81	8.74	100	10.17	116	11.24
40 or older	36	2.86	39	3.01	22	1.67

Source: OIG analysis of Board-provided data.

[a]Percentage of the total demographic group in the workforce for that year.

[b]*Other* includes (1) Native Hawaiian or Other Pacific Islander (Not Hispanic or Latino), (2) American Indian or Alaska Native (Not Hispanic or Latino), (3) Two or More Races/Ethnicities (Not Hispanic or Latino), and (4) Not Specified (i.e., individuals who chose not to disclose demographic data).

Appendix I
Management's Response

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
WASHINGTON, DC 20551

OFFICE OF THE
CHIEF OPERATING OFFICER

DATE: March 30, 2015

TO: Mark Bialek, Inspector General

FROM: Don Hammond, Chief Operating Officer

SUBJECT: Response to March 19, 2015 Draft – "The Board Can Enhance Its Diversity and Inclusion Efforts"

Board staff has reviewed the above referenced draft report prepared by the Office of Inspector General ("OIG"). We appreciate the amount of work that went into the report and the opportunity to respond to its recommendations.

At the outset we would like to take the opportunity to emphasize that the Board is committed to increasing diversity and enhancing inclusion, and we believe that the evidence in the report shows some successes in that effort. For example, as noted in Figure 4 of the draft report, the representation of minorities in the Board's mid-level and senior level positions increased in each year under review. We believe this is a clear indication of this commitment.

Upon reviewing the draft report we consider it significant that the independent consultant who analyzed the Board's performance ratings concluded that there is "not a trend of statistically significant differences" in ratings based on race, gender, or age when the data are evaluated by job level.[1] Because performance ratings at the Board are not awarded on an agency-wide basis, agency-wide results do not provide useful information about whether employment discrimination may have occurred,[2] although the Board's agency-wide results are generally positive. The independent consultant concluded that the agency-wide results across years "indicate no pattern of statistically significant differences in average performance ratings between: (a) women and men, (b) Hispanics and Whites, or (c) those age 40 or older and those younger than 40," and that agency-wide White-African American differences were lower than those typically found in

[1] OIG draft report, dated March 19, 2015, entitled, "The Board Can Enhance Its Diversity and Inclusion Efforts," p.98 (Appendix E, "An Analysis of Gender, Race, and Age Differences in Performance Ratings of FRB Employees: 2011-2013").

[2] *See Wal-Mart Stores v. Dukes*, 131 S. Ct. 2541, 2555 (2011).

www.federalreserve.gov

studies of performance appraisal differences.[3] With respect to the more relevant job-level analyses, the independent consultant concluded that there is no trend of statistically significant differences between White and African American performance ratings when the data are analyzed at the job level.[4] Similarly, all White-Asian differences disappeared when the data were analyzed at the job level.[5] It is also important to keep in mind that, as stated in the independent consultant's analysis, differences in performance ratings could be due to a wide variety of explanations. The independent consultant also suggested a number of measures that could be taken to assess an agency's performance rating system process and content. Management will keep these in mind as we evaluate our performance appraisal system.

Although the Board's results are positive, management is fully committed to making further improvements in its diversity and inclusion efforts given the utmost importance of providing a work environment that is free of employment discrimination and that supports the engagement of all employees. In this regard we note that the OIG has recommended several additional improvements to the Board's diversity and inclusion efforts. Management generally agrees with the OIG's recommendations and, in a number of instances, has already implemented, or has begun to implement, changes to address them. Each OIG recommendation, and management's response, is discussed in more detail below.

OIG Recommendations and Management's Response

Recommendation 1: Develop and implement an alternative method for collecting the demographic data of economic and research assistant applicants to improve the response rate.

Management's Response: Management agrees with this recommendation and, as the OIG notes, in 2013, management began implementing a new process to automatically request self-disclosure of demographic information within 24 hours of obtaining an economist applicant's email address. Management will assess whether this change provides a significant improvement in response rates, and if not will consider other changes in order to obtain demographic data for economist and research assistant applicants.

Recommendation 2: Ensure that the demographic data for all internal and external officer applicants are maintained in the Board's centralized applicant database.

Management's Response: Management agrees with this recommendation and, as the OIG notes, in 2014, management implemented a process to track all officer positions through a centralized applicant database. This process will allow management to accumulate demographic data and measure trends in diversity at the officer-applicant

[3] *Id.*

[4] *Id.*

[5] *Id.* at 94.

level. Although this process does not currently fully capture applicant data when an executive search firm is used to recruit officer candidates, management plans to implement a process in the near future to capture this data.

Recommendation 3: Consider conducting annual analyses of the distribution of employee performance ratings to identify whether patterns exist that may indicate unfair or unequal treatment. If the analyses reveal patterns that may indicate unfair or unequal treatment, determine whether any actions are necessary.

Management's Response: Management agrees that a periodic analysis focused on areas where management has potential concerns may be useful. Management will consider establishing a process for identifying such areas and determining what type of statistical review would be warranted, and if statistically significant discrepancies are found from such analyses, will explore steps that may be appropriate to address those discrepancies. It is unclear whether the costs of paying for an annual statistical analyses on a Board-wide basis or even on the basis of job level provide corresponding value.

Recommendation 4: Ensure that aggregate non-EEO case statistics are provided to all Division Directors and that division-specific statistics are provided to the respective Division Director.

Management's Response: Management agrees with this recommendation and, as the OIG notes, in 2014 management began providing Division Directors with a non-EEO trend statistics report and we will continue to do so on a quarterly basis.

Recommendation 5: Finalize and implement the Board's diversity and inclusion strategic plan, and ensure that: (a) the plan incorporates the agency's overall diversity and inclusion objectives; and (b) key elements of the plan are included in the Board's 2016–2019 agency strategic plan.

Management's Response: Management agrees with this recommendation to finalize the diversity and inclusion strategic plan currently being developed, as noted in the OIG report. The OMWI Director is a member of the Board's 2016-19 strategic plan workgroup, ensuring that the key elements of the diversity and inclusion plan are included.

Recommendation 6: Formalize the standards the OD&I relies on for equal employment opportunity and the racial, ethnic, and gender diversity of the workforce and the senior management of the agency.

Management's Response: The standards will be formalized and incorporated in the diversity and inclusion strategic plan which is currently under development and scheduled for issuance in 2015.

Recommendation 7: Ensure that No FEAR Act training: (a) is offered on a regular basis; (b) is tailored to the Board and includes EEO and diversity and inclusion topics in accordance with the Board's *No FEAR Act Written Training Plan;* (c) is evaluated for effectiveness and that any improvements identified are incorporated into the training as needed; and (d) attendance records are retained.

Management's Response: Management agrees with this recommendation and notes that the Board has historically offered No FEAR Act training on a regular basis. Management recognizes that there was one instance in which No FEAR training was not offered during the planned year because of a procurement issue; the Board resolved this discrepancy by providing No FEAR Act training in October of 2014. Going forward, management agrees that it continues to be important to provide No FEAR Act training on a regular basis and to evaluate the training for effectiveness. Management also will explore methods of evaluating the effectiveness of training and incorporating improvements. Finally, while management has historically monitored employees to ensure they complete the training, management has not typically retained evidence of completion at the Board. Rather, such records have been held by the vendor that provides the training materials. The Board will consider providing in its contract for these services that the vendor provide the Board with evidence of employees' completion of training.

Recommendations 8-10: Document the roles and responsibilities of the OD&I and distribute to all Board divisions; Partner with divisions to cooperatively develop strategies and initiatives that will help advance diversity and inclusion throughout the Board; and work with divisions to finalize and implement the quarterly reporting tool and establish a schedule to communicate the results for each division to the respective Division Director. The quarterly reporting tool should include diversity and inclusion activities for each division with clear goals, objectives, and corresponding measures.

Management's Response: Management agrees with these recommendations; however, it should be noted that the mission and objectives of OD&I are updated annually as part of the Board's budget process. Management will take steps to increase the divisions' awareness of OD&I's role and responsibilities. Also, each division, has a designated EEO Officer as Liaison to OD&I. A new quarterly reporting tool for divisions aimed at establishing specific diversity and inclusion strategies and initiatives will be implemented in the second quarter. The new tool slated for the second quarter will strengthen the strategic direction of diversity and inclusion and provide transparency and accountability for achievement of objectives.

Recommendation 11: Strengthen internal controls for reporting MD-715 data, to include: (a) documenting the methodology for extracting and filtering the appropriate data; and (b) verifying the accuracy and completeness of the data in the MD-715 report prior to submission.

Management's Response: Although the very low error rate in reporting these data (less than 0.8 percent) suggests that data reporting errors were not a significant problem, management agrees that it is always useful to take steps to ensure that data are reported as completely and accurately as possible. Thus, management agrees to take the steps noted by the OIG to provide an enhanced data reporting process.

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU

HOTLINE

1-800-827-3340

OIGHotline@frb.gov

Report Fraud, Waste, and Abuse

Those suspecting possible wrongdoing may contact the OIG Hotline by mail, e-mail, fax, or telephone.

Office of Inspector General, c/o Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW, Mail Stop K-300, Washington, DC 20551
Attention: OIG Hotline

Fax: 202-973-5044

Questions about what to report?

Visit the OIG website at www.federalreserve.gov/oig
or
www.consumerfinance.gov/oig

Federal Reserve Act

Print

Section 10. Board of Governors of the Federal Reserve System

1. Appointment and qualification of members

The Board of Governors of the Federal Reserve System (hereinafter referred to as the "Board") shall be composed of seven members, to be appointed by the President, by and with the advice and consent of the Senate, after the date of enactment of the Banking Act of 1935, for terms of fourteen years except as hereinafter provided, but each appointive member of the Federal Reserve Board in office on such date shall continue to serve as a member of the Board until February 1, 1936, and the Secretary of the Treasury and the Comptroller of the Currency shall continue to serve as members of the Board until February 1, 1936. In selecting the members of the Board, not more than one of whom shall be selected from any one Federal Reserve district, the President shall have due regard to a fair representation of the financial, agricultural, industrial, and commercial interests, and geographical divisions of the country. The members of the Board shall devote their entire time to the business of the Board and shall each receive an annual salary of $15,000, payable monthly, together with actual necessary traveling expenses.

[12 USC 241. As amended by acts of June 3, 1922 (42 Stat. 620); Aug. 23, 1935 (49 Stat. 704). Prior to the enactment of the Banking Act of 1935, approved Aug. 23, 1935, the Board of Governors of the Federal Reserve System was known as the Federal Reserve Board. See note to the third paragraph of section 1. The portion of this paragraph dealing with salaries of Board members has in effect been amended numerous times, most recently by Executive Order. Prior to the act of December 27, 2000, section 1002 of which revised the executive schedule, the salary of the chairman of the Board was set at executive schedule level 2 and the salary of other members at level 3. The salary of the chairman of the Board is now set at executive schedule level I, and the salary of other members at level II (see 2 USC 358 and 5 USC 5313 and 5314).]

Back to Top

2. Members ineligible to serve member banks; term of office; chairman and vice chairman

The members of the Board shall be ineligible during the time they are in office and for two years thereafter to hold any office, position, or employment in any member bank, except that this restriction shall not apply to a member who has served the full term for which he was appointed. Upon the expiration of the term of any appointive member of the Federal Reserve Board in office on the date of enactment of the Banking Act of 1935, the President shall fix the term of the successor to such member at not to exceed fourteen years, as designated by the President at the time of nomination, but in such manner as to provide for the expiration of the term of not more than one member in any two-year period, and thereafter each member shall hold office for a term of fourteen years from the expiration of the term of his predecessor, unless sooner removed for cause by the President. Of the persons thus appointed, 1 shall be designated by the President, by and with the advice and consent of the Senate, to serve as Chairman of the Board for a term of 4 years, and 2 shall be designated by the President, by and with the advice and consent of the Senate, to serve as Vice Chairmen of the Board, each for a term of 4 years, 1 of whom shall serve in the absence of the Chairman, as provided in the fourth undesignated paragraph of this section, and 1 of whom shall be designated Vice Chairman for Supervision. The Vice Chairman for Supervision shall develop policy recommendations for the Board regarding supervision and regulation of depository institution holding companies and other financial firms supervised by the Board, and shall oversee the supervision and regulation of such firms. The chairman of the Board, subject to its supervision, shall be its active executive officer. Each member of the Board shall within fifteen days after notice of appointment make and subscribe to the oath of office. Upon the expiration of their terms of office, members of the Board shall continue to serve until their successors are appointed and have qualified. Any person appointed as a member of the Board after the date of enactment of the Banking Act of 1935 shall not be eligible for reappointment as such member after he shall have served a full term of fourteen years.

[12 USC 242. As amended by acts of March 3, 1919 (40 Stat. 1315); June 3, 1922 (42 Stat. 620); June 16, 1933 (48 Stat. 166); Aug. 23, 1935 (49 Stat. 704); November 16, 1977 (91 Stat. 1388); and act of July 21, 2010 (124 Stat. 2126). The Banking Act of 1935, referred to in this paragraph, became effective Aug. 23, 1935. Prior to the enactment of that act, the chairman and vice chairman of the Board of Governors of the Federal Reserve System were known as the governor and vice governor of the Federal Reserve Board, respectively. See note to the third paragraph of section 1. The act of November 16, 1977, amended the second sentence of this paragraph. The amendment takes effect on Jan. 1, 1979, and applies to individuals who are designated by the President on or after such date to serve as chairman or vice chairman. The act of July 21, 2010, designated a new Vice Chairman for Supervision.]

Back to Top

3. Assessments on Federal reserve banks

The Board of Governors of the Federal Reserve System shall have power to levy semiannually upon the Federal reserve banks, in proportion to their capital stock and surplus, an assessment sufficient to pay its estimated expenses and the salaries of its members and employees for the half year succeeding the levying of such assessments, together with any deficit carried forward from the preceding half year, and such assessments may include amounts sufficient to provide for the acquisition by the Board in its own name of such site or building in the District of Columbia as in its judgment alone shall be necessary for the purpose of providing suitable and adequate quarters for the performance of its functions. After September 1, 2000, the Board may also use such assessments to acquire, in its own name, a site or building (in addition to the facilities existing on such date) to provide for the performance of the functions of the Board. After approving such plans, estimates, and specifications as it shall have caused to be prepared, the Board may, notwithstanding any other provision of law, cause to be constructed on any site so acquired by it a building or buildings suitable and adequate in its judgment for

its purposes and proceed to take all such steps as it may deem necessary or appropriate in connection with the construction, equipment, and furnishing of such building or buildings. The Board may maintain, enlarge, or remodel any building or buildings so acquired or constructed and shall have sole control of such building or buildings and space therein.

[12 USC 243. As reenacted without change by act of June 3, 1922 (42 Stat. 621); and amended by acts of June 19, 1934 (48 Stat. 1108) and Dec. 27, 2000 (114 Stat. 3027). By act approved June 27, 1935 (49 Stat. 425), provision was made for the furnishing of steam from the central heating plant to the Federal Reserve Board, now the Board of Governors of the Federal Reserve System.]

Back to Top

4. Principal offices; expenses; deposit of funds; members not to be officers or stockholders of banks

The principal offices of the Board shall be in the District of Columbia. At meetings of the Board the chairman shall preside, and, in his absence, the vice chairman shall preside. In the absence of the chairman and the vice chairman, the board shall elect a member to act as chairman pro tempore. The Board shall determine and prescribe the manner in which its obligations shall be incurred and its disbursements and expenses allowed and paid, and may leave on deposit in the Federal Reserve banks the proceeds of assessments levied upon them to defray its estimated expenses and the salaries of its members and employees, whose employment, compensation, leave, and expenses shall be governed solely by the provisions of this Act, specific amendments thereof, and rules and regulations of the Board not inconsistent therewith; and funds derived from such assessments shall not be construed to be Government funds or appropriated moneys. No member of the Board of Governors of the Federal Reserve System shall be an officer or director of any bank, banking institution, trust company, or Federal Reserve bank or hold stock in any bank, banking institution, or trust company; and before entering upon his duties as a member of the Board of Governors of the Federal Reserve System he shall certify under oath that he has complied with this requirement, and such certification shall be filed with the secretary of the Board. Whenever a vacancy shall occur, other than by expiration of term, among the six members of the Board of Governors of the Federal Reserve System appointed by the President as above provided, a successor shall be appointed by the President, by and with the advice and consent of the Senate, to fill such vacancy, and when appointed he shall hold office for the unexpired term of his predecessor.

[12 USC 244. As amended by acts of June 3, 1922 (42 Stat. 621); June 16, 1933 (48 Stat. 167); Aug. 23, 1935 (49 Stat. 705). The reference to "the six members" of the Board of Governors is an apparent error in the law and should read "the seven members." See section 10, first paragraph, this act.]

Back to Top

5. Vacancies during recess of Senate

The President shall have power to fill all vacancies that may happen on the Board of Governors of the Federal Reserve System during the recess of the Senate by granting commissions which shall expire with the next session of the Senate.

[12 USC 245. As amended by act of June 3, 1922 (42 Stat. 621).]

Back to Top

6. Reservation of powers of Secretary of Treasury

Nothing in this Act contained shall be construed as taking away any powers heretofore vested by law in the Secretary of the Treasury which relate to the supervision, management, and control of the Treasury Department and bureaus under such department, and wherever any power vested by this Act in the Board of Governors of the Federal Reserve System or the Federal reserve agent appears to conflict with the powers of the Secretary of the Treasury, such powers shall be exercised subject to the supervision and control of the Secretary.

[12 USC 246. As reenacted without change by act of June 3, 1922 (42 Stat. 621).]

Back to Top

7. Annual report

The Board of Governors of the Federal Reserve System shall annually make a full report of its operations to the Speaker of the House of Representatives, who shall cause the same to be printed for the information of the Congress. The report required under this paragraph shall include the reports required under section 707 of the Equal Credit Opportunity Act, section 18(f)(7) of the Federal Trade Commission Act, section 114 of the Truth in Lending Act, and the tenth undesignated paragraph of this section.

[12 USC 247. As reenacted without change by act of June 3, 1922 (42 Stat. 621) and amended by acts of June 3, 1922, and Dec. 27, 2000 (114 Stat. 3030).]

Back to Top

8. Office of the Comptroller of the Currency

Section three hundred and twenty-four of the Revised Statutes of the United States shall be amended so as to read as follows:

(a) Office Of The Comptroller Of The Currency Established. There is established in the Department of the Treasury a bureau to be known as the “Office of the Comptroller of the Currency” which is charged with assuring the safety and soundness of, and compliance with laws and regulations, fair access to financial services, and fair treatment of customers by, the institutions and other persons subject to its jurisdiction.

(b) Comptroller Of The Currency.

1. **In General.** The chief officer of the Office of the Comptroller of the Currency shall be known as the Comptroller of the Currency. The Comptroller of the Currency shall perform the duties of the Comptroller of the Currency under the general direction of the Secretary of the Treasury. The Secretary of the Treasury may not delay or prevent the issuance of any rule or the promulgation of any regulation by the Comptroller of the Currency, and may not intervene in any matter or proceeding before the Comptroller of the Currency (including agency enforcement actions), unless otherwise specifically provided by law.
2. **Additional Authority.** The Comptroller of the Currency shall have the same authority with respect to functions

transferred to the Comptroller of the Currency under the Enhancing Financial Institution Safety and Soundness Act of 2010 as was vested in the Director of the Office of Thrift Supervision on the transfer date, as defined in section 311 of that Act.

[12 USC 1. As reenacted without change by act of June 3, 1922 (42 Stat. 621); and amended by acts of May 20, 1966 (80 Stat. 161), Sept. 23, 1994 (108 Stat. 2232), and July 21, 2010 (124 Stat. 1523).]

Back to Top

9. Branch Federal Reserve bank buildings

No Federal Reserve bank may authorize the acquisition or construction of any branch building, or enter into any contract or other obligation for the acquisition or construction of any branch building, without the approval of the Board.

[12 USC 522. As added by act of June 3, 1922 (42 Stat. 622); and amended by acts of Feb. 6, 1923 (42 Stat. 1223); July 30, 1947 (61 Stat. 520); May 29, 1953 (67 Stat. 41); Aug. 31, 1962 (76 Stat. 418); Oct. 28, 1974 (88 Stat. 1505); and Oct. 24, 1992 (106 Stat. 3144).]

Back to Top

10. Record of open market and other policies

The Board of Governors of the Federal Reserve System shall keep a complete record of the action taken by the Board and by the Federal Open Market Committee upon all questions of policy relating to open-market operations and shall record therein the votes taken in connection with the determination of open-market policies and the reasons underlying the action of the Board and the Committee in each instance. The Board shall keep a similar record with respect to all questions of policy determined by the Board, and shall include in its annual report to the Congress a full account of the action so taken during the preceding year with respect to open-market policies and operations and with respect to the policies determined by it and shall include in such report a copy of the records required to be kept under the provisions of this paragraph.

[12 USC 247a. As added by act of Aug. 23, 1935 (49 Stat. 705).]

Back to Top

12. Appearances before Congress*

The Vice Chairman for Supervision shall appear before the Committee on Banking, Housing, and Urban Affairs of the Senate and the Committee on Financial Services of the House of Representatives and at semi-annual hearings regarding the efforts, activities, objectives, and plans of the Board with respect to the conduct of supervision and regulation of depository institution holding companies and other financial firms supervised by the Board.

[12 USC 247b. As added by act of July 21, 2010 (124 Stat. 2126).]

* The act of July 21, 2010, added paragraph 12 without adding paragraph 11.

Back to Top

Government Performance and Results Act Annual Performance Report 2011

Print

Mission, Values, and Goals of the Board of Governors

Mission

The mission of the Board is to foster the stability, integrity, and efficiency of the nation's monetary, financial, and payment systems so as to promote optimal macroeconomic performance.

Back to section top

Values

The following values of the Board guide its organizational decisions and its employees' actions.

- **Public interest.** In its actions and policies, the Board seeks to promote the public interest. It is accountable and responsive to the general public, the U.S. government, and the financial community.
- **Integrity.** The Board adheres to the highest standards of integrity in its dealings with the public, the financial community, and its employees.
- **Excellence.** The conduct of monetary policy, responsibility for bank supervision, and maintenance of the payment system demand high-quality analysis; high performance standards; and a secure, robust infrastructure. The pursuit of excellence drives the Board's policies concerning recruitment, selection, and retention of Board employees.
- **Efficiency and effectiveness.** In carrying out its functions, the Board is continually aware that its operations are supported primarily by public funds, and it recognizes its obligation to manage resources efficiently and effectively.
- **Independence of views.** The Board values the diversity of its employees, input from a variety of sources, and the independent professional judgment that is fostered by the System's highly valued regional structure. It relies on strong teamwork to mold independent viewpoints into coherent, effective policies.

Back to section top

Strategic Goals

The Board has six primary strategic goals with interrelated and mutually reinforcing elements:

conduct monetary policy that promotes the achievement of the Federal Reserve's statutory objectives of maximum employment and stable prices

promote a safe, sound, competitive, and accessible banking system and stable financial markets

administer federal consumer financial protection laws that fall within the Board's statutory authority, including those designed to encourage regulated financial institutions to help meet the credit needs of their local communities

foster the integrity, efficiency, and accessibility of U.S. payment and settlement systems

provide oversight of the Reserve Banks

foster the integrity, efficiency, and effectiveness of Board programs and operations

Back to section top

Role of Strategic Planning

Unlike most other government agencies, the Board's budget is not subject to the congressional appropriations process or to review by the Administration through the Office of Management and Budget. Rather, the Board establishes its own budget formulation procedures, conducts strategic planning to identify changes to its critical activities and the proper amount and allocation of resources to support its mission, and provides various reports to the Congress.

The Board, like the framers of the Federal Reserve Act, considers its budgetary independence directly relevant to independence in managing monetary policy. The Board believes that to maintain budgetary independence, it must demonstrate effective and efficient use of its financial resources. Resource management begins with a clear mission statement, identification of goals, a review of factors that might affect the long-term attainment of these goals, and consideration of possible responses to those factors. By establishing objectives to attain its goals and by identifying the resources needed to accomplish them, the Board develops a budget necessary to implement its strategic plan.

Strategic planning is a critical factor in ensuring the long-term effectiveness of Board operations and in minimizing its costs. Effectiveness is improved through timely identification of threats and through efforts to improve operational efficiency. Efficiency is increased by early identification of issues and timely responses.

As technological and other changes evolve and accelerate, planning is essential to the effective and efficient conduct of Board operations. A continuing challenge to government agencies in this regard is identifying the appropriate measures of performance. The Board's strategic planning effort recognizes the key distinctions between government and private-sector strategic planning efforts and measurement of those efforts.

Private-sector planning often relies on measures of cost and revenue derived from prices determined in competitive markets; the results of that planning are reflected in the ability of the private entity to prosper over time. The government does not have direct competition in certain areas and has a monopoly in others (conducting monetary policy, for example); establishing a comparable metric to costs and prices is therefore extraordinarily difficult. Moreover, the results are judged relative to public policy objectives embodied in law, which often are not readily measurable. The Board seeks to accomplish its mission effectively while creating the efficiencies that come from strategic planning, recognizing that analogies to the private sector are just that. The Board's central planning objective is oriented toward achieving efficiency and effectiveness specific to the functions it serves.

Back to section top

Interagency Coordination

The Federal Reserve works closely with other regulators, the Congress, and the Administration to ensure that its responsibilities are carried out in a manner that best protects the stability of the nation's financial system and strengthens the U.S. economy. Following are some highlights of the Board's interagency coordination efforts.

In this Section:

Federal Financial Institutions Examination Council (FFIEC)

Other Interagency Efforts

To promote uniformity in the supervision of financial institutions by the federal regulatory agencies, the Board participates in the FFIEC, a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions and to make recommendations to the federal supervisory agencies. The FFIEC is composed of a Board governor, the Comptroller of the Currency, the director of the CFPB, the chairman of the Federal Deposit Insurance Corporation (FDIC), the chairman of the National Credit Union Administration (NCUA), and the chairman of the State Liaison Committee, representing state banking supervisors.

Financial Stability Oversight Council (FSOC)

The FSOC, which was established by the Dodd-Frank Act, is charged with a number of important duties, including monitoring and identifying emerging risks to financial stability across the entire financial system, identifying potential regulatory gaps, and coordinating financial regulatory agencies' responses to potential systemic risks. The FSOC is composed of the Secretary of the U.S. Department of the Treasury (Treasury) (serves as chairperson of the FSOC); the Chairman of the Federal Reserve Board; the heads of the Commodity Futures Trading Commission, CFPB, FDIC, Federal Housing Finance Agency, NCUA, Office of the Comptroller of the Currency (OCC), Securities and Exchange Commission (SEC); and an independent member with insurance expertise, appointed by the President and confirmed by the Senate.

Other Interagency Efforts

In addition to participating in the FFIEC and FSOC, the Board also works bilaterally with federal agencies to coordinate key initiatives, such as the Board's implementation efforts under the Dodd-Frank Act. For example, shortly after the Dodd-Frank Act was enacted in July 2010, the Board developed a transition team, headed by a Board governor, to provide technical assistance to Treasury in setting up the functions of the CFPB.[4] The Board also worked with the Office of Thrift Supervision (OTS) to develop comprehensive plans relating to the transfer of the supervisory authority of the OTS for savings associations and their parent holding companies.[5] The Board will continue to work closely and cooperatively with other federal agencies to develop several joint rules required under the Dodd-Frank Act.

Back to section top

References

4. On July 21, 2011, certain consumer protection functions designated by the Dodd-Frank Act were transferred from the Board and other banking agencies to the CFPB. Return to text

5. The Dodd-Frank Act transferred the OTS's responsibilities with respect to the supervision and regulation of savings and loan holding companies to the Board. The transfer of this authority occurred on July 21, 2011. Return to text

Last update: July 10, 2012

SYSTEM PUBLICATION

The Federal Reserve System

PURPOSES & FUNCTIONS

The Federal Reserve System

PURPOSES & FUNCTIONS

Board of Governors of the Federal Reserve System
Washington, D.C.

First Edition, May 1939
Second Edition, November 1947
Third Edition, April 1954
Fourth Edition, February 1961
Fifth Edition, December 1963
Sixth Edition, September 1974
Seventh Edition, December 1984
Eighth Edition, December 1994
Ninth Edition, June 2005

Library of Congress Control Number 39026719

Copies of this book may be obtained from Publications Fulfillment, Board of Governors of the Federal Reserve System, Washington, DC 20551.

Purposes and Functions is published under the direction of the staff Publications Committee. It is assisted by the Publications Department, under the direction of Lucretia M. Boyer.

Preface

This is the ninth edition of The Federal Reserve System: Purposes and Functions. *It has been revised by staff members of the Federal Reserve Board to reflect the changes that have taken place in the monetary, regulatory, and other policy areas since publication of the eighth edition in 1994. It incorporates major changes in the law and in the structure of the financial system that have occurred over the past decade.*

The Board's Publications Committee had overall responsibility for the preparation of this edition. Major contributions were made by the following:

Division of Research and Statistics
Thomas D. Simpson

Division of Monetary Affairs
Cheryl L. Edwards, William R. Nelson, Seth B. Carpenter, and Selva Demiralp

Division of International Finance
Joseph E. Gagnon

Division of Banking Supervision and Regulation
Richard Spillenkothen, Virginia M. Gibbs, and Greg Feldberg

Division of Consumer and Community Affairs
Jeanne Hogarth, Adrienne Hurt, Terri Johnsen, Elizabeth Eurgubian, Yvonne Cooper, and Tracy Anderson

Division of Reserve Bank Operations and Payment Systems
Jeffrey C. Marquardt and Theresa A. Trimble

Legal Division
Kieran Fallon, Joshua H. Kaplan, Amanda Allexon, and Heatherun Allison

Office of Board Members
Rose Pianalto, Diana Lahm, Anita Bennett, and Britt Leckman

Contents

1 Overview of the Federal Reserve System

The Federal Reserve System is the central bank of the United States. It was founded by Congress in 1913 to provide the nation with a safer, more flexible, and more stable monetary and financial system. Over the years, its role in banking and the economy has expanded.

Today, the Federal Reserve's duties fall into four general areas:

- conducting the nation's monetary policy by influencing the monetary and credit conditions in the economy in pursuit of maximum employment, stable prices, and moderate long-term interest rates
- supervising and regulating banking institutions to ensure the safety and soundness of the nation's banking and financial system and to protect the credit rights of consumers
- maintaining the stability of the financial system and containing systemic risk that may arise in financial markets
- providing financial services to depository institutions, the U.S. government, and foreign official institutions, including playing a major role in operating the nation's payments system

Most developed countries have a central bank whose functions are broadly similar to those of the Federal Reserve. The oldest, Sweden's Riksbank, has existed since 1668 and the Bank of England since 1694. Napoleon I established the Banque de France in 1800, and the Bank of Canada began operations in 1935. The German Bundesbank was reestablished after World War II and is loosely modeled on the Federal Reserve. More recently, some functions of the Banque de France and the Bundesbank have been assumed by the European Central Bank, formed in 1998.

Background

During the nineteenth century and the beginning of the twentieth century, financial panics plagued the nation, leading to bank failures and business bankruptcies that severely disrupted the economy. The failure of the nation's banking system to effectively provide funding to troubled depository institutions contributed significantly to the economy's vulnerability to financial panics. Short-term credit is an important source of liquidity when a bank experiences unexpected and widespread withdrawals during a financial panic. A particularly severe crisis in 1907 prompted

Congress to establish the National Monetary Commission, which put forth proposals to create an institution that would help prevent and contain financial disruptions of this kind. After considerable debate, Congress passed the Federal Reserve Act "to provide for the establishment of Federal reserve banks, to furnish an elastic currency, to afford means of rediscounting commercial paper, to establish a more effective supervision of banking in the United States, and for other purposes." President Woodrow Wilson signed the act into law on December 23, 1913.

DECEMBER 24, 1913—SIXTEEN PAGES. PRICE TWO CENTS.

PRESIDENT'S SIGNATURE ENACTS CURRENCY LAW

Wilson Declares It the First of Series of Constructive Acts to Aid Business.

Makes Speech to Group of Democratic Leaders.

Conference Report Adopted in Senate by Vote of 43 to 25.

Banks All Over the Country Hasten to Enter Federal Reserve System.

Gov-Elect Walsh Calls Passage of Bill A Fine Christmas Present.

WILSON SEES DAWN OF NEW ERA IN BUSINESS

Aims to Make Prosperity Free to Have Unimpeded Momentum.

HOME VIEWS OF CURRENCY ACT

FOUR PENS USED BY PRESIDENT

President Wilson signed the Federal Reserve Act on December 23, 1913.

Soon after the creation of the Federal Reserve, it became clear that the act had broader implications for national economic and financial policy. As time has passed, further legislation has clarified and supplemented the original purposes. Key laws affecting the Federal Reserve have been the Banking Act of 1935; the Employment Act of 1946; the Bank Holding Company Act of 1956 and the amendments of 1970; the International Banking Act of 1978; the Full Employment and Balanced Growth Act of 1978; the Depository Institutions Deregulation and Monetary Control Act of 1980; the Financial Institutions Reform, Recovery, and Enforcement Act of 1989; the Federal Deposit Insurance Corporation Improvement Act of 1991; and the Gramm-Leach-Bliley Act of 1999. Congress has also adopted legislation defining the primary objectives of national economic policy, including the Employment Act of 1946; the Federal Reserve Reform Act of 1977; and the Full Employment and Balanced Growth Act of 1978, which is sometimes called the Humphrey-Hawkins Act, after its original sponsors. These objectives include economic growth in line with the economy's potential to expand; a high level of employment; stable prices (that is, stability in the purchasing power of the dollar); and moderate long-term interest rates.

The Federal Reserve System is considered to be an independent central bank because its decisions do not have to be ratified by the President or

anyone else in the executive branch of government. The System is, however, subject to oversight by the U.S. Congress. The Federal Reserve must work within the framework of the overall objectives of economic and financial policy established by the government; therefore, the description of the System as "independent within the government" is more accurate.

Structure of the System

Congress designed the structure of the Federal Reserve System to give it a broad perspective on the economy and on economic activity in all parts of the nation. It is a federal system, composed of a central, governmental agency—the Board of Governors—in Washington, D.C., and twelve regional Federal Reserve Banks. The Board and the Reserve Banks share responsibility for supervising and regulating certain financial institutions and activities, for providing banking services to depository institutions and the federal government, and for ensuring that consumers receive adequate information and fair treatment in their business with the banking system.

The Federal Reserve must work within the framework of the overall objectives of economic and financial policy established by the government.

A major component of the System is the Federal Open Market Committee (FOMC), which is made up of the members of the Board of Governors, the president of the Federal Reserve Bank of New York, and presidents of four other Federal Reserve Banks, who serve on a rotating basis. The FOMC oversees open market operations, which is the main tool used by the Federal Reserve to influence overall monetary and credit conditions. These operations are described in greater detail in chapter 3.

The Federal Reserve implements monetary policy through its control over the federal funds rate—the rate at which depository institutions trade balances at the Federal Reserve. It exercises this control by influencing the demand for and supply of these balances through the following means:

- Open market operations—the purchase or sale of securities, primarily U.S. Treasury securities, in the open market to influence the level of balances that depository institutions hold at the Federal Reserve Banks
- Reserve requirements—requirements regarding the percentage of certain deposits that depository institutions must hold in reserve in the form of cash or in an account at a Federal Reserve Bank
- Contractual clearing balances—an amount that a depository institution agrees to hold at its Federal Reserve Bank in addition to any required reserve balance
- Discount window lending—extensions of credit to depository institutions made through the primary, secondary, or seasonal lending programs

Two other groups play roles in the functioning of the Federal Reserve Sys-

tem: depository institutions, through which monetary policy operates, and advisory committees, which make recommendations to the Board of Governors and to the Reserve Banks regarding the System's responsibilities.

Board of Governors

The Board of Governors of the Federal Reserve System is a federal government agency. The Board is composed of seven members, who are appointed by the President of the United States and confirmed by the U.S. Senate. The full term of a Board member is fourteen years, and the appointments are staggered so that one term expires on January 31 of each even-numbered year. After serving a full term, a Board member may not be reappointed. If a member leaves the Board before his or her term expires, however, the person appointed and confirmed to serve the remainder of the term may later be reappointed to a full term.

The first Federal Reserve Board, 1914

The Chairman and the Vice Chairman of the Board are also appointed by the President and confirmed by the Senate. The nominees to these posts must already be members of the Board or must be simultaneously appointed to the Board. The terms for these positions are four years.

The Board of Governors is supported by a staff in Washington, D.C., numbering about 1,800 as of 2004. The Board's responsibilities require thorough analysis of domestic and international financial and economic developments. The Board carries out those responsibilities in conjunction with other components of the Federal Reserve System. The Board of Governors also supervises and regulates the operations of the Federal Reserve Banks, exercises broad responsibility in the nation's payments system, and administers most of the nation's laws regarding consumer credit protection.

Policy regarding open market operations is established by the FOMC. However, the Board of Governors has sole authority over changes in reserve requirements, and it must approve any change in the discount rate initiated by a Federal Reserve Bank.

The Board also plays a major role in the supervision and regulation of the U.S. banking system. It has supervisory responsibilities for state-chartered banks that are members of the Federal Reserve System, bank holding companies (companies that control banks), the foreign activities of member banks, the U.S. activities of foreign banks, and Edge Act and agreement corporations (limited-purpose institutions that engage in a foreign banking business). The Board and, under delegated authority, the Federal

Reserve Banks, supervise approximately 900 state member banks and 5,000 bank holding companies. Other federal agencies also serve as the primary federal supervisors of commercial banks; the Office of the Comptroller of the Currency supervises national banks, and the Federal Deposit Insurance Corporation supervises state banks that are not members of the Federal Reserve System.

Some regulations issued by the Board apply to the entire banking industry, whereas others apply only to member banks, that is, state banks that have chosen to join the Federal Reserve System and national banks, which by law must be members of the System. The Board also issues regulations to carry out major federal laws governing consumer credit protection, such as the Truth in Lending, Equal Credit Opportunity, and Home Mortgage Disclosure Acts. Many of these consumer protection regulations apply to various lenders outside the banking industry as well as to banks.

Members of the Board of Governors are in continual contact with other policy makers in government. They frequently testify before congressional committees on the economy, monetary policy, banking supervision and regulation, consumer credit protection, financial markets, and other matters. For instance, as required by the Federal Reserve Act, the Chairman of the Board of Governors testifies before the Senate Committee on Banking, Housing, and Urban Affairs and the House Committee on Financial Services on or about February 20 and July 20 of each year. The Chairman's testimony addresses the efforts, activities, objectives, and plans of the Board of Governors and the Federal Open Market Committee with respect to the conduct of monetary policy, as well as economic developments in the United States and the prospects for the future. Concurrently, the Board of Governors must submit a report on these same issues to the House and Senate committees before which the Chairman testifies.

The Board has regular contact with members of the President's Council of Economic Advisers and other key economic officials. The Chairman also meets from time to time with the President of the United States and has regular meetings with the Secretary of the Treasury.

The Chairman has formal responsibilities in the international arena as well. For example, he is the alternate U.S. member of the board of governors of the International Monetary Fund, a member of the board of the Bank for International Settlements (BIS), and a member, along with the heads of other relevant U.S. agencies and departments, of the National Advisory Council on International Monetary and Financial Policies. He is also a member of U.S. delegations to key international meetings, such as those of the finance ministers and central bank governors of the seven largest industrial countries—referred to as the Group of Seven, or G-7. He, other Board members, and Board staff members share many inter-

national responsibilities, including representing the Federal Reserve at meetings at the BIS in Basel, Switzerland, and at the Organisation for Economic Co-operation and Development in Paris, France.

One member of the Board of Governors serves as the System's representative to the Federal Financial Institutions Examination Council (FFIEC), which is responsible for coordinating, at the federal level, examinations of depository institutions and related policies. The FFIEC has representatives from the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, as well.

The Board publishes detailed statistics and other information about the System's activities and the economy in publications such as the quarterly *Federal Reserve Bulletin*, the monthly *Statistical Supplement*, and separate statistical releases. Through the *Federal Reserve Regulatory Service*, it provides materials relating to its regulatory and supervisory functions. Extensive information about the Board of Governors is available on the Board's web site (www.federalreserve.gov), including the testimony and speeches of Board members; actions on banking and consumer regulations and other matters; and statistics and research papers concerning economic, banking, and financial matters.

The Reserve Banks are the operating arms of the central banking system.

The Board is audited annually by a major public accounting firm. In addition, the Government Accountability Office (GAO) generally exercises its authority to conduct a number of reviews each year to look at specific aspects of the Federal Reserve's activities. The audit report of the public accounting firm and a complete list of GAO reviews under way are available in the Board's *Annual Report*, which is sent to Congress during the second quarter of each calendar year. Monetary policy is exempt from audit by the GAO because it is monitored directly by Congress through written reports, including the semiannual *Monetary Policy Report to the Congress*, prepared by the Board of Governors.

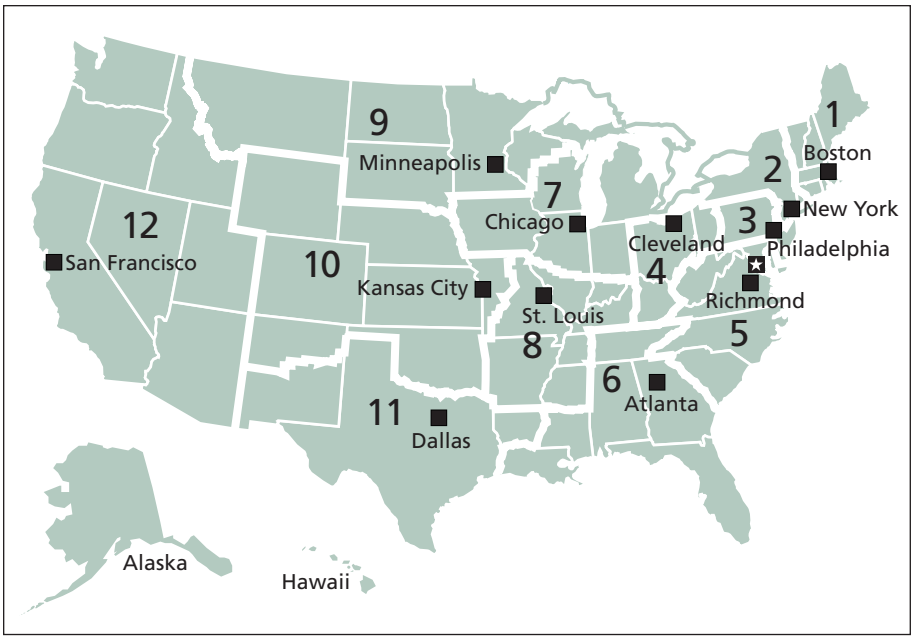
Federal Reserve Banks

A network of twelve Federal Reserve Banks and their Branches (twenty-five as of 2004) carries out a variety of System functions, including operating a nationwide payments system, distributing the nation's currency and coin, supervising and regulating member banks and bank holding companies, and serving as banker for the U.S. Treasury. The twelve Reserve Banks are each responsible for a particular geographic area or district of the United States. Each Reserve District is identified by a number and a letter (see the list of District offices on page 7). Besides carrying out functions for the System as a whole, such as administering nationwide banking and credit policies, each Reserve Bank acts as a depository for the banks in its own District and fulfills other District responsibilities. The various

Federal Reserve District Banks and Branches

Number	Letter	Bank	Branch
1	A	Boston	
2	B	New York	Buffalo, New York
3	C	Philadelphia	
4	D	Cleveland	Cincinnati, Ohio Pittsburgh, Pennsylvania
5	E	Richmond	Baltimore, Maryland Charlotte, North Carolina
6	F	Atlanta	Birmingham, Alabama Jacksonville, Florida Miami, Florida Nashville, Tennessee New Orleans, Louisiana
7	G	Chicago	Detroit, Michigan
8	H	St. Louis	Little Rock, Arkansas Louisville, Kentucky Memphis, Tennessee
9	I	Minneapolis	Helena, Montana
10	J	Kansas City	Denver, Colorado Oklahoma City, Oklahoma Omaha, Nebraska
11	K	Dallas	El Paso, Texas Houston, Texas San Antonio, Texas
12	L	San Francisco	Los Angeles, California Portland, Oregon Salt Lake City, Utah Seattle, Washington

The Federal Reserve System



Legend

- ■ Federal Reserve Bank city
- ✪ Board of Governors of the Federal Reserve System, Washington, D.C.
- • Federal Reserve Branch city
- — Branch boundary

Notes

The Federal Reserve officially identifies Districts by number and by Reserve Bank city (shown on both pages) as well as by letter (shown on the facing page).

In the 12th District, the Seattle Branch serves Alaska and the San Francisco Bank serves Hawaii.

The New York Bank serves the Commonwealth of Puerto Rico and the U.S. Virgin Islands; the San Francisco Bank serves American Samoa, Guam, and the Commonwealth of the Northern Mariana Islands.

The Board of Governors revised the Branch boundaries of the System most recently in February 1996.


1–A
ME
VT
NH
MA
CT
RI
Boston
2–B
NY
CT
Buffalo
NJ
NY
New York
3–C
PA
NJ
DE
Philadelphia
4–D
Pittsburgh
PA
OH
WV
Cincinnati
KY
Cleveland
5–E
Baltimore
MD
VA
WV
NC
Charlotte
SC
Richmond
6–F
Nashville
TN
Birmingham
AL
GA
MS
LA
New Orleans
Jacksonville
FL
Miami
Atlanta
7–G
WI
MI
Detroit
IA
IL
IN
Chicago
8–H
IN
KY
IL
Louisville
MO
TN
AR
Memphis
Little Rock
MS
St. Louis
9–I
MT
Helena
ND
SD
MN
MI
WI
Minneapolis
10–J
WY
NE
Omaha
CO
Denver
MO
NM
Oklahoma City
OK
Kansas City
11–K
TX
NM
El Paso
LA
Houston
San Antonio
Dallas
12–L
Alaska
WA
Seattle
Portland
OR
ID
CA
NV
Salt Lake City
UT
Los Angeles
AZ
Hawaii
San Francisco

offices and boundaries of the Federal Reserve Districts are shown on the maps on pages 8 and 9.

The Board of Governors has broad oversight responsibility for the operations and activities of the Federal Reserve Banks and their Branches. This authority includes oversight of the Reserve Banks' services to banks and other depository institutions and of their examination and supervision of various banking institutions. Each Federal Reserve Bank must submit its annual budget to the Board of Governors for approval. Particular types of expenditures—such as those for construction or major alterations of Reserve Bank buildings and for the salaries of Reserve Bank presidents and first vice presidents—also are subject to specific Board approval.

Congress chartered the Federal Reserve Banks for a public purpose. The Reserve Banks are the operating arms of the central banking system, and they combine both public and private elements in their makeup and organization. As part of the Federal Reserve System, the Banks are subject to oversight by Congress.

Each Reserve Bank has its own board of nine directors chosen from outside the Bank as provided by law. The boards of the Reserve Banks are intended to represent a cross-section of banking, commercial, agricultural, industrial, and public interests within the Federal Reserve District. Three directors, designated Class A directors, represent commercial banks that are members of the Federal Reserve System. Three Class B and three Class C directors represent the public. The member commercial banks in each District elect the Class A and Class B directors. The Board of Governors appoints the Class C directors to their posts. From the Class C directors, the Board of Governors selects one person as chairman and another as deputy chairman. No Class B or Class C director may be an officer, director, or employee of a bank or a bank holding company. No Class C director may own stock in a bank or a bank holding company. The directors in turn nominate a president and first vice president of the Reserve Bank, whose selection is subject to approval by the Board of Governors. Each Branch of a Reserve Bank has its own board of directors composed of at least three and no more than seven members. A majority of these directors are appointed by the Branch's Reserve Bank; the others are appointed by the Board of Governors.

Boards of directors of the Reserve Banks provide the Federal Reserve System with a wealth of information on economic conditions in virtually every corner of the nation. This information is used by the FOMC and the Board of Governors in reaching major decisions about monetary policy. Information from directors and other sources gathered by the Reserve Banks is also shared with the public in a special report—informally called the Beige Book—which is issued about two weeks

before each meeting of the FOMC. In addition, every two weeks, the board of each Bank must recommend interest rates for its Bank's discount window lending, subject to review and determination by the Board of Governors.

The income of the Federal Reserve System is derived primarily from the interest on U.S. government securities that it has acquired through open market operations. Other major sources of income are the interest on foreign currency investments held by the System; interest on loans to depository institutions; and fees received for services provided to depository institutions, such as check clearing, funds transfers, and automated clearinghouse operations.

After it pays its expenses, the Federal Reserve turns the rest of its earnings over to the U.S. Treasury. About 95 percent of the Reserve Banks' net earnings have been paid into the Treasury since the Federal Reserve System began operations in 1914. (Income and expenses of the Federal Reserve Banks from 1914 to the present are included in the *Annual Report* of the Board of Governors.) In 2003, the Federal Reserve paid approximately $22 billion to the Treasury.

After it pays its expenses, the Federal Reserve turns the rest of its earnings over to the U.S. Treasury.

The Board of Governors contracts with an accounting firm to conduct an audit of the Reserve Banks every year, and Board staff periodically reviews the operations of the Reserve Banks in key functional areas. The audited combined financial statements of the Reserve Banks are published in the Board's *Annual Report.* The Reserve Banks, like the Board, are subject to audit by the GAO, but certain functions, such as transactions with foreign central banks and open market operations, are excluded from the GAO's audit. Each Reserve Bank has an internal auditor who is responsible to the Bank's board of directors.

Federal Open Market Committee

The FOMC is charged under law with overseeing open market operations, the principal tool of national monetary policy. These operations affect the amount of Federal Reserve balances available to depository institutions (see chapter 3), thereby influencing overall monetary and credit conditions. The FOMC also directs operations undertaken by the Federal Reserve in foreign exchange markets.

The FOMC is composed of the seven members of the Board of Governors and five of the twelve Reserve Bank presidents. The president of the Federal Reserve Bank of New York is a permanent member; the other

presidents serve one-year terms on a rotating basis.[1] All the presidents participate in FOMC discussions, contributing to the committee's assessment of the economy and of policy options, but only the five presidents who are committee members vote on policy decisions. The FOMC, under law, determines its own internal organization and by tradition elects the Chairman of the Board of Governors as its chairman and the president of the Federal Reserve Bank of New York as its vice chairman. Formal meetings typically are held eight times each year in Washington, D.C. Telephone consultations and other meetings are held when needed.

The FOMC is composed of the seven members of the Board of Governors and five of the twelve Reserve Bank presidents.

Member Banks

The nation's commercial banks can be divided into three types according to which governmental body charters them and whether or not they are members of the Federal Reserve System. Those chartered by the federal government (through the Office of the Comptroller of the Currency in the Department of the Treasury) are national banks; by law, they are members of the Federal Reserve System. Banks chartered by the states are divided into those that are members of the Federal Reserve System (state member banks) and those that are not (state nonmember banks). State banks are not required to join the Federal Reserve System, but they may elect to become members if they meet the standards set by the Board of Governors. As of March 2004, of the nation's approximately 7,700 commercial banks approximately 2,900 were members of the Federal Reserve System—approximately 2,000 national banks and 900 state banks.

Member banks must subscribe to stock in their regional Federal Reserve Bank in an amount equal to 6 percent of their capital and surplus, half of which must be paid in while the other half is subject to call by the Board of Governors. The holding of this stock, however, does not carry with it the control and financial interest conveyed to holders of common stock in for-profit organizations. It is merely a legal obligation of Federal Reserve membership, and the stock may not be sold or pledged as collateral for loans. Member banks receive a 6 percent dividend annually on their stock, as specified by law, and vote for the Class A and Class B directors of the Reserve Bank. Stock in Federal Reserve Banks is not available for purchase by individuals or entities other than member banks.

1. The rotating seats are filled from the following four groups of Banks, one Bank president from each group: Boston, Philadelphia, and Richmond; Cleveland and Chicago; Atlanta, St. Louis, and Dallas; and Minneapolis, Kansas City, and San Francisco. An alternate for each Reserve Bank president also is elected. This alternate, who must be a president or first vice president of a Reserve Bank, may serve on the FOMC in the absence of the relevant Reserve Bank president.

Advisory Committees

The Federal Reserve System uses advisory committees in carrying out its varied responsibilities. Three of these committees advise the Board of Governors directly:

- ***Federal Advisory Council.*** This council, which is composed of twelve representatives of the banking industry, consults with and advises the Board on all matters within the Board's jurisdiction. It ordinarily meets four times a year, as required by the Federal Reserve Act. These meetings are held in Washington, D.C., customarily on the first Friday of February, May, September, and December, although occasionally the meetings are set for different times to suit the convenience of either the council or the Board. Annually, each Reserve Bank chooses one person to represent its District on the Federal Advisory Committee, and members customarily serve three one-year terms and elect their own officers.
- ***Consumer Advisory Council.*** This council, established in 1976, advises the Board on the exercise of its responsibilities under the Consumer Credit Protection Act and on other matters in the area of consumer financial services. The council's membership represents the interests of consumers, communities, and the financial services industry. Members are appointed by the Board of Governors and serve staggered three-year terms. The council meets three times a year in Washington, D.C., and the meetings are open to the public.
- ***Thrift Institutions Advisory Council.*** After the passage of the Depository Institutions Deregulation and Monetary Control Act of 1980, which extended to thrift institutions the Federal Reserve's reserve requirements and access to the discount window, the Board of Governors established this council to obtain information and views on the special needs and problems of thrift institutions. Unlike the Federal Advisory Council and the Consumer Advisory Council, the Thrift Institutions Advisory Council is not a statutorily mandated body, but it performs a comparable function in providing firsthand advice from representatives of institutions that have an important relationship with the Federal Reserve. The council meets with the Board in Washington, D.C., three times a year. The members are representatives from savings and loan institutions, mutual savings banks, and credit unions. Members are appointed by the Board of Governors and generally serve for two years.

The Federal Reserve Banks also use advisory committees. Of these advisory committees, perhaps the most important are the committees (one for each Reserve Bank) that advise the Banks on matters of agriculture, small business, and labor. Biannually, the Board solicits the views of each of these committees by mail.

2 Monetary Policy and the Economy

The Federal Reserve sets the nation's monetary policy to promote the objectives of maximum employment, stable prices, and moderate long-term interest rates. The challenge for policy makers is that tensions among the goals can arise in the short run and that information about the economy becomes available only with a lag and may be imperfect.

Goals of Monetary Policy

The goals of monetary policy are spelled out in the Federal Reserve Act, which specifies that the Board of Governors and the Federal Open Market Committee should seek "to promote effectively the goals of maximum employment, stable prices, and moderate long-term interest rates." Stable prices in the long run are a precondition for maximum sustainable output growth and employment as well as moderate long-term interest rates. When prices are stable and believed likely to remain so, the prices of goods, services, materials, and labor are undistorted by inflation and serve as clearer signals and guides to the efficient allocation of resources and thus contribute to higher standards of living. Moreover, stable prices foster saving and capital formation, because when the risk of erosion of asset values resulting from inflation—and the need to guard against such losses—are minimized, households are encouraged to save more and businesses are encouraged to invest more.

Although price stability can help achieve maximum sustainable output growth and employment over the longer run, in the short run some tension can exist between the two goals. Often, a slowing of employment is accompanied by lessened pressures on prices, and moving to counter the weakening of the labor market by easing policy does not have adverse inflationary effects. Sometimes, however, upward pressures on prices are developing as output and employment are softening—especially when an adverse supply shock, such as a spike in energy prices, has occurred. Then, an attempt to restrain inflation pressures would compound the weakness in the economy, or an attempt to reverse employment losses would aggravate inflation. In such circumstances, those responsible for monetary policy face a dilemma and must decide whether to focus on defusing price pressures or on cushioning the loss of employment and output. Adding to the difficulty is the possibility that an expectation of

increasing inflation might get built into decisions about prices and wages, thereby adding to inflation inertia and making it more difficult to achieve price stability.

Beyond influencing the level of prices and the level of output in the near term, the Federal Reserve can contribute to financial stability and better economic performance by acting to contain financial disruptions and preventing their spread outside the financial sector. Modern financial systems are highly complex and interdependent and may be vulnerable to widescale systemic disruptions, such as those that can occur during a plunge in stock prices. The Federal Reserve can enhance the financial system's resilience to such shocks through its regulatory policies toward banking institutions and payment systems. If a threatening disturbance develops, the Federal Reserve can also cushion the impact on financial markets and the economy by aggressively and visibly providing liquidity through open market operations or discount window lending.

Depository institutions have accounts at their Reserve Banks, and they actively trade balances held in these accounts in the federal funds market at an interest rate known as the federal funds rate.

How Monetary Policy Affects the Economy

The initial link in the chain between monetary policy and the economy is the market for balances held at the Federal Reserve Banks. Depository institutions have accounts at their Reserve Banks, and they actively trade balances held in these accounts in the federal funds market at an interest rate known as the federal funds rate. The Federal Reserve exercises considerable control over the federal funds rate through its influence over the supply of and demand for balances at the Reserve Banks.

The FOMC sets the federal funds rate at a level it believes will foster financial and monetary conditions consistent with achieving its monetary policy objectives, and it adjusts that target in line with evolving economic developments. A change in the federal funds rate, or even a change in expectations about the future level of the federal funds rate, can set off a chain of events that will affect other short-term interest rates, longer-term interest rates, the foreign exchange value of the dollar, and stock prices. In turn, changes in these variables will affect households' and businesses' spending decisions, thereby affecting growth in aggregate demand and the economy.

Short-term interest rates, such as those on Treasury bills and commercial paper, are affected not only by the current level of the federal funds rate but also by expectations about the overnight federal funds rate over the duration of the short-term contract. As a result, short-term interest rates could decline if the Federal Reserve surprised market participants with a reduction in the federal funds rate, or if unfolding events convinced participants that the Federal Reserve was going to be holding the federal funds rate lower than had been anticipated. Similarly, short-term inter-

est rates would increase if the Federal Reserve surprised market participants by announcing an increase in the federal funds rate, or if some event prompted market participants to believe that the Federal Reserve was going to be holding the federal funds rate at higher levels than had been anticipated.

It is for these reasons that market participants closely follow data releases and statements by Federal Reserve officials, watching for clues that the economy and prices are on a different trajectory than had been thought, which would have implications for the stance of monetary policy.

Changes in short-term interest rates will influence long-term interest rates, such as those on Treasury notes, corporate bonds, fixed-rate mortgages, and auto and other consumer loans. Long-term rates are affected not only by changes in current short-term rates but also by expectations about short-term rates over the rest of the life of the long-term contract. Generally, economic news or statements by officials will have a greater impact on short-term interest rates than on longer rates because they typically have a bearing on the course of the economy and monetary policy over a shorter period; however, the impact on long rates can also be considerable because the news has clear implications for the expected course of short-term rates over a long period.

Lower interest rates in the United States will lead to a decline in the exchange value of the dollar, prompting an increase in the price of imports and a decline in the price of exports.

Changes in long-term interest rates also affect stock prices, which can have a pronounced effect on household wealth. Investors try to keep their investment returns on stocks in line with the return on bonds, after allowing for the greater riskiness of stocks. For example, if long-term interest rates decline, then, all else being equal, returns on stocks will exceed returns on bonds and encourage investors to purchase stocks and bid up stock prices to the point at which expected risk-adjusted returns on stocks are once again aligned with returns on bonds. Moreover, lower interest rates may convince investors that the economy will be stronger and profits higher in the near future, which should further lift equity prices.

Furthermore, changes in monetary policy affect the exchange value of the dollar on currency markets. For example, if interest rates rise in the United States, yields on dollar assets will look more favorable, which will lead to bidding up of the dollar on foreign exchange markets. The higher dollar will lower the cost of imports to U.S. residents and raise the price of U.S. exports to those living outside the United States. Conversely, lower interest rates in the United States will lead to a decline in the exchange value of the dollar, prompting an increase in the price of imports and a decline in the price of exports.

Changes in the value of financial assets, whether the result of an actual or expected change in monetary policy, will affect a wide range of spending decisions. For example, a drop in interest rates, a lower exchange value of

the dollar, and higher stock prices will stimulate various types of spending. Investment projects that businesses believed would be only marginally profitable will become more attractive with lower financing costs. Lower consumer loan rates will elicit greater demand for consumer goods, especially bigger-ticket items such as motor vehicles. Lower mortgage rates will make housing more affordable and lead to more home purchases. They will also encourage mortgage refinancing, which will reduce ongoing housing costs and enable households to purchase other goods. When refinancing, some homeowners may withdraw a portion of their home equity to pay for other things, such as a motor vehicle, other consumer goods, or a long-desired vacation trip. Higher stock prices can also add to household wealth and to the ability to make purchases that had previously seemed beyond reach. The reduction in the value of the dollar associated with a drop in interest rates will tend to boost U.S. exports by lowering the cost of U.S. goods and services in foreign markets. It will also make imported goods more expensive, which will encourage businesses and households to purchase domestically produced goods instead. All of these responses will strengthen growth in aggregate demand. A tightening of monetary policy will have the opposite effect on spending and will moderate growth of aggregate demand.

If the economy slows and employment softens, policy makers will be inclined to ease monetary policy to stimulate aggregate demand.

If the economy slows and employment softens, policy makers will be inclined to ease monetary policy to stimulate aggregate demand. When growth in aggregate demand is boosted above growth in the economy's potential to produce, slack in the economy will be absorbed and employment will return to a more sustainable path. In contrast, if the economy is showing signs of overheating and inflation pressures are building, the Federal Reserve will be inclined to counter these pressures by tightening monetary policy—to bring growth in aggregate demand below that of the economy's potential to produce—for as long as necessary to defuse the inflationary pressures and put the economy on a path to sustainable expansion.

While these policy choices seem reasonably straightforward, monetary policy makers routinely face certain notable uncertainties. First, the actual position of the economy and growth in aggregate demand at any point in time are only partially known, as key information on spending, production, and prices becomes available only with a lag. Therefore, policy makers must rely on estimates of these economic variables when assessing the appropriate course of policy, aware that they could act on the basis of misleading information. Second, exactly how a given adjustment in the federal funds rate will affect growth in aggregate demand—in terms of both the overall magnitude and the timing of its impact—is never certain. Economic models can provide rules of thumb for how the economy will respond, but these rules of thumb are subject to statistical error. Third, the growth in aggregate supply, often called the growth in potential

output, cannot be measured with certainty. Key here is the growth of the labor force and associated labor input, as well as underlying growth in labor productivity. Growth in labor input typically can be measured with more accuracy than underlying productivity; for some time, growth in labor input has tended to be around the growth in the overall population of 1 percentage point per year. However, underlying productivity growth has varied considerably over recent decades, from approximately 1 percent or so per year to somewhere in the neighborhood of 3 percent or even higher, getting a major boost during the mid- and late 1990s from applications of information technology and advanced management systems. If, for example, productivity growth is 2 percent per year, then growth in aggregate supply would be the sum of this amount and labor input growth of 1 percent—that is, 3 percent per year. In which case, growth in aggregate demand in excess of 3 percent per year would result in a pickup in growth in employment in excess of that of the labor force and a reduction in unemployment. In contrast, growth in aggregate demand below 3 percent would result in a softening of the labor market and, in time, a reduction in inflationary pressures.

If the economy is showing signs of overheating and inflation pressures are building, the Federal Reserve will be inclined to counter these pressures by tightening monetary policy.

Limitations of Monetary Policy

Monetary policy is not the only force acting on output, employment, and prices. Many other factors affect aggregate demand and aggregate supply and, consequently, the economic position of households and businesses. Some of these factors can be anticipated and built into spending and other economic decisions, and some come as a surprise. On the demand side, the government influences the economy through changes in taxes and spending programs, which typically receive a lot of public attention and are therefore anticipated. For example, the effect of a tax cut may precede its actual implementation as businesses and households alter their spending in anticipation of the lower taxes. Also, forward-looking financial markets may build such fiscal events into the level and structure of interest rates, so that a stimulative measure, such as a tax cut, would tend to raise the level of interest rates even before the tax cut becomes effective, which will have a restraining effect on demand and the economy before the fiscal stimulus is actually applied.

Other changes in aggregate demand and supply can be totally unpredictable and influence the economy in unforeseen ways. Examples of such shocks on the demand side are shifts in consumer and business confidence, and changes in the lending posture of commercial banks and other creditors. Lessened confidence regarding the outlook for the economy and labor market or more restrictive lending conditions tend to curb business and household spending. On the supply side, natural disasters, disruptions in the oil market that reduce supply, agricultural losses, and slowdowns in

productivity growth are examples of adverse supply shocks. Such shocks tend to raise prices and reduce output. Monetary policy can attempt to counter the loss of output or the higher prices but cannot fully offset both.

In practice, as previously noted, monetary policy makers do not have up-to-the-minute information on the state of the economy and prices. Useful information is limited not only by lags in the construction and availability of key data but also by later revisions, which can alter the picture considerably. Therefore, although monetary policy makers will eventually be able to offset the effects that adverse demand shocks have on the economy, it will be some time before the shock is fully recognized and—given the lag between a policy action and the effect of the action on aggregate demand—an even longer time before it is countered. Add to this the uncertainty about how the economy will respond to an easing or tightening of policy of a given magnitude, and it is not hard to see how the economy and prices can depart from a desired path for a period of time.

The statutory goals of maximum employment and stable prices are easier to achieve if the public understands those goals and believes that the Federal Reserve will take effective measures to achieve them.

The statutory goals of maximum employment and stable prices are easier to achieve if the public understands those goals and believes that the Federal Reserve will take effective measures to achieve them. For example, if the Federal Reserve responds to a negative demand shock to the economy with an aggressive and transparent easing of policy, businesses and consumers may believe that these actions will restore the economy to full employment; consequently, they may be less inclined to pull back on spending because of concern that demand may not be strong enough to warrant new business investment or that their job prospects may not warrant the purchase of big-ticket household goods. Similarly, a credible anti-inflation policy will lead businesses and households to expect less wage and price inflation; workers then will not feel the same need to protect themselves by demanding large wage increases, and businesses will be less aggressive in raising their prices, for fear of losing sales and profits. As a result, inflation will come down more rapidly, in keeping with the policy-related slowing in growth of aggregate demand, and will give rise to less slack in product and resource markets than if workers and businesses continued to act as if inflation were not going to slow.

Guides to Monetary Policy

Although the goals of monetary policy are clearly spelled out in law, the means to achieve those goals are not. Changes in the FOMC's target federal funds rate take some time to affect the economy and prices, and it is often far from obvious whether a selected level of the federal funds rate will achieve those goals. For this reason, some have suggested that the Federal Reserve pay close attention to guides that are intermediate between its operational target—the federal funds rate—and the economy.

Among those frequently mentioned are monetary aggregates, the level and structure of interest rates, the so-called Taylor rule (discussed on page 23), and foreign exchange rates. Some suggest that one of these guides be selected as an intermediate target—that is, that a specific formal objective be set for the intermediate target and pursued aggressively with the policy instruments. Others suggest that these guides be used more as indictors, to be monitored regularly; in other words, the Federal Reserve could establish a reference path for the intermediate variable that it thought to be consistent with achieving the final goals of monetary policy, and actual outcomes departing appreciably from that path would be seen as suggesting that the economy might be drifting off course and that a policy adjustment might be necessary.

Monetary Aggregates

Monetary aggregates have at times been advocated as guides to monetary policy on the grounds that they may have a fairly stable relationship with the economy and can be controlled to a reasonable extent by the central bank, either through control over the supply of balances at the Federal Reserve or the federal funds rate. An increase in the federal funds rate (and other short-term interest rates), for example, will reduce the attractiveness of holding money balances relative to now higher-yielding money market instruments and thereby reduce the amount of money demanded and slow growth of the money stock. There are a few measures of the money stock—ranging from the transactions-dominated M1 to the broader M2 and M3 measures, which include other liquid balances—and these aggregates have different behaviors. (See page 22 for a description of the composition of the monetary aggregates.)

Ordinarily, the rate of money growth sought over time would be equal to the rate of nominal GDP growth implied by the objective for inflation and the objective for growth in real GDP. For example, if the objective for inflation is 1 percent in a given year and the rate of growth in real GDP associated with achieving maximum employment is 3 percent, then the guideline for growth in the money stock would be 4 percent. However, the relation between the growth in money and the growth in nominal GDP, known as "velocity," can vary, often unpredictably, and this uncertainty can add to difficulties in using monetary aggregates as a guide to policy. Indeed, in the United States and many other countries with advanced financial systems over recent decades, considerable slippage and greater complexity in the relationship between money and GDP have made it more difficult to use monetary aggregates as guides to policy. In addition, the narrow and broader aggregates often give very different signals about the need to adjust policy. Accordingly, monetary aggregates have taken on less importance in policy making over time.

The Components of the Monetary Aggregates

The Federal Reserve publishes data on three monetary aggregates. The first, M1, is made up of types of money commonly used for payment, basically currency and checking deposits. The second, M2, includes M1 plus balances that generally are similar to transaction accounts and that, for the most part, can be converted fairly readily to M1 with little or no loss of principal. The M2 measure is thought to be held primarily by households. The third aggregate, M3, includes M2 plus certain accounts that are held by entities other than individuals and are issued by banks and thrift institutions to augment M2-type balances in meeting credit demands; it also includes balances in money market mutual funds held by institutional investors.

The aggregates have had different roles in monetary policy as their reliability as guides has changed. The following details their principal components:

M1 Currency (and traveler's checks)
Demand deposits
NOW and similar interest-earning checking accounts

M2 M1
Savings deposits and money market deposit accounts
Small time deposits[1]
Retail money market mutual fund balances[2]

M3 M2
Large time deposits
Institutional money market mutual fund balances
Repurchase agreements
Eurodollars

1. Time deposits in amounts of less than $100,000, excluding balances in IRA and Keogh accounts at depository institutions.
2. Excludes balances held in IRA and Keogh accounts with money market mutual funds.

Interest Rates

Interest rates have frequently been proposed as a guide to policy, not only because of the role they play in a wide variety of spending decisions but also because information on interest rates is available on a real-time basis. Arguing against giving interest rates the primary role in guiding monetary policy is uncertainty about exactly what level or path of interest rates is consistent with the basic goals of monetary policy. The appropriate level of interest rates will vary with the stance of fiscal policy, changes in the pattern of household and business spending, productivity growth, and economic developments abroad. It can be difficult not only to gauge the strength of these forces but also to translate them into a path for interest rates.

The slope of the yield curve (that is, the difference between the interest rate on longer-term and shorter-term instruments) has also been suggested as a guide to monetary policy. Whereas short-term interest rates are strongly influenced by the current setting of the policy instrument, longer-term interest rates are influenced by expectations of future short-term interest rates and thus by the longer-term effects of monetary policy on inflation and output. For example, a yield curve with a steeply positive slope (that is, longer-term interest rates far above short-term rates) may be a signal that participants in the bond market believe that monetary policy has become too expansive and thus, without a monetary policy correction, more inflationary. Conversely, a yield curve with a downward slope (short-term rates above longer rates) may be an indication that policy is too restrictive, perhaps risking an unwanted loss of output and employment. However, the yield curve is also influenced by other factors, including prospective fiscal policy, developments in foreign exchange markets, and expectations about the future path of monetary policy. Thus, signals from the yield curve must be interpreted carefully.

The Taylor Rule

The "Taylor rule," named after the prominent economist John Taylor, is another guide to assessing the proper stance of monetary policy. It relates the setting of the federal funds rate to the primary objectives of monetary policy—that is, the extent to which inflation may be departing from something approximating price stability and the extent to which output and employment may be departing from their maximum sustainable levels. For example, one version of the rule calls for the federal funds rate to be set equal to the rate thought to be consistent in the long run with the achievement of full employment and price stability plus a component based on the gap between current inflation and the inflation objective less a component based on the shortfall of actual output from the full-employment level. If inflation is picking up, the Taylor rule prescribes

the amount by which the federal funds rate would need to be raised or, if output and employment are weakening, the amount by which it would need to be lowered. The specific parameters of the formula are set to describe actual monetary policy behavior over a period when policy is thought to have been fairly successful in achieving its basic goals.

Although this guide has appeal, it too has shortcomings. The level of short-term interest rates associated with achieving longer-term goals, a key element in the formula, can vary over time in unpredictable ways. Moreover, the current rate of inflation and position of the economy in relation to full employment are not known because of data lags and difficulties in estimating the full-employment level of output, adding another layer of uncertainty about the appropriate setting of policy.

Foreign Exchange Rates

Exchange rate movements are an important channel through which monetary policy affects the economy, and exchange rates tend to respond promptly to a change in the federal funds rate. Moreover, information on exchange rates, like information on interest rates, is available continuously throughout the day.

Interpreting the meaning of movements in exchange rates, however, can be difficult. A decline in the foreign exchange value of the dollar, for example, could indicate that monetary policy has become, or is expected to become, more accommodative, resulting in inflation risks. But exchange rates respond to other influences as well, notably developments abroad; so a weaker dollar on foreign exchange markets could instead reflect higher interest rates abroad, which make other currencies more attractive and have fewer implications for the stance of U.S. monetary policy and the performance of the U.S. economy. Conversely, a strengthening of the dollar on foreign exchange markets could reflect a move to a more restrictive monetary policy in the United States—or expectations of such a move. But it also could reflect expectations of a lower path for interest rates elsewhere or a heightened perception of risk in foreign financial assets relative to U.S. assets.

Some have advocated taking the exchange rate guide a step further and using monetary policy to stabilize the dollar's value in terms of a particular currency or in terms of a basket of currencies. However, there is a great deal of uncertainty about which level of the exchange rate is most consistent with the basic goals of monetary policy, and selecting the wrong rate could lead to a protracted period of deflation and economic slack or to an overheated economy. Also, attempting to stabilize the exchange rate in the face of a disturbance from abroad would short-circuit the cushioning effect that the associated movement in the exchange rate would have on the U.S. economy.

Conclusion

All of the guides to monetary policy discussed here have something to do with the transmission of monetary policy to the economy. All have certain advantages; however, none has shown so consistently close a relationship with the ultimate goals of monetary policy that it can be relied on alone. Consequently, monetary policy makers have tended to use a broad range of indicators—those mentioned above along with many others, including the actual behavior of output and prices—to judge trends in the economy and to assess the stance of monetary policy.

Such an eclectic approach enables the Federal Reserve and other central banks to use all the available information in conducting monetary policy. This tack may be especially important as market structures and economic processes change in ways that reduce the utility of any single indictor. However, a downside to such an approach is the difficulty it poses in communicating the central bank's intentions to the public; the lack of a relatively simple set of procedures may make it difficult for the public to understand the actions of the Federal Reserve and to judge whether those actions are consistent with achieving its statutory goals. This downside risk can be mitigated if the central bank develops a track record of achieving favorable policy outcomes when no single guide to policy has proven reliable.

3 The Implementation of Monetary Policy

The Federal Reserve exercises considerable control over the demand for and supply of balances that depository institutions hold at the Reserve Banks. In so doing, it influences the federal funds rate and, ultimately, employment, output, and prices.

The Federal Reserve implements U.S. monetary policy by affecting conditions in the market for balances that depository institutions hold at the Federal Reserve Banks. The operating objectives or targets that it has used to effect desired conditions in this market have varied over the years. At one time, the FOMC sought to achieve a specific quantity of balances, but now it sets a target for the interest rate at which those balances are traded between depository institutions—the federal funds rate. (See "Operational Approaches over the Years" on page 28.) By conducting open market operations, imposing reserve requirements, permitting depository institutions to hold contractual clearing balances, and extending credit through its discount window facility, the Federal Reserve exercises considerable control over the demand for and supply of Federal Reserve balances and the federal funds rate. Through its control of the federal funds rate, the Federal Reserve is able to foster financial and monetary conditions consistent with its monetary policy objectives.

The Market for Federal Reserve Balances

The Federal Reserve influences the economy through the market for balances that depository institutions maintain in their accounts at Federal Reserve Banks. Depository institutions make and receive payments on behalf of their customers or themselves in these accounts. The end-of-day balances in these accounts are used to meet reserve and other balance requirements. If a depository institution anticipates that it will end the day with a larger balance than it needs, it can reduce that balance in several ways, depending on how long it expects the surplus to persist. For example, if it expects the surplus to be temporary, the institution can lend excess balances in financing markets, such as the market for repurchase agreements or the market for federal funds.

Operational Approaches over the Years

The Federal Reserve can try to achieve a desired quantity of balances at the Federal Reserve Banks or a desired price of those balances (the federal funds rate), but it may not be able to achieve both at once. The greater the emphasis on a quantity objective, the more short-run changes in the demand for balances will influence the federal funds rate. Conversely, the greater the emphasis on a funds-rate objective, the more shifts in demand will influence the quantity of balances at the Federal Reserve. Over the years, the Federal Reserve has used variations of both of these operational approaches.

During most of the 1970s, the Federal Reserve targeted the price of Federal Reserve balances. The FOMC would choose a target federal funds rate that it thought would be consistent with its objective for M1 growth over short intervals of time. The funds-rate target would be raised or lowered if M1 growth significantly exceeded or fell short of the desired rate. At times, large rate movements were needed to bring money growth back in line with the target, but the extent of the necessary policy adjustment was not always gauged accurately. Moreover, there appears to have been some reluctance to permit substantial variation in the funds rate. As a result, the FOMC did not have great success in combating the increase in inflationary pressures that resulted from oil-price shocks and excessive money growth over the decade.

By late 1979, the FOMC recognized that a change in tactics was necessary. In October, the Federal Reserve began to target the quantity of reserves—the sum of balances at the Federal Reserve and cash in the vaults of depository institutions that is used to meet reserve requirements—to achieve greater control over M1 and bring down inflation. In particular, the operational objective for open market operations was a specific level of nonborrowed reserves, or total reserves less the quantity of discount window borrowing. A predetermined target path for nonborrowed reserves was based on the FOMC's objectives for M1. If M1 grew faster than the objective, required reserves, which were linked to M1 through the required reserve ratios, would expand more quickly than nonborrowed reserves. With the fixed supply of nonborrowed reserves falling short of demand, banks would bid up the

federal funds rate, sometimes sharply. The rise in short-term interest rates would eventually damp M1 growth, and M1 would be brought back toward its targeted path.

By late 1982, it had become clear that the combination of interest rate deregulation and financial innovation had weakened the historical link between M1 and the economic objectives of monetary policy. The FOMC began to make more discretionary decisions about money market conditions, using a wider array of economic and financial variables to judge the need for adjustments in short-term interest rates. In the day-to-day implementation of open market operations, this change was manifested in a shift of focus from a nonborrowed-reserve target to a borrowed-reserve target. The Federal Reserve routinely supplied fewer nonborrowed reserves than the estimated demand for total reserves, thus forcing depository institutions to meet their remaining need for reserves by borrowing at the discount window. The total amount borrowed was limited, however, even though the discount rate was generally below the federal funds rate, because access to discount window credit was restricted. In particular, depository institutions were required to pursue all other reasonably available sources of funds, including those available in the federal funds market, before credit was granted. During the time it was targeting borrowed reserves, the Federal Reserve influenced the level of the federal funds rate by controlling the extent to which depository institutions had to turn to the discount window. When it wanted to ease monetary policy, it would reduce the borrowed-reserve target and supply more nonborrowed reserves to meet estimated demand. With less pressure to borrow from the discount window, depository institutions would bid less aggressively for balances at the Federal Reserve and the federal funds rate would fall.

Beginning in the mid-1980s, spreading doubts about the financial health of some depository institutions led to an increasing reluctance on the part of many institutions to borrow at the discount window, thus weakening the link between borrowing and the federal funds rate. Consequently, the Federal Reserve increasingly sought to attain a specific level of the federal funds rate rather than a targeted amount of borrowed reserves. In July 1995, the FOMC began to announce its target for the federal funds rate.

In the federal funds market, depository institutions actively trade balances held at the Federal Reserve with each other, usually overnight, on an uncollateralized basis. Institutions with surplus balances in their accounts lend those balances to institutions in need of larger balances. The federal funds rate—the interest rate at which these transactions occur—is an important benchmark in financial markets. Daily fluctuations in the federal funds rate reflect demand and supply conditions in the market for Federal Reserve balances.

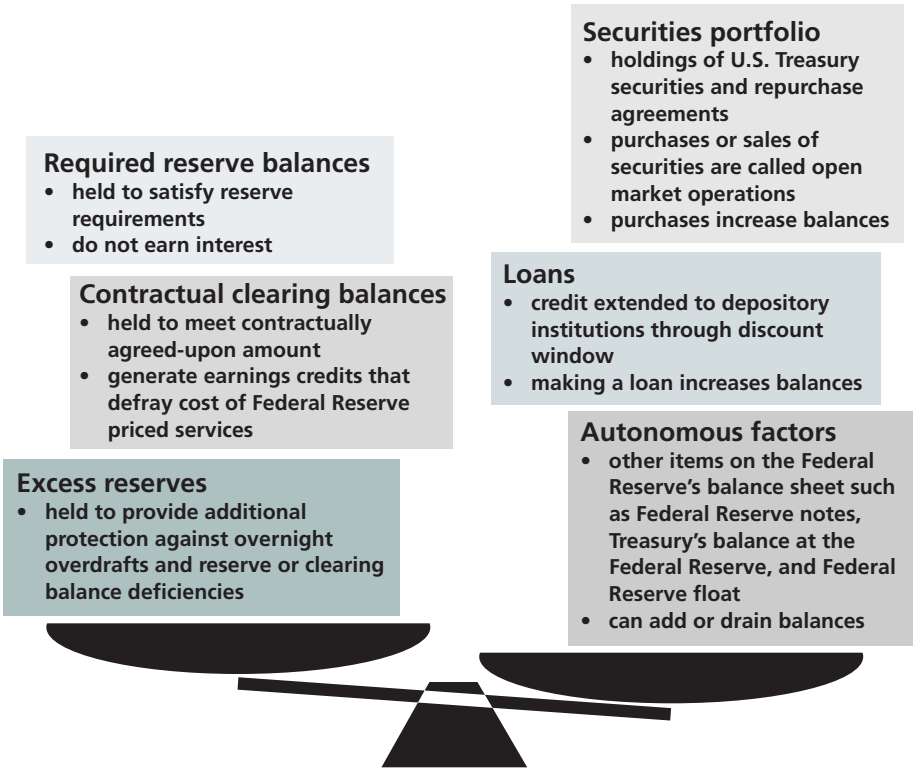
Demand for Federal Reserve Balances

The demand for Federal Reserve balances has three components: required reserve balances, contractual clearing balances, and excess reserve balances.

Required Reserve Balances

Required reserve balances are balances that a depository institution must hold with the Federal Reserve to satisfy its reserve requirement. Reserve requirements are imposed on all depository institutions—which include commercial banks, savings banks, savings and loan associations, and credit unions—as well as U.S. branches and agencies of foreign banks and other

The Market for Balances at the Federal Reserve



domestic banking entities that engage in international transactions. Since the early 1990s, reserve requirements have been applied only to transaction deposits, which include demand deposits and interest-bearing accounts that offer unlimited checking privileges. An institution's reserve requirement is a fraction of such deposits; the fraction—the required reserve ratio—is set by the Board of Governors within limits prescribed in the Federal Reserve Act. A depository institution's reserve requirement expands or contracts with the level of its transaction deposits and with the required reserve ratio set by the Board. In practice, the changes in required reserves reflect movements in transaction deposits because the Federal Reserve adjusts the required reserve ratio only infrequently.

A depository institution satisfies its reserve requirement by its holdings of vault cash (currency in its vault) and, if vault cash is insufficient to meet the requirement, by the balance maintained directly with a Federal Reserve Bank or indirectly with a pass-through correspondent bank (which in turn holds the balances in its account at the Federal Reserve). The difference between an institution's reserve requirement and the vault cash used to meet that requirement is called the required reserve balance. If the balance maintained by the depository institution does not satisfy its reserve balance requirement, the deficiency may be subject to a charge.

Contractual Clearing Balances

Depository institutions use their accounts at Federal Reserve Banks not only to satisfy their reserve balance requirements but also to clear many financial transactions. Given the volume and unpredictability of transactions that clear through their accounts every day, depository institutions seek to hold an end-of-day balance that is high enough to protect against unexpected debits that could leave their accounts overdrawn at the end of the day and against any resulting charges, which could be quite large. If a depository institution finds that targeting an end-of-day balance equal to its required reserve balance provides insufficient protection against overdrafts, it may establish a contractual clearing balance (sometimes referred to as a required clearing balance).

A contractual clearing balance is an amount that a depository institution agrees to hold at its Reserve Bank in addition to any required reserve balance. In return, the depository institution earns implicit interest, in the form of earnings credits, on the balance held to satisfy its contractual clearing balance. It uses these credits to defray the cost of the Federal Reserve services it uses, such as check clearing and wire transfers of funds and securities. If the depository institution fails to satisfy its contractual requirement, the deficiency is subject to a charge.

Excess Reserve Balances

A depository institution may hold balances at its Federal Reserve Bank in addition to those it must hold to meet its reserve balance requirement and its contractual clearing balance; these balances are called excess reserve balances (or excess reserves). In general, a depository institution attempts to keep excess reserve balances at low levels because balances at the Federal Reserve do not earn interest. However, a depository institution may aim to hold some positive excess reserve balances at the end of the day as additional protection against an overnight overdraft in its account or the risk of failing to hold enough balances to satisfy its reserve or clearing balance requirement. This desired cushion of balances can vary considerably from day to day, depending in part on the volume and uncertainty about payments flowing through the institution's account. The daily demand for excess reserve balances is the least-predictable component of the demand for balances. (See table 3.1 for data on required reserve balances, contractual clearing balances, and excess reserve balances.)

Purchases or sales of securities by the Federal Reserve, whether outright or temporary, are called open market operations.

Table 3.1

Measures of aggregate balances, 2001–2004

Billions of dollars; annual averages of daily data

Year	Required reserve balances	Contractual clearing balances	Excess reserve balances
2001	7.2	7.0	2.8
2002	8.0	9.7	1.5
2003	10.0	11.0	1.8
2004	11.0	10.4	1.6

Supply of Federal Reserve Balances

The supply of Federal Reserve balances to depository institutions comes from three sources: the Federal Reserve's portfolio of securities and repurchase agreements; loans from the Federal Reserve through its discount window facility; and certain other items on the Federal Reserve's balance sheet known as autonomous factors.

Securities Portfolio

The most important source of balances to depository institutions is the Federal Reserve's portfolio of securities. The Federal Reserve buys and sells securities either on an outright (also called permanent) basis or temporarily in the form of repurchase agreements and reverse repurchase

agreements. Purchases or sales of securities by the Federal Reserve, whether outright or temporary, are called open market operations, and they are the Federal Reserve's principal tool for influencing the supply of balances at the Federal Reserve Banks. Open market operations are conducted to align the supply of balances at the Federal Reserve with the demand for those balances at the target rate set by the FOMC.

Purchasing securities or arranging a repurchase agreement increases the quantity of balances because the Federal Reserve creates balances when it credits the account of the seller's depository institution at the Federal Reserve for the amount of the transaction; there is no corresponding offset in another institution's account. Conversely, selling securities or conducting a reverse repurchase agreement decreases the quantity of Federal Reserve balances because the Federal Reserve extinguishes balances when it debits the account of the purchaser's depository institution at the Federal Reserve; there is no corresponding increase in another institution's account. In contrast, when financial institutions, business firms, or individuals buy or sell securities among themselves, the credit to the account of the seller's depository institution is offset by the debit to the account of the purchaser's depository institution; so existing balances held at the Federal Reserve are redistributed from one depository institution to another without changing the total available.

The supply of Federal Reserve balances increases when depository institutions borrow from the Federal Reserve's discount window.

Discount Window Lending

The supply of Federal Reserve balances increases when depository institutions borrow from the Federal Reserve's discount window. Access to discount window credit is established by rules set by the Board of Governors, and loans are made at interest rates set by the Reserve Banks and approved by the Board. Depository institutions decide to borrow based on the level of the lending rate and their liquidity needs. Beginning in early 2003, rates for discount window loans have been set above prevailing market rates (see "Major Revision to Discount Window Programs" on page 47). As a result, depository institutions typically will borrow from the discount window in significant volume only when overall market conditions have tightened enough to push the federal funds rate up close to the discount rate. Overall market conditions tend to tighten to such an extent only infrequently, so the volume of balances supplied through the discount window is usually only a small portion of the total supply of Federal Reserve balances. However, at times of market disruptions, such as after the terrorist attacks in 2001, loans extended through the discount window can supply a considerable volume of Federal Reserve balances.

Autonomous Factors

The supply of balances can vary substantially from day to day because of movements in other items on the Federal Reserve's balance sheet (table

3.2). These so-called autonomous factors are generally outside the Federal Reserve's direct day-to-day control. The most important of these factors are Federal Reserve notes, the Treasury's balance at the Federal Reserve, and Federal Reserve float.

The largest autonomous factor is Federal Reserve notes. When a depository institution needs currency, it places an order with a Federal Reserve Bank. When the Federal Reserve fills the order, it debits the account of the depository institution at the Federal Reserve, and total Federal Reserve balances decline. The amount of currency demanded tends to grow over time, in part reflecting increases in nominal spending as the economy grows. Consequently, an increasing volume of balances would be extinguished, and the federal funds rate would rise, if the Federal Reserve did not offset the contraction in balances by purchasing securities. Indeed, the expansion of Federal Reserve notes is the primary reason that the Federal Reserve's holdings of securities grow over time.

Table 3.2

Consolidated balance sheet of the Federal Reserve Banks, December 31, 2004

Millions of dollars

Assets		Liabilities	
Securities	717,819	Federal Reserve notes	719,436
Repurchase agreements	33,000	Reverse repurchase agreements	30,783
Loans	43	Balance, U.S. Treasury account	5,912
Float	927	Other liabilities and capital	27,745
All other assets	56,130	Balances, all depository institutions	24,043

Another important factor is the balance in the U.S. Treasury's account at the Federal Reserve. The Treasury draws on this account to make payments by check or direct deposit for all types of federal spending. When these payments clear, the Treasury's account is reduced and the account of the depository institution for the person or entity that receives the funds is increased. The Treasury is not a depository institution, so a payment by the Treasury to the public (for example, a Social Security payment) raises the volume of Federal Reserve balances available to depository institutions. Movements in the Treasury's balance at the Federal Reserve tend to be less predictable following corporate and individual tax dates, especially in the weeks following the April 15 deadline for federal income tax payments.

Federal Reserve float is created when the account of the depository institution presenting a check for payment is credited on a different day than

the account of the depository institution on which the check is drawn is debited. This situation can arise because credit is granted to the presenting depository institution on a preset schedule, whereas the paying institution's account is not debited until the check is presented to it. Float temporarily adds Federal Reserve balances when there is a delay in debiting the paying institution's account because the two depository institutions essentially are credited with the same balances. Float temporarily drains balances when the paying institution's account is debited before the presenting institution receives credit under the schedule. Float tends to be quite high and variable following inclement weather that disrupts the normal check-delivery process.

Controlling the Federal Funds Rate

Open market operations are the most powerful and often-used tool for controlling the federal funds rate.

The Federal Reserve's conduct of open market operations, its policies related to required reserves and contractual clearing balances, and its lending through the discount window all play important roles in keeping the federal funds rate close to the FOMC's target rate. Open market operations are the most powerful and often-used tool for controlling the funds rate. These operations, which are arranged nearly every business day, are designed to bring the supply of Federal Reserve balances in line with the demand for those balances at the FOMC's target rate. Required reserve balances and contractual clearing balances facilitate the conduct of open market operations by creating a predictable demand for Federal Reserve balances. If, even after an open market operation is arranged, the supply of balances falls short of demand, then discount window lending provides a mechanism for expanding the supply of balances to contain pressures on the funds rate.

Reserve balance requirements and contractual clearing balances need to be met only on average over a so-called reserve maintenance period, not each day. This structure gives depository institutions considerable flexibility in managing their end-of-day balances at the Federal Reserve from one day to the next. This flexibility helps smooth fluctuations in the federal funds rate. If a depository institution finds that its balance at the Federal Reserve is unexpectedly high on one day (for instance, because a customer made an unexpected deposit or an expected payment was not made), it does not have to offer to lend the extra balance at very low rates; it can absorb the surplus by choosing to hold lower balances in the remaining days of the maintenance period and still meet its balance requirements. Holding a lower balance on a subsequent day of the period does not necessarily increase the likelihood that the depository institution will incur an overnight overdraft if the sum of its required reserve balance and contractual clearing balance is high relative to its payment needs. This flexibility in managing account balances protects against variations in the

demand for and supply of Federal Reserve balances that would otherwise put pressure on the federal funds rate.

Reserve balance requirements and contractual clearing balances also help create a predictable demand for balances at the Federal Reserve. Without reserve balance requirements or contractual clearing balances, many depository institutions would still hold positive balances at the Federal Reserve to facilitate payments on behalf of themselves or their customers and to avoid having a negative balance in their account at the end of the day. The exact amount of balances that depository institutions want to hold at the Federal Reserve at the end of the day for clearing purposes can vary considerably from day to day, often depending on the volume and uncertainty of the payment flows through their accounts. These demands are very difficult for the Federal Reserve to forecast. When the level of reserve balance requirements, contractual clearing balances, or the sum of the two make it necessary for depository institutions to hold balances above the shifting and unpredictable level needed for clearing purposes, the Federal Reserve can more accurately determine the demand for Federal Reserve balances and, by manipulating the supply of Federal Reserve balances through open market operations, more readily attain the target funds rate.

The remainder of this chapter takes a more detailed look at open market operations, reserve requirements, contractual clearing balances, and the discount window.

Open Market Operations

In theory, the Federal Reserve could conduct open market operations by purchasing or selling any type of asset. In practice, however, most assets cannot be traded readily enough to accommodate open market operations. For open market operations to work effectively, the Federal Reserve must be able to buy and sell quickly, at its own convenience, in whatever volume may be needed to keep the federal funds rate at the target level. These conditions require that the instrument it buys or sells be traded in a broad, highly active market that can accommodate the transactions without distortions or disruptions to the market itself.

The market for U.S. Treasury securities satisfies these conditions. The U.S. Treasury securities market is the broadest and most active of U.S. financial markets. Transactions are handled over the counter, not on an organized exchange. Although most of the trading occurs in New York City, telephone and computer connections link dealers, brokers, and customers—regardless of their location—to form a global market.

Composition of the Federal Reserve's Portfolio

The overall size of the Federal Reserve's holdings of Treasury securities depends principally on the growth of Federal Reserve notes; however, the amounts and maturities of the individual securities held depends on the FOMC's preferences for liquidity. The Federal Reserve has guidelines that limit its holdings of individual Treasury securities to a percentage of the total amount outstanding. These guidelines are designed to help the Federal Reserve manage the liquidity and average maturity of the System portfolio. The percentage limits under these guidelines are larger for shorter-dated issues than longer-dated ones. Consequently, a sizable share of the Federal Reserve's holdings is held in Treasury securities with remaining maturities of one year or less. This structure provides the Federal Reserve with the ability to alter the composition of its assets quickly when developments warrant. At the end of 2004, the Federal Reserve's holdings of Treasury securities were about evenly weighted between those with maturities of one year or less and those with maturities greater than one year (table 3.3).

Table 3.3

U.S. Treasury securities held in the Federal Reserve's open market account, December 31, 2004

Billions of dollars

Remaining maturity	U.S. Treasury securities
1 year or less	379.4
More than 1 year to 5 years	208.3
More than 5 years to 10 years	54.4
More than 10 years	75.8
Total	717.8

The Conduct of Open Market Operations

The Federal Reserve Bank of New York conducts open market operations for the Federal Reserve, under an authorization from the Federal Open Market Committee. The group that carries out the operations is commonly referred to as "the Open Market Trading Desk" or "the Desk." The Desk is permitted by the FOMC's authorization to conduct business with U.S. securities dealers and with foreign official and international institutions that maintain accounts at the Federal Reserve Bank of New York. The dealers with which the Desk transacts business are called primary dealers. The Federal Reserve requires primary dealers to meet the

capital standards of their primary regulators and satisfy other criteria consistent with being a meaningful and creditworthy counterparty. All open market operations transacted with primary dealers are conducted through an auction process.

Each day, the Desk must decide whether to conduct open market operations, and, if so, the types of operations to conduct. It examines forecasts of the daily supply of Federal Reserve balances from autonomous factors and discount window lending. The forecasts, which extend several weeks into the future, assume that the Federal Reserve abstains from open market operations. These forecasts are compared with projections of the demand for balances to determine the need for open market operations. The decision about the types of operations to conduct depends on how long a deficiency or surplus of Federal Reserve balances is expected to last. If staff projections indicate that the demand for balances is likely to exceed the supply of balances by a large amount for a number of weeks or months, the Federal Reserve may make outright purchases of securities or arrange longer-term repurchase agreements to increase supply. Conversely, if the projections suggest that demand is likely to fall short of supply, then the Federal Reserve may sell securities outright or redeem maturing securities to shrink the supply of balances.

Even after accounting for planned outright operations or long-term repurchase agreements, there may still be a short-term need to alter Federal Reserve balances. In these circumstances, the Desk assesses whether the federal funds rate is likely to remain near the FOMC's target rate in light of the estimated imbalance between supply and demand. If the funds rate is likely to move away from the target rate, then the Desk will arrange short-term repurchase agreements, which add balances, or reverse repurchase agreements, which drain balances, to better align the supply of and demand for balances. If the funds rate is likely to remain close to the target, then the Desk will not arrange a short-term operation. Short-term temporary operations are much more common than outright transactions because daily fluctuations in autonomous factors or the demand for excess reserve balances can create a sizable imbalance between the supply of and demand for balances that might cause the federal funds rate to move significantly away from the FOMC's target.

Outright Purchases and Sales

The Federal Reserve tends to conduct far more outright purchases than outright sales or redemptions of securities primarily because it must offset the drain of balances resulting from the public's increasing demand for Federal Reserve notes (table 3.4). When the Desk decides to buy securities in an outright operation, it first determines how much it wants to buy to address the mismatch between supply and demand. It then divides that

amount into smaller portions and makes a series of purchases in different segments of the maturity spectrum, rather than buying securities across all maturities at once, in order to minimize the impact on market prices.

When the projections indicate a need to drain Federal Reserve balances, the Desk may choose to sell securities or to redeem maturing securities. Sales of securities are extremely rare. By redeeming some maturing securities, rather than exchanging all of them for new issues, the Federal Reserve can reduce the size of its holdings gradually without having to enter the market. Redemptions drain Federal Reserve balances when the Treasury takes funds out of its accounts at depository institutions, transfers those funds to its account at the Federal Reserve, and then pays the Federal Reserve for the maturing issues.

Table 3.4

Federal Reserve System outright transactions, 2001–2004

Billions of dollars

Transaction	2001	2002	2003	2004
Purchases	68.5	54.2	36.8	50.5
Redemptions	26.9	—	—	—
Total	95.4	54.2	36.8	50.5

Purchases from and sales to foreign official and international customers enable the Federal Reserve to make small adjustments to its portfolio without formally entering the market. These transactions occur at market prices. The size of the buy or sell orders of these customers and the projected need for open market operations determine whether the Desk chooses to arrange these customer transactions directly with the Federal Reserve, in which case they affect Federal Reserve balances, or to act as agent by conducting the transactions in the market, with no effect on balances.

Repurchase Agreements

The Federal Reserve frequently arranges repurchase agreements to add Federal Reserve balances temporarily (table 3.5). In these transactions, it acquires a security from a primary dealer under an agreement to return the security on a specified date. Most repurchase agreements have an overnight term, although short-term repurchase agreements with maturities of two to thirteen days are also arranged to address shortages in Federal Reserve balances that are expected to extend over several days. Longer-term repurchase agreements are used to address more-persistent needs. The Federal Reserve accepts Treasury, federal agency, and mort-

gage-backed securities guaranteed by federal agencies as collateral for its repurchase agreements.

Table 3.5

Federal Reserve System temporary transactions, 2001–2004

Volume in billions of dollars

	2001		2002		2003		2004	
	Num.	Vol.	Num.	Vol.	Num.	Vol.	Num.	Vol.
Repurchase agreements[1]	305	1,497.7	262	1,143.1	288	1,522.9	299	1,876.9
Matched sale–purchase transactions/ Reverse repurchase agreements[2]	10	25.0	7	11.3	10	22.8	2	4.8

1. Includes all types of repurchase agreements.
2. Reverse repurchase agreements after 2003.

Reverse Repurchase Agreements

When the Federal Reserve needs to absorb Federal Reserve balances temporarily, it enters into reverse repurchase agreements with primary dealers. These transactions involve selling a Treasury security to a primary dealer under an agreement to receive the security back on a specified date. As in repurchase agreement transactions, these operations are arranged on an auction basis. When the Federal Reserve transfers the collateral (usually a Treasury bill) to the dealer, the account of the dealer's clearing bank at the Federal Reserve is debited, and total Federal Reserve balances decline. When the transaction unwinds, the account of the dealer's clearing bank is credited and total balances increase.

Every business day, the Federal Reserve also arranges reverse repurchase agreements with foreign official and international accounts. These institutions have accounts at the Federal Reserve Bank of New York to help manage their U.S. dollar payments and receipts. The Federal Reserve permits these institutions to invest cash balances overnight through these agreements.

A Typical Day in the Conduct of Open Market Operations

Each weekday, beginning at around 7:30 a.m., two groups of Federal Reserve staff members, one at the Federal Reserve Bank of New York and one at the Board of Governors in Washington, prepare independent projections of the supply of and demand for Federal Reserve balances.

The manager of the System Open Market Account and the group in New York are linked in a telephone conference call with members of the staff at the Board of Governors and with a Federal Reserve Bank president who is currently a member of the FOMC. Participants in the call discuss staff forecasts for Federal Reserve balances and recent developments in financial markets. They pay special attention to trading conditions in the federal funds market, particularly the level of the federal funds rate in relation to the FOMC's target. In light of this information, they determine a plan for open market operations. The decision is announced to the markets at around 9:30 a.m., at the same time that the Desk solicits offers from dealers. (Typically, longer-term repurchase agreements are arranged earlier in the morning, usually on a specific day of the week.) If an outright operation is also needed, it would typically be executed later in the morning, after the daily operation is complete.

Securities Lending

The Federal Reserve has a securities lending program designed to provide a secondary and temporary source of securities to the market in order to promote the smooth clearing of Treasury securities. Under this program, securities from the portfolio are offered for loan to primary dealers through an auction process each day at noon. The total amount available for an individual security is a fraction of the Federal Reserve's total holdings, and there are limits on the amount of securities that can be lent to a single dealer. As collateral, the dealer gives the Federal Reserve other securities, not cash; therefore, the Federal Reserve's lending operations do not affect the supply of Federal Reserve balances and are not considered open market operations.

Reserve requirements play a useful role in the conduct of open market operations by helping to ensure a predictable demand for Federal Reserve balances.

Reserve Requirements

Reserve requirements have long been a part of our nation's banking history. Depository institutions maintain a fraction of certain liabilities in reserve in specified assets. The Federal Reserve can adjust reserve requirements by changing required reserve ratios, the liabilities to which the ratios apply, or both. Changes in reserve requirements can have profound effects on the money stock and on the cost to banks of extending credit and are also costly to administer; therefore, reserve requirements are not adjusted frequently. Nonetheless, reserve requirements play a useful role in the conduct of open market operations by helping to ensure a predictable demand for Federal Reserve balances and thus enhancing the Federal Reserve's control over the federal funds rate.

Requiring depository institutions to hold a certain fraction of their deposits in reserve, either as cash in their vaults or as non-interest-bearing

balances at the Federal Reserve, does impose a cost on the private sector. The cost is equal to the amount of forgone interest on these funds—or at least on the portion of these funds that depository institutions hold only because of legal requirements and not to meet their customers' needs.

The burden of reserve requirements is structured to bear generally less heavily on smaller institutions. At every depository institution, a certain amount of reservable liabilities is exempt from reserve requirements, and a relatively low required reserve ratio is applied to reservable liabilities up to a specific level. The amounts of reservable liabilities exempt from reserve requirements and subject to the low required reserve ratio are adjusted annually to reflect growth in the banking system. Table 3.6 shows the reserve requirement ratios in effect in 2004.

The burden of reserve requirements is structured to bear generally less heavily on smaller institutions.

Table 3.6

Reserve requirement ratios, 2004

Category	Reserve requirement
Net transaction accounts	
$0 to $6.6 million	0 percent of amount
Over $6.6 million and up to $45.4 million	3 percent of amount
Over $45.4 million	$1,164,000 plus 10 percent of amount over $45.4 million
Nonpersonal time deposits	0 percent
Eurocurrency liabilities	0 percent

Changes in reserve requirements can affect the money stock, by altering the volume of deposits that can be supported by a given level of reserves, and bank funding costs. Unless it is accompanied by an increase in the supply of Federal Reserve balances, an increase in reserve requirements (through an increase in the required reserve ratio, for example) reduces excess reserves, induces a contraction in bank credit and deposit levels, and raises interest rates. It also pushes up bank funding costs by increasing the amount of non-interest-bearing assets that must be held in reserve. Conversely, a decrease in reserve requirements, unless accompanied by a reduction in Federal Reserve balances, initially leaves depository institutions with excess reserves, which can encourage an expansion of bank credit and deposit levels and reduce interest rates.

Recent History of Reserve Requirements

In the 1960s and 1970s, the Federal Reserve actively used reserve requirements as a tool of monetary policy in order to influence the expansion of

money and credit partly by manipulating bank funding costs. As financial innovation spawned new sources of bank funding, the Federal Reserve adapted reserve requirements to these new financial products. It changed required reserve ratios on specific bank liabilities that were most frequently used to fund new lending. Reserve requirements were also imposed on other, newly emerging liabilities that were the functional equivalents of deposits, such as Eurodollar borrowings. At times, it supplemented these actions by placing a marginal reserve requirement on large time deposits —that is, an additional requirement applied only to each new increment of these deposits.

As the 1970s unfolded, it became increasingly apparent that the structure of reserve requirements was becoming outdated. At this time, only banks that were members of the Federal Reserve System were subject to reserve requirements established by the Federal Reserve. The regulatory structure and competitive pressures during a period of high interest rates were putting an increasing burden on member banks. This situation fostered the growth of deposits, especially the newly introduced interest-bearing transaction deposits, at institutions other than member banks and led many banks to leave the Federal Reserve System. Given this situation, policy makers felt that reserve requirements needed to be applied to a broad group of institutions for more effective monetary control—that is, to strengthen the relationship between the amount of reserves supplied by the Federal Reserve and the overall quantity of money in the economy.

Changes in reserve requirements can affect the money stock and bank funding costs.

The Monetary Control Act of 1980 (MCA) ended the problem of membership attrition and facilitated monetary control by reforming reserve requirements. Under the act, all depository institutions are subject to reserve requirements set by the Federal Reserve, whether or not they are members of the Federal Reserve System. The Board of Governors may impose reserve requirements solely for the purpose of implementing monetary policy. The required reserve ratio may range from 8 percent to 14 percent on transaction deposits and from 0 percent to 9 percent on nonpersonal time deposits. The Board may also set reserve requirements on the net liabilities owed by depository institutions in the United States to their foreign affiliates or to other foreign banks. The MCA permits the Board, under certain circumstances, to establish supplemental and emergency reserve requirements, but these powers have never been exercised.

Following the passage of the MCA in 1980, reserve requirements were not adjusted for policy purposes for a decade. In December 1990, the required reserve ratio on nonpersonal time deposits was pared from 3 percent to 0 percent, and in April 1992 the 12 percent ratio on transaction deposits was trimmed to 10 percent. These actions were partly motivated by evidence suggesting that some lenders had adopted a more cautious approach to extending credit, which was increasing the cost and restricting the availability of credit to some types of borrowers. By reducing funding costs and thus

providing depository institutions with easier access to capital markets, the cuts in required reserve ratios put depository institutions in a better position to extend credit.

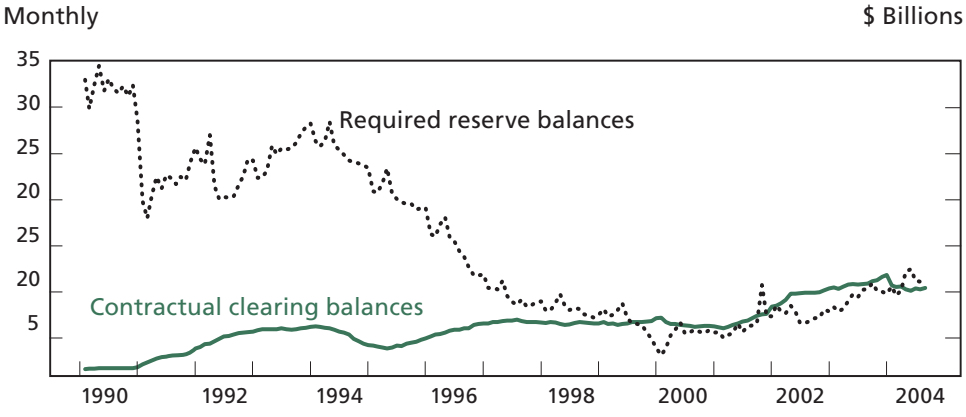
Although reserve requirement ratios have not been changed since the early 1990s, the level of reserve requirements and required reserve balances has fallen considerably since then because of the widespread implementation of retail sweep programs by depository institutions. Under such a program, a depository institution sweeps amounts above a predetermined level from a depositor's checking account into a special-purpose money market deposit account created for the depositor. In this way, the depository institution shifts funds from an account that is subject to reserve requirements to one that is not and therefore reduces its reserve requirement. With no change in its vault cash holdings, the depository institution can lower its required reserve balance, on which it earns no interest, and invest the funds formerly held at the Federal Reserve in interest-earning assets.

Contractual Clearing Balances

Contractual clearing balances, like required reserve balances, help to create a stable, predictable demand for Federal Reserve balances, which assists in the conduct of open market operations. In early 1981, the Federal Reserve Board established a policy that permitted all depository institutions to hold contractual clearing balances at the Federal Reserve Banks. Such balances, which were referred to as required clearing balances at the time, were established following the passage of the MCA to facilitate access to Federal Reserve priced services by depository institutions with zero or low required reserve balances. Use of these arrangements was minimal in the early 1980s because required reserve balances were sufficiently high to facilitate clearing and meet reserve requirements.

Chart 3.1

Balances at Federal Reserve Banks, 1990–2004

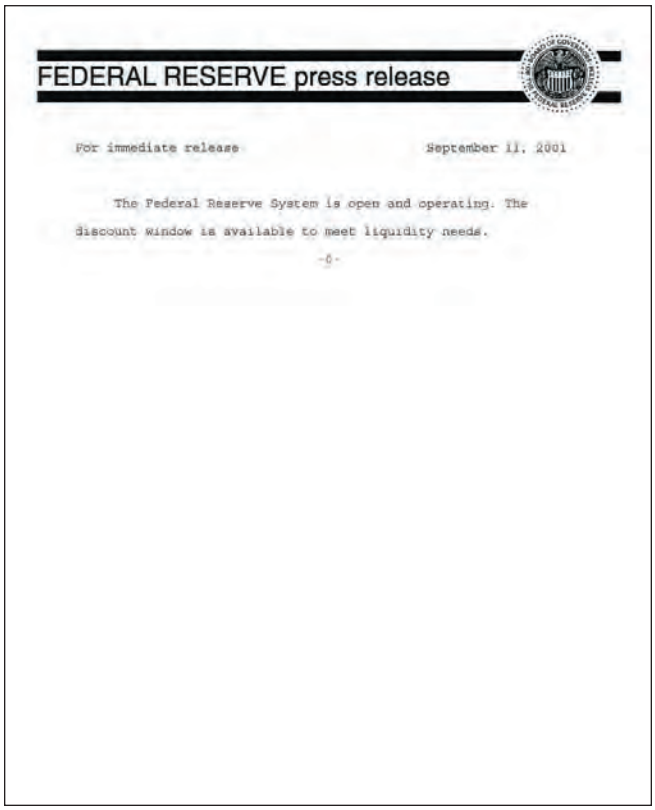


The use of contractual clearing balances rose considerably in the 1990s as required reserve balances dropped in the wake of the cuts in required reserve ratios early in the decade and the widespread implementation of retail sweep programs by depository institutions. The resulting reduction in required reserve balances left some depository institutions with insufficient protection against overnight overdrafts, so they established or expanded their contractual clearing balances. The rise in contractual clearing balances during the 1990s did not match the decline in required reserve balances, however, in part because depository institutions apparently did not need as large a cushion to protect against overnight overdrafts as was once provided by their required reserve balance. In addition, the ability of some depository institutions to expand their contractual clearing balances was limited by the extent to which they use Federal Reserve priced services.

The Discount Window

The Federal Reserve's lending at the discount window serves two primary functions. It complements open market operations in achieving the target federal funds rate by making Federal Reserve balances available to depository institutions when the supply of balances falls short of demand. It also serves as a backup source of liquidity for individual depository institutions.

At times when the normal functioning of financial markets is disrupted, the discount window can become the principal channel for supplying balances to depository institutions.



FEDERAL RESERVE press release

For immediate release September 11, 2001

The Federal Reserve System is open and operating. The discount window is available to meet liquidity needs.

-0-

Although the volume of discount window borrowing is relatively small, it plays an important role in containing upward pressures on the federal funds rate. If a depository institution faces an unexpectedly low balance in its account at the Federal Reserve, either because the total supply of balances has fallen short of demand or because it failed to receive an expected transfer of funds from a counterparty, it can borrow at the discount window. This extension of credit increases the supply of Federal

Reserve balances and helps to limit any upward pressure on the federal funds rate. At times when the normal functioning of financial markets is disrupted—for example after operational problems, a natural disaster, or a terrorist attack—the discount window can become the principal channel for supplying balances to depository institutions.

The discount window can also, at times, serve as a useful tool for promoting financial stability by providing temporary funding to depository institutions that are having significant financial difficulties. If the institution's sudden collapse were likely to have severe adverse effects on the financial system, an extension of central bank credit could be desirable because it would address the liquidity strains and permit the institution to make a transition to sounder footing. Discount window credit can also be used to facilitate an orderly resolution of a failing institution. An institution obtaining credit in either situation must be monitored appropriately to ensure that it does not take excessive risks in an attempt to return to profitability and that the use of central bank credit would not increase costs to the deposit insurance fund and ultimately the taxpayer.

Types of Credit

In ordinary circumstances, the Federal Reserve extends discount window credit to depository institutions under the primary, secondary, and seasonal credit programs. The rates charged on loans under each of these programs are established by each Reserve Bank's board of directors every two weeks, subject to review and determination by the Board of Governors. The rates for each of the three lending programs are the same at all Reserve Banks, except occasionally for very brief periods following the Board's action to adopt a requested rate change. The Federal Reserve also has the authority under the Federal Reserve Act to extend credit to entities that are not depository institutions in "unusual and exigent circumstances"; however, such lending has not occurred since the 1930s.

Primary Credit

Primary credit is available to generally sound depository institutions on a very short-term basis, typically overnight. To assess whether a depository institution is in sound financial condition, its Reserve Bank regularly reviews the institution's condition, using supervisory ratings and data on adequacy of the institution's capital. Depository institutions are not required to seek alternative sources of funds before requesting occasional advances of primary credit, but primary credit is expected to be used as a backup, rather than a regular, source of funding.

The rate on primary credit has typically been set 1 percentage point above the FOMC's target federal funds rate, but the spread can vary depending on circumstances. Because primary credit is the Federal Reserve's main dis-

Major Revision to Discount Window Programs

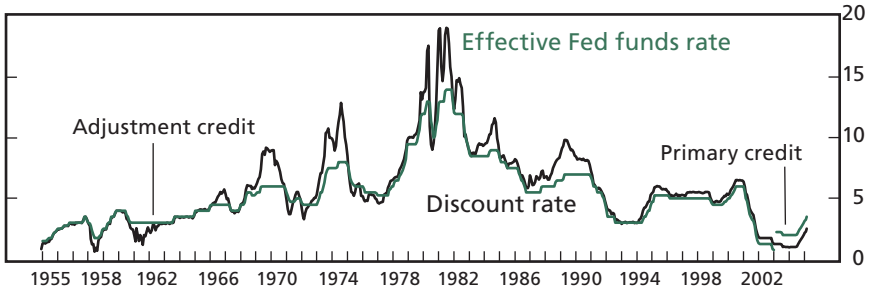
On January 9, 2003, the Federal Reserve significantly revised its discount window lending programs, replacing the previous adjustment and extended credit programs with primary and secondary credit facilities. Adjustment credit had been made available to help depository institutions make short-term balance-sheet adjustments and to provide an alternate source of funds in the event of a shortfall in the supply of Federal Reserve balances. Extended credit, which was intended to accommodate depository institutions' somewhat longer-term liquidity needs resulting from exceptional circumstances, had not been used since 1995.

Adjustment credit was extended at the basic discount rate, which over the previous decade had been 25 to 50 basis points below the usual level of overnight market interest rates. The below-market interest rate on adjustment credit had caused several significant problems. The incentive for depository institutions to exploit the below-market rate meant that borrowing requests necessarily were subject to considerable administration by Reserve Banks. In particular, borrowers were required to seek funds elsewhere before coming to the window. Partly as a result of those requirements, many depository institutions were reluctant to borrow from the discount window, reducing the effectiveness of the discount window in buffering shocks to the money market.

Under the revised lending programs, the above-market rate and the fact that primary credit is restricted to financially sound institutions mean that primary credit can be extended largely without administration, making depository institutions more willing to borrow and so making the discount window a more effective monetary policy tool. The central banks of nearly all industrialized countries have similar lending facilities that extend collateralized credit at an above-market rate with little or no administration.

Chart 3.3

Effective federal funds rate and discount rate, 1955–2004*



* On January 9, 2003, the main discount rate switched from being the rate on adjustment credit to the rate on primary credit.

count window program, the Federal Reserve at times uses the term *discount rate* specifically to mean the primary credit rate.

Reserve Banks ordinarily do not require depository institutions to provide reasons for requesting very short-term primary credit. Borrowers are asked to provide only the minimum information necessary to process a loan, usually the requested amount and term of the loan. If a pattern of borrowing or the nature of a particular borrowing request strongly indicates that a depository institution is not generally sound or is using primary credit as a regular rather than a backup source of funding, a Reserve Bank may seek additional information before deciding whether to extend the loan.

Primary credit may be extended for longer periods of up to a few weeks if a depository institution is in generally sound financial condition and cannot obtain temporary funds in the market at reasonable terms. Large and medium-sized institutions are unlikely to meet this test.

Depository institutions that have reservable transaction accounts or nonpersonal time deposits may borrow from the discount window.

Secondary Credit

Secondary credit is available to depository institutions that are not eligible for primary credit. It is extended on a very short-term basis, typically overnight. Reflecting the less-sound financial condition of borrowers of secondary credit, the rate on secondary credit has typically been 50 basis points above the primary credit rate, although the spread can vary as circumstances warrant. Secondary credit is available to help a depository institution meet backup liquidity needs when its use is consistent with the borrowing institution's timely return to a reliance on market sources of funding or with the orderly resolution of a troubled institution's difficulties. Secondary credit may not be used to fund an expansion of the borrower's assets.

Loans extended under the secondary credit program entail a higher level of Reserve Bank administration and oversight than loans under the primary credit program. A Reserve Bank must have sufficient information about a borrower's financial condition and reasons for borrowing to ensure that an extension of secondary credit would be consistent with the purpose of the facility. Moreover, under the Federal Deposit Insurance Corporation Improvement Act of 1991, extensions of Federal Reserve credit to an FDIC-insured depository institution that has fallen below minimum capital standards are generally limited to 60 days in any 120-day period or, for the most severely undercapitalized, to only five days.

Seasonal Credit

The Federal Reserve's seasonal credit program is designed to help small depository institutions manage significant seasonal swings in their loans and deposits. Seasonal credit is available to depository institutions that can

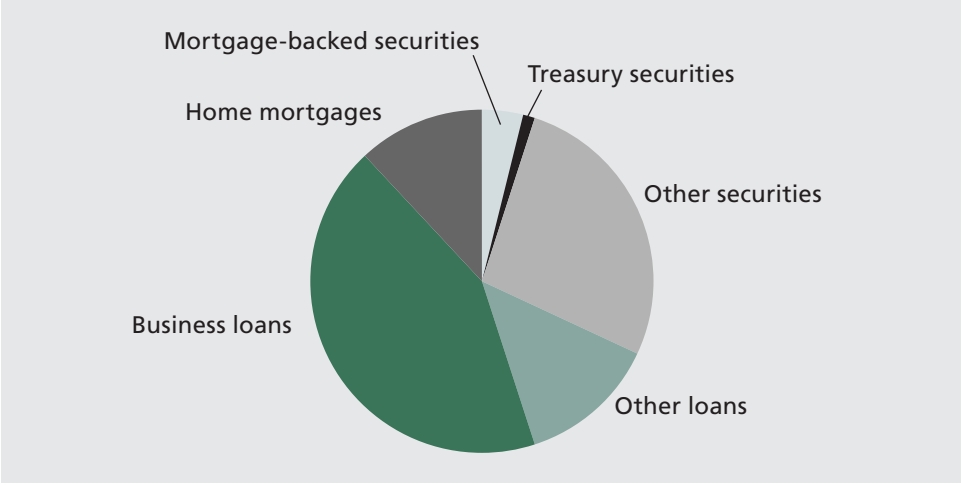
demonstrate a clear pattern of recurring swings in funding needs throughout the year—usually institutions in agricultural or tourist areas. Borrowing longer-term funds from the discount window during periods of seasonal need allows institutions to carry fewer liquid assets during the rest of the year and make more funds available for local lending.

The seasonal credit rate is based on market interest rates. It is set on the first business day of each two-week reserve maintenance period as the average of the effective federal funds rate and the interest rate on three-month certificates of deposit over the previous reserve maintenance period.

Eligibility to Borrow

By law, depository institutions that have reservable transaction accounts or nonpersonal time deposits may borrow from the discount window. U.S. branches and agencies of foreign banks that are subject to reserve requirements are eligible to borrow under the same general terms and conditions that apply to domestic depository institutions. Banker's banks, corporate credit unions, and certain other banking institutions that are not subject to reserve requirements generally do not have access to the discount window. However, the Board of Governors has determined that those institutions may obtain access to the discount window if they voluntarily maintain required reserve balances.

Chart 3.2
Collateral value by asset type, December 31, 2004



Discount Window Collateral

By law, all discount window loans must be secured by collateral to the satisfaction of the lending Reserve Bank. Most loans that are not past due and most investment-grade securities held by depository institutions are acceptable as collateral. Reserve Banks must be able to establish a legal right in the event of default to be first in line to take possession of and, if necessary, sell all collateral that secures discount window loans.

Reserve Banks assign a lendable value to assets accepted as collateral. The lendable value is the maximum loan amount that can be backed by that asset. It is based on market values, if available, or par values—in both cases reduced by a margin. The margin depends on how accurately the asset can be valued, how much its value tends to vary over time, the liquidity of the asset, and the financial condition of the pledging institution.

4 The Federal Reserve in the International Sphere

The U.S. economy and the world economy are linked in many ways. Economic developments in this country have a major influence on production, employment, and prices beyond our borders; at the same time, developments abroad significantly affect our economy. The U.S. dollar, which is the currency most used in international transactions, constitutes more than half of other countries' official foreign exchange reserves. U.S. banks abroad and foreign banks in the United States are important actors in international financial markets.

The activities of the Federal Reserve and the international economy influence each other. Therefore, when deciding on the appropriate monetary policy for achieving basic economic goals, the Board of Governors and the FOMC consider the record of U.S. international transactions, movements in foreign exchange rates, and other international economic developments. And in the area of bank supervision and regulation, innovations in international banking require continual assessments of, and occasional modifications in, the Federal Reserve's procedures and regulations.

The Federal Reserve formulates policies that shape, and are shaped by, international developments. It also participates directly in international affairs. For example, the Federal Reserve occasionally undertakes foreign exchange transactions aimed at influencing the value of the dollar in relation to foreign currencies, primarily with the goal of stabilizing disorderly market conditions. These transactions are undertaken in close and continuous consultation and cooperation with the U.S. Treasury. The Federal Reserve also works with the Treasury and other government agencies on various aspects of international financial policy. It participates in a number of international organizations and forums and is in almost continuous contact with other central banks on subjects of mutual concern.

International Linkages

The Federal Reserve's actions to adjust U.S. monetary policy are designed to attain basic objectives for the U.S. economy. But any policy move also influences, and is influenced by, international developments. For example,

U.S. monetary policy actions influence exchange rates. The dollar's exchange value in terms of other currencies is therefore one of the channels through which U.S. monetary policy affects the U.S. economy. If Federal Reserve actions raised U.S. interest rates, for instance, the foreign exchange value of the dollar generally would rise. An increase in the foreign exchange value of the dollar, in turn, would raise the price in foreign currency of U.S. goods traded on world markets and lower the dollar price of goods imported into the United States. By restraining exports and boosting imports, these developments could lower output and price levels in the U.S. economy. In contrast, an increase in interest rates in a foreign country could raise worldwide demand for assets denominated in that country's currency and thereby reduce the dollar's value in terms of that currency. Other things being equal, U.S. output and price levels would tend to increase—just the opposite of what happens when U.S. interest rates rise.

Economic developments in the United States, including U.S. monetary policy actions, have significant effects on growth and inflation in foreign economies.

Therefore, when formulating monetary policy, the Board of Governors and the FOMC draw upon information about and analysis of international as well as U.S. domestic influences. Changes in public policies or in economic conditions abroad and movements in international variables that affect the U.S. economy, such as exchange rates, must be factored into the determination of U.S. monetary policy.

Conversely, economic developments in the United States, including U.S. monetary policy actions, have significant effects on growth and inflation in foreign economies. Although the Federal Reserve's policy objectives are limited to economic outcomes in the United States, it is mutually beneficial for macroeconomic and financial policy makers in the United States and other countries to maintain a continuous dialogue. This dialogue enables the Federal Reserve to better understand and anticipate influences on the U.S. economy that emanate from abroad.

The increasing complexity of global financial markets—combined with ever-increasing linkages between national markets through trade, finance, and direct investment—have led to a proliferation of forums in which policy makers from different countries can meet and discuss topics of mutual interest. One important forum is provided by the Bank for International Settlements (BIS) in Basel, Switzerland. Through the BIS, the Federal Reserve works with representatives of the central banks of other countries on mutual concerns regarding monetary policy, international financial markets, banking supervision and regulation, and payments systems. (The Chairman of the Board of Governors and the president of the Federal Reserve Board of New York represent the U.S. central bank on the board of directors of the BIS.) Representatives of the Federal Reserve also participate in the activities of the International Monetary Fund (IMF) and discuss macroeconomic, financial market, and structural issues with representatives of other industrial countries at the Organisation for Economic

Co-operation and Development (OECD). Following the Asian Financial Crises of 1997 and 1998, the Financial Stability Forum (FSF) was established to enable central banks, finance ministries, and financial regulatory authorities in systemically important economies to work together to address issues related to financial stability. The Federal Reserve also sends delegates to international meetings such as those of the Asia Pacific Economic Cooperation (APEC) Finance Ministers' Process, the G-7 Finance Ministers and Central Bank Governors, the G-20, and the Governors of Central Banks of the American Continent.

Foreign Currency Operations

The Federal Reserve conducts foreign currency operations—the buying and selling of dollars in exchange for foreign currency—under the direction of the FOMC, acting in close and continuous consultation and cooperation with the U.S. Treasury, which has overall responsibility for U.S. international financial policy. The manager of the System Open Market Account at the Federal Reserve Bank of New York acts as the agent for both the FOMC and the Treasury in carrying out foreign currency operations. Since the late 1970s, the U.S. Treasury and the Federal Reserve have conducted almost all foreign currency operations jointly and equally.

The purpose of Federal Reserve foreign currency operations has evolved in response to changes in the international monetary system. The most important of these changes was the transition in the 1970s from a system of fixed exchange rates—established in 1944 at an international monetary conference held in Bretton Woods, New Hampshire—to a system of flexible (or floating) exchange rates for the dollar in terms of other countries' currencies. Under the Bretton Woods Agreements, which created the IMF and the International Bank for Reconstruction and Development (known informally as the World Bank), foreign authorities were responsible for intervening in exchange markets to maintain their countries' exchange rates within 1 percent of their currencies' parities with the U.S. dollar; direct exchange market intervention by U.S. authorities was extremely limited. Instead, U.S. authorities were obliged to buy and sell dollars against gold to maintain the dollar price of gold near $35 per ounce. After the United States suspended the gold convertibility of the dollar in 1971, a regime of flexible exchange rates emerged; in 1973, under that regime, the United States began to intervene in exchange markets on a more significant scale. In 1978, the regime of flexible exchange rates was codified in an amendment to the IMF's Articles of Agreement.

Under flexible exchange rates, the main aim of Federal Reserve foreign currency operations has been to counter disorderly conditions in exchange markets through the purchase or sale of foreign currencies (called foreign

exchange intervention operations), primarily in the New York market. During some episodes of downward pressure on the foreign exchange value of the dollar, the Federal Reserve has purchased dollars (sold foreign currency) and has thereby absorbed some of the selling pressure on the dollar. Similarly, the Federal Reserve may sell dollars (purchase foreign currency) to counter upward pressure on the dollar's foreign exchange value. The Federal Reserve Bank of New York also executes transactions in the U.S. foreign exchange market for foreign monetary authorities, using their funds.

Under flexible exchange rates, the main aim of Federal Reserve foreign currency operations has been to counter disorderly conditions in exchange markets.

In the early 1980s, the United States curtailed its official exchange market operations, although it remained ready to enter the market when necessary to counter disorderly conditions. In 1985, particularly after September, when representatives of the five major industrial countries reached the so-called Plaza Agreement on exchange rates, the United States began to use exchange market intervention as a policy instrument more frequently. Between 1985 and 1995, the Federal Reserve—sometimes in coordination with other central banks—intervened to counter dollar movements that were perceived as excessive. Based on an assessment of past experience with official intervention and a reluctance to let exchange rate issues be seen as a major focus of monetary policy, U.S. authorities have intervened only rarely since 1995.

Sterilization

Intervention operations involving dollars affect the supply of Federal Reserve balances to U.S. depository institutions, unless the Federal Reserve offsets the effect. A purchase of foreign currency by the Federal Reserve increases the supply of balances when the Federal Reserve credits the account of the seller's depository institution at the Federal Reserve. Conversely, a sale of foreign currency by the Federal Reserve decreases the supply of balances. The Federal Reserve offsets, or "sterilizes," the effects of intervention on Federal Reserve balances through open market operations; otherwise, the intervention could cause the federal funds rate to move away from the target set by the FOMC.

For example, assume that the Federal Reserve, perhaps in conjunction with Japanese authorities, wants to counter downward pressure on the dollar's foreign exchange value in relation to the Japanese yen. The Federal Reserve would sell some of its yen-denominated securities for yen on the open market and then trade the yen for dollars in the foreign exchange market, thus reducing the supply of dollar balances at the Federal Reserve. In order to sterilize the effect of intervention on the supply of Federal Reserve balances, the Open Market Desk would then purchase an equal amount of U.S. Treasury securities in the open market (or arrange a repurchase agreement), thereby raising the supply of balances back to

its former level. The net effect of such an intervention is a reduction in dollar-denominated securities in the hands of the public and an increase in yen-denominated securities. The operations have no net effect on the level of yen balances at the Bank of Japan or on the level of dollar balances at the Federal Reserve.

A dollar intervention initiated by a foreign central bank also leaves the supply of balances at the Federal Reserve unaffected, unless the central bank changes the amount it has on deposit at the Federal Reserve. If, for example, the foreign central bank purchases dollars in the foreign exchange market and places them in its account at the Federal Reserve Bank of New York, then the supply of Federal Reserve balances available to U.S. depository institutions decreases because the dollars are transferred from the bank of the seller of dollars to the foreign central bank's account with the Federal Reserve. However, the Open Market Desk would offset this drain by buying a Treasury security or arranging a repurchase agreement to increase the supply of Federal Reserve balances to U.S. depository institutions. Most dollar purchases by foreign central banks are used to purchase dollar securities directly, and thus they do not need to be countered by U.S. open market operations to leave the supply of dollar balances at the Federal Reserve unchanged.

U.S. Foreign Currency Resources

The main source of foreign currencies used in U.S. intervention operations currently is U.S. holdings of foreign exchange reserves. At the end of June 2004, the United States held foreign currency reserves valued at $40 billion. Of this amount, the Federal Reserve held foreign currency assets of $20 billion, and the Exchange Stabilization Fund of the Treasury held the rest.

The U.S. monetary authorities have also arranged swap facilities with foreign monetary authorities to support foreign currency operations. These facilities, which are also known as reciprocal currency arrangements, provide short-term access to foreign currencies. A swap transaction involves both a spot (immediate delivery) transaction, in which the Federal Reserve transfers dollars to another central bank in exchange for foreign currency, and a simultaneous forward (future delivery) transaction, in which the two central banks agree to reverse the spot transaction, typically no later than three months in the future. The repurchase price incorporates a market rate of return in each currency of the transaction. The original purpose of swap arrangements was to facilitate a central bank's support of its own currency in case of undesired downward pressure in foreign exchange markets. Drawings on swap arrangements were common in the 1960s but over time declined in frequency as policy authorities came to rely more on foreign exchange reserve balances to finance currency operations.

In years past, the Federal Reserve had standing commitments to swap currencies with the central banks of more than a dozen countries. In the middle of the 1990s, these arrangements totaled more than $30 billion, but they were almost never drawn upon. At the end of 1998, these facilities were allowed to lapse by mutual agreement among the central banks involved, with the exception of arrangements with the central banks of Canada and Mexico (see table 4.1).

Reciprocal currency arrangements can be an important policy tool in times of unusual market disruptions. For example, immediately after the terrorist attacks of September 11, 2001, the Federal Reserve established temporary swap arrangements with the European Central Bank and the Bank of England, as well as a temporary augmentation of the existing arrangement with the Bank of Canada (see table 4.1). The purpose of these arrangements was to enable the foreign central banks to lend dollars to local financial institutions to facilitate the settlement of their dollar obligations and to guard against possible disruptions to the global payments system. The European Central Bank drew $23.5 billion of its swap line; the balance was repaid after three days. The other central banks did not draw on their lines. The temporary arrangements lapsed after thirty days.

Table 4.1

Federal Reserve standing reciprocal currency arrangements, June 30, 2004

Millions of U.S. dollars

Institution	Amount of facility	Amount drawn
Bank of Canada	2,000	0
Bank of Mexico	3,000	0
Temporary reciprocal currency arrangements of September 2001		
European Central Bank	50,000	23,500*
Bank of England	30,000	0
Bank of Canada	10,000†	0

* Total drawings on September 12, 13, and 14, 2001. Balance repaid as of September 15, 2001.

† Includes 2,000 from existing arrangement (see upper panel).

International Banking

The Federal Reserve is interested in the international activities of banks, not only because it functions as a bank supervisor but also because such activities are often close substitutes for domestic banking activities and need to be monitored carefully to help interpret U.S. monetary and credit conditions. Moreover, international banking institutions are important vehicles for capital flows into and out of the United States.

Where international banking activities are conducted depends on such factors as the business needs of customers, the scope of operations permitted by a country's legal and regulatory framework, and tax considerations. The international activities of U.S.-chartered banks include lending to and accepting deposits from foreign customers at the banks' U.S. offices and engaging in other financial transactions with foreign counterparts. However, the bulk of the international business of U.S.-chartered banks takes place at their branch offices located abroad and at their foreign-incorporated subsidiaries, usually wholly owned. Much of the activity of foreign branches and subsidiaries of U.S. banks has been Eurocurrency[1] business—that is, taking deposits and lending in currencies other than that of the country in which the banking office is located. Increasingly, U.S. banks are also offering a range of sophisticated financial products to residents of other countries and to U.S. firms abroad.

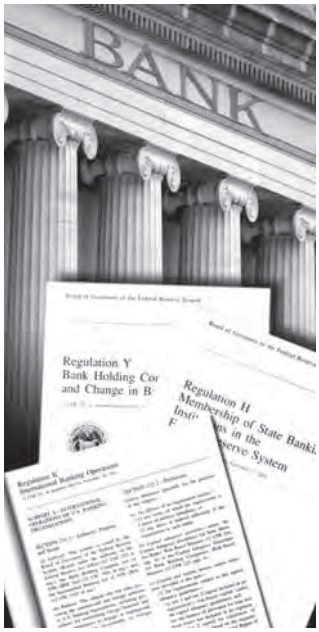
The international role of U.S. banks has a counterpart in foreign bank operations in the United States. U.S. offices of foreign banks actively participate as both borrowers and investors in U.S. domestic money markets and are active in the market for loans to U.S. businesses. (See chapter 5 for a discussion of the Federal Reserve's supervision and regulation of the international activities of U.S. banks and the U.S. activities of foreign banks.)

International banking by both U.S.-based and foreign banks facilitates the holding of Eurodollar deposits—dollar deposits in banking offices outside the United States—by nonbank U.S. entities. Similarly, Eurodollar loans—dollar loans from banking offices outside the United States—can be an important source of credit for U.S. companies (banks and nonbanks). Because they are close substitutes for deposits at domestic banks, Eurodollar deposits of nonbank U.S. entities at foreign branches of U.S. banks are included in the U.S. monetary aggregate M3; Eurodollar deposits of nonbank U.S. entities at all other banking offices in the United Kingdom and Canada are also included in M3. (See page 21 for a discussion of U.S. monetary aggregates.)

1. The term *Eurocurrency* should not be confused with *euro,* the common currency of several European Union countries.

5 Supervision and Regulation

The Federal Reserve has supervisory and regulatory authority over a wide range of financial institutions and activities. It works with other federal and state supervisory authorities to ensure the safety and soundness of financial institutions, stability in the financial markets, and fair and equitable treatment of consumers in their financial transactions. As the U.S. central bank, the Federal Reserve also has extensive and well-established relationships with the central banks and financial supervisors of other countries, which enables it to coordinate its actions with those of other countries when managing international financial crises and supervising institutions with a substantial international presence.



The Federal Reserve has responsibility for supervising and regulating the following segments of the banking industry to ensure safe and sound banking practices and compliance with banking laws:

- bank holding companies, including diversified financial holding companies formed under the Gramm-Leach-Bliley Act of 1999 and foreign banks with U.S. operations
- state-chartered banks that are members of the Federal Reserve System (state member banks)
- foreign branches of member banks
- Edge and agreement corporations, through which U.S. banking organizations may conduct international banking activities
- U.S. state-licensed branches, agencies, and representative offices of foreign banks
- nonbanking activities of foreign banks

Although the terms *bank supervision* and *bank regulation* are often used interchangeably, they actually refer to distinct, but complementary, activities. Bank supervision involves the monitoring, inspecting, and examining of banking organizations to assess their condition and their compliance with relevant laws and regulations. When a banking organization within the Federal Reserve's supervisory jurisdiction is found to be noncompliant or to have other problems, the Federal Reserve may use its supervisory authority to take formal or informal action to have the organization correct the problems.

Bank regulation entails issuing specific regulations and guidelines governing the operations, activities, and acquisitions of banking organizations.

Responsibilities of the Federal Banking Agencies

The primary supervisor of a domestic banking institution is generally determined by the type of institution that it is and the governmental authority that granted it permission to commence business.

The Federal Reserve shares supervisory and regulatory responsibilities for domestic banking institutions with the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), and the Office of Thrift Supervision (OTS) at the federal level, and with the banking departments of the various states. The primary supervisor of a domestic banking institution is generally determined by the type of institution that it is and the governmental authority that granted it permission to commence business (commonly referred to as a charter). Banks that are chartered by a state government are referred to as state banks; banks that are chartered by the OCC, which is a bureau of the Department of the Treasury, are referred to as national banks.

The Federal Reserve has primary supervisory authority for state banks that elect to become members of the Federal Reserve System (state member banks). State banks that are not members of the Federal Reserve System (state nonmember banks) are supervised by the FDIC. In addition to being supervised by the Federal Reserve or FDIC, all state banks are supervised by their chartering state. The OCC supervises national banks. All national banks must become members of the Federal Reserve System. This dual federal–state banking system has evolved partly out of the complexity of the U.S. financial system, with its many kinds of depository institutions and numerous chartering authorities. It has also resulted from a wide variety of federal and state laws and regulations designed to remedy problems that the U.S. commercial banking system has faced over its history.

Banks are often owned or controlled by another company. These companies are referred to as bank holding companies. The Federal Reserve has supervisory authority for all bank holding companies, regardless of whether the subsidiary bank of the holding company is a national bank, state member bank, or state nonmember bank.

Savings associations, another type of depository institution, have historically focused on residential mortgage lending. The OTS, which is a bureau of the Department of the Treasury, charters and supervises federal savings associations and also supervises companies that own or control a savings association. These companies are referred to as thrift holding companies.

The FDIC insures the deposits of banks and savings associations up to certain limits established by law. As the insurer, the FDIC has special exami-

nation authority to determine the condition of an insured bank or savings association for insurance purposes.

Table 5.1 summarizes the supervisory responsibilities of the Federal Reserve and other federal banking agencies.

Table 5.1
Federal supervisor and regulator of corporate components of banking organizations in the United States

Component	Supervisor and regulator
Bank holding companies (including financial holding companies)	FR
Nonbank subsidiaries of bank holding companies	FR/Functional regulator[1]
National banks	OCC
State banks	
Members	FR
Nonmembers	FDIC
Thrift holding companies	OTS
Savings banks	OTS/FDIC/FR
Savings and loan associations	OTS
Edge and agreement corporations	FR
Foreign banks[2]	
Branches and agencies[3]	
State-licensed	FR/FDIC
Federally licensed	OCC/FR/FDIC
Representative offices	FR

NOTE: FR = Federal Reserve; OCC = Office of the Comptroller of the Currency; FDIC = Federal Deposit Insurance Corporation; OTS = Office of Thrift Supervision

1. Nonbank subsidiaries engaged in securities, commodities, or insurance activities are supervised and regulated by their appropriate functional regulators. Such functionally regulated subsidiaries include a broker, dealer, investment adviser, and investment company registered with and regulated by the Securities and Exchange Commission (or, in the case of an investment adviser, registered with any state); an insurance company or insurance agent subject to supervision by a state insurance regulator; and a subsidiary engaged in commodity activities regulated by the Commodity Futures Trading Commission.

2. Applies to direct operations in the United States. Foreign banks may also have indirect operations in the United States through their ownership of U.S. banking organizations.

3. The FDIC has responsibility for branches that are insured.

Federal Financial Institutions Examination Council

To promote consistency in the examination and supervision of banking organizations, in 1978 Congress created the Federal Financial Institutions Examination Council (FFIEC). The FFIEC is composed of the chairpersons of the FDIC and the National Credit Union Administration, the comptroller of the currency, the director of the OTS, and a governor of the Federal Reserve Board appointed by the Board Chairman. The FFIEC's purposes are to prescribe uniform federal principles and standards for the examination of depository institutions, to promote coordination of bank supervision among the federal agencies that regulate financial institutions, and to encourage better coordination of federal and state regulatory activities. Through the FFIEC, state and federal regulatory agencies may exchange views on important regulatory issues. Among other things, the FFIEC has developed uniform financial reports for federally supervised banks to file with their federal regulator.

The main objective of the supervisory process is to evaluate the overall safety and soundness of the banking organization.

Supervisory Process

The main objective of the supervisory process is to evaluate the overall safety and soundness of the banking organization. This evaluation includes an assessment of the organization's risk-management systems, financial condition, and compliance with applicable banking laws and regulations.

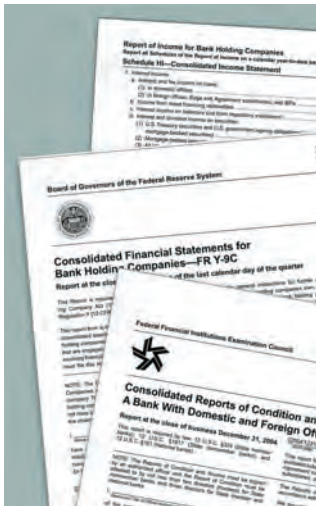
The supervisory process entails both on-site examinations and inspections and off-site surveillance and monitoring. Typically, state member banks must have an on-site examination at least once every twelve months. Banks that have assets of less than $250 million and that meet certain management, capital, and other criteria may be examined once every eighteen months. The Federal Reserve coordinates its examinations with those of the bank's chartering state and may alternate exam cycles with the bank's state supervisor.

The Federal Reserve generally conducts an annual inspection of large bank holding companies (companies with consolidated assets of $1 billion or greater) and smaller bank holding companies that have significant nonbank assets. Small, noncomplex bank holding companies are subject to a special supervisory program that permits a more flexible approach that relies on off-site monitoring and the supervisory ratings of the lead subsidiary depository institution. When evaluating the consolidated condition of the holding company, Federal Reserve examiners rely heavily on the results of the examination of the company's subsidiary banks by the primary federal or state banking authority, to minimize duplication of efforts and reduce burden on the banking organization.

Risk-Focused Supervision

With the largest banking organizations growing in both size and complexity, the Federal Reserve has moved towards a risk-focused approach to supervision that is more a continuous process than a point-in-time examination. The goal of the risk-focused supervision process is to identify the greatest risks to a banking organization and assess the ability of the organization's management to identify, measure, monitor, and control these risks. Under the risk-focused approach, Federal Reserve examiners focus on those business activities that may pose the greatest risk to the organization.

Supervisory Rating System



The results of an on-site examination or inspection are reported to the board of directors and management of the bank or holding company in a report of examination or inspection, which includes a confidential supervisory rating of the financial condition of the bank or holding company. The supervisory rating system is a supervisory tool that all of the federal and state banking agencies use to communicate to banking organizations the agency's assessment of the organization and to identify institutions that raise concern or require special attention. This rating system for banks is commonly referred to as CAMELS, which is an acronym for the six components of the rating system: capital adequacy, asset quality, management and administration, earnings, liquidity, and sensitivity to market risk. The Federal Reserve also uses a supervisory rating system for bank holding companies, referred to as RFI/C(D), that takes into account risk management, financial condition, potential impact of the parent company and nondepository subsidiaries on the affiliated depository institutions, and the CAMELS rating of the affiliated depository institutions.[1]

Financial Regulatory Reports

In carrying out their supervisory activities, Federal Reserve examiners and supervisory staff rely on many sources of financial and other information about banking organizations, including reports of recent examinations and inspections, information published in the financial press and elsewhere, and the standard financial regulatory reports filed by institutions.

1. The risk-management component has four subcomponents that reflect the effectiveness of the banking organization's risk management and controls: board and senior management oversight; policies, procedures, and limits; risk monitoring and management information systems; and internal controls. The financial-condition component has four subcomponents reflecting an assessment of the quality of the banking organization's capital, assets, earnings, and liquidity.

The financial report for banks is the Consolidated Reports of Condition and Income, often referred to as the Call Report. It is used to prepare the Uniform Bank Performance Report, which employs ratio analysis to detect unusual or significant changes in a bank's financial condition that may warrant supervisory attention. The financial report for bank holding companies is the Consolidated Financial Statements for Bank Holding Companies (the FR Y-9 series).

The number and type of report forms that must be filed by a banking organization depend on the size of the organization, the scope of its operations, and the types of activities that it conducts either directly or through a subsidiary. The report forms filed by larger institutions that engage in a wider range of activities are generally more numerous and more detailed than those filed by smaller organizations.

The Federal Reserve plays a significant role in promoting sound accounting policies and meaningful public disclosure by financial institutions.

Off-Site Monitoring

In its ongoing off-site supervision of banks and bank holding companies, the Federal Reserve uses automated screening systems to identify organizations with poor or deteriorating financial profiles and to help detect adverse trends developing in the banking industry. The System to Estimate Examinations Ratings (SEER) statistically estimates an institution's supervisory rating based on prior examination data and information that banks provide in their quarterly Call Report filings. This information enables the Federal Reserve to better direct examiner resources to those institutions needing supervisory attention.

Accounting Policy and Disclosure

Enhanced market discipline is an important component of bank supervision. Accordingly, the Federal Reserve plays a significant role in promoting sound accounting policies and meaningful public disclosure by financial institutions. In 1991, Congress passed the Federal Deposit Insurance Corporation Improvement Act, emphasizing the importance of financial institution accounting, auditing, and control standards. In addition, the Sarbanes-Oxley Act of 2002 seeks to improve the accuracy and reliability of corporate disclosures and to detect and address corporate and accounting fraud. Through its supervision and regulation function, the Federal Reserve seeks to strengthen the accounting, audit, and control standards related to financial institutions. The Federal Reserve is involved in the development of international and domestic capital, accounting, financial disclosure, and other supervisory standards. Federal Reserve examiners also review the quality of financial institutions' disclosure practices. Public disclosure allows market participants to assess the strength of individual institutions and is a critical element in market discipline.

Umbrella Supervision and Coordination with Other Functional Regulators

In addition to owning banks, bank holding companies also may own broker-dealers engaged in securities activities or insurance companies. Indeed, one of the primary purposes of the Gramm-Leach-Bliley Act (GLB Act), enacted in 1999, was to allow banks, securities broker-dealers, and insurance companies to affiliate with each other through the bank holding company structure. To take advantage of the expanded affiliations permitted by the GLB Act, a bank holding company must meet certain capital, managerial, and other requirements and must elect to become a "financial holding company." When a bank holding company or financial holding company owns a subsidiary broker-dealer or insurance company, the Federal Reserve seeks to coordinate its supervisory responsibilities with those of the subsidiary's functional regulator—the Securities and Exchange Commission (SEC) in the case of a broker-dealer and the state insurance authorities in the case of an insurance company.

The Federal Reserve's role as the supervisor of a bank holding company or financial holding company is to review and assess the consolidated organization's operations, risk-management systems, and capital adequacy to ensure that the holding company and its nonbank subsidiaries do not threaten the viability of the company's depository institutions. In this role, the Federal Reserve serves as the "umbrella supervisor" of the consolidated organization. In fulfilling this role, the Federal Reserve relies to the fullest extent possible on information and analysis provided by the appropriate supervisory authority of the company's bank, securities, or insurance subsidiaries.

Anti-Money-Laundering Program

To enhance domestic security following the terrorist attacks of September 11, 2001, Congress passed the USA Patriot Act, which contained provisions for fighting international money laundering and for blocking terrorists' access to the U.S. financial system. The provisions of the act that affect banking organizations were generally set forth as amendments to the Bank Secrecy Act (BSA), which was enacted in 1970.

The BSA requires financial institutions doing business in the United States to report large currency transactions and to retain certain records, including information about persons involved in large currency transactions and about suspicious activity related to possible violations of federal law, such as money laundering, terrorist financing, and other financial crimes. The BSA also prohibits the use of foreign bank accounts to launder illicit funds or to avoid U.S. taxes and statutory restrictions.

The Department of the Treasury maintains primary responsibility for issuing and enforcing regulations to implement this statute. However, Treasury has delegated to the federal financial regulatory agencies responsibility for monitoring banks' compliance with the BSA. The Federal Reserve Board's Regulation H requires banking organizations to develop a written program for BSA compliance. During examinations of state member banks and U.S. branches and agencies of foreign banks, Federal Reserve examiners verify an institution's compliance with the recordkeeping and reporting requirements of the BSA and with related regulations, including those related to economic sanctions imposed by Congress against certain countries, as implemented by the Office of Foreign Assets Control.

Business Continuity

After September 11, 2001, the Federal Reserve implemented a number of measures to promote the continuous operation of financial markets and to ensure the continuity of Federal Reserve operations in the event of a future crisis. The process of strengthening the resilience of the private-sector financial system—focusing on organizations with systemic elements—is largely accomplished through the existing regulatory framework. In 2003, responding to the need for further guidance for financial institutions in this area, the Federal Reserve Board, the OCC, and the SEC issued the "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System." The paper sets forth sound practices for the financial industry to ensure a rapid recovery of the U.S. financial system in the event of a wide-scale disruption that may include loss or inaccessibility of staff. Many of the concepts in the paper amplify long-standing and well-recognized principles relating to safeguarding information and the ability to recover and resume essential financial services.

Other Supervisory Activities

The Federal Reserve conducts on-site examinations of banks to ensure compliance with consumer protection laws (discussed in chapter 6) as well as compliance in other areas, such as fiduciary activities, transfer agency, securities clearing agency, government and municipal securities dealing, securities credit lending, and information technology. Further, in light of the importance of information technology to the safety and soundness of banking organizations, the Federal Reserve has the authority to examine the operations of certain independent organizations that provide information technology services to supervised banking organizations.

Enforcement

If the Federal Reserve determines that a state member bank or bank holding company has problems that affect the institution's safety and soundness

or is not in compliance with laws and regulations, it may take a supervisory action to ensure that the institution undertakes corrective measures. Typically, such findings are communicated to the management and directors of a banking organization in a written report. The management and directors are then asked to address all identified problems voluntarily and to take measures to ensure that the problems are corrected and will not recur. Most problems are resolved promptly after they are brought to the attention of an institution's management and directors. In some situations, however, the Federal Reserve may need to take an informal supervisory action, requesting that an institution adopt a board resolution or agree to the provisions of a memorandum of understanding to address the problem.

If necessary, the Federal Reserve may take formal enforcement actions to compel the management and directors of a troubled banking organization, or persons associated with it, to address the organization's problems. For example, if an institution has significant deficiencies or fails to comply with an informal action, the Federal Reserve may enter into a written agreement with the troubled institution or may issue a cease-and-desist order against the institution or against an individual associated with the institution, such as an officer or director. The Federal Reserve may also assess a fine, remove an officer or director from office and permanently bar him or her from the banking industry, or both. All final enforcement orders issued by the Board and all written agreements executed by Reserve Banks are available to the public on the Board's web site.

Under federal law, U.S. banking organizations generally may conduct a wider range of activities abroad than they may conduct in this country.

Supervision of International Operations of U.S. Banking Organizations

The Federal Reserve also has supervisory and regulatory responsibility for the international operations of member banks (that is, national and state member banks) and bank holding companies. These responsibilities include

- authorizing the establishment of foreign branches of national banks and state member banks and regulating the scope of their activities;
- chartering and regulating the activities of Edge and agreement corporations, which are specialized institutions used for international and foreign business;
- authorizing foreign investments of member banks, Edge and agreement corporations, and bank holding companies and regulating the activities of foreign firms acquired by such investors; and
- establishing supervisory policy and practices regarding foreign lending by state member banks.

Under federal law, U.S. banking organizations generally may conduct a wider range of activities abroad than they may conduct in this country.

The Board has broad discretionary powers to regulate the foreign activities of member banks and bank holding companies so that, in financing U.S. trade and investments abroad, U.S. banking organizations can be fully competitive with institutions of the host country. U.S. banks also may conduct deposit and loan business in U.S. markets outside their home states through Edge and agreement corporations if the operations of the corporations are related to international transactions.

The Federal Reserve examines the international operations of state member banks, Edge and agreement corporations, and bank holding companies principally at the U.S. head offices of these organizations. When appropriate, the Federal Reserve will conduct an examination at the foreign operations of a U.S. banking organization in order to review the accuracy of financial and operational information maintained at the head office as well as to test the organization's adherence to safe and sound banking practices and to evaluate its efforts to implement corrective measures. Examinations abroad are conducted in cooperation with the responsible foreign-country supervisor.

Supervision of U.S. Activities of Foreign Banking Organizations

Although foreign banks have been operating in the United States for more than a century, before 1978 the U.S. branches and agencies of these banks were not subject to supervision or regulation by any federal banking agency. When Congress enacted the International Banking Act of 1978 (IBA), it created a federal regulatory structure for the activities of foreign banks with U.S. branches and agencies. The IBA established a policy of "national treatment" for foreign banks operating in the United States to promote competitive equality between them and domestic institutions. This policy generally gives foreign banking organizations operating in the United States the same powers as U.S. banking organizations and subjects them to the same restrictions and obligations that apply to the domestic operations of U.S. banking organizations.

The Foreign Bank Supervision Enhancement Act of 1991 (FBSEA) increased the Federal Reserve's supervisory responsibility and authority over the U.S. operations of foreign banking organizations and eliminated gaps in the supervision and regulation of foreign banking organizations. The FBSEA amended the IBA to require foreign banks to obtain Federal Reserve approval before establishing branches, agencies, or commercial lending company subsidiaries in the United States. An application by a foreign bank to establish such offices or subsidiaries generally may be approved only if the Board determines that the foreign bank and any foreign-bank parents engage in banking business outside the United States and are subject to comprehensive supervision or regulation on a consolidated basis by their home-country supervisors. The Board may also take into account other factors, such as whether the home-country supervisor has consented

to the proposed new office or subsidiary, the financial and managerial resources of the foreign bank, the condition of any existing U.S. offices, the bank's compliance with U.S. law, the extent of access by the Federal Reserve to information on the foreign bank from the bank and its home-country supervisor, and whether both the foreign bank and its home-country supervisor have taken actions to combat money laundering. The Board's prior approval is also required before a foreign bank may establish a representative office and, in approving the establishment of such an office, the Board takes the above-mentioned standards into account to the extent deemed appropriate.

The FBSEA also increased the responsibility and the authority of the Federal Reserve to regularly examine the U.S. operations of foreign banks. Under the FBSEA, all branches and agencies of foreign banks must be examined on-site at least once every twelve months, although this period may be extended to eighteen months if the branch or agency meets certain criteria. Supervisory actions resulting from examinations may be taken by the Federal Reserve alone or with other agencies. Representative offices are also subject to examination by the Federal Reserve.

The Federal Reserve evaluates transactions between a bank and its affiliates to determine the effect of the transactions on the bank's condition.

The Federal Reserve coordinates the supervisory program for the U.S. operations of foreign banking organizations with the other federal and state banking agencies. Since a foreign banking organization may have both federally and state-chartered offices in the United States, the Federal Reserve plays a key role in assessing the condition of the organization's entire U.S. operations and the foreign banking organization's ability to support its U.S. operations. In carrying out their supervisory responsibilities, the Federal Reserve and other U.S. supervisors rely on two supervisory tools: SOSA rankings and ROCA ratings. SOSA (the Strength of Support Assessment) is the examiners' assessment of a foreign bank's ability to provide support for its U.S. operations. The ROCA rating is an assessment of the organization's U.S. activities in terms of its risk management, operational controls, compliance, and asset quality.

Under the Bank Holding Company Act and the IBA, the Federal Reserve is also responsible for approving, reviewing, and monitoring the U.S. nonbanking activities of foreign banking organizations that have a branch, agency, commercial lending company, or subsidiary bank in the United States. In addition, such foreign banks must obtain Federal Reserve approval to acquire more than 5 percent of the shares of a U.S. bank or bank holding company.

Supervision of Transactions with Affiliates

As part of the supervisory process, the Federal Reserve also evaluates transactions between a bank and its affiliates to determine the effect of the transactions on the bank's condition and to ascertain whether the transac-

tions are consistent with sections 23A and 23B of the Federal Reserve Act, as implemented by the Federal Reserve Board's Regulation W. Since the GLB Act increased the range of affiliations permitted to banking organizations, sections 23A and 23B play an increasingly important role in limiting the risk to depository institutions from these broader affiliations. Among other things, section 23A prohibits a bank from purchasing an affiliate's low-quality assets. In addition, it limits a bank's loans and other extensions of credit to any single affiliate to 10 percent of the bank's capital and surplus, and it limits loans and other extensions of credit to all affiliates in the aggregate to 20 percent of the bank's capital and surplus. Section 23B requires that all transactions between a bank and its affiliates be on terms that are substantially the same, or at least as favorable, as those prevailing at the time for comparable transactions with nonaffiliated companies. The Federal Reserve Board is the only banking agency that has the authority to exempt any bank from these requirements. During the course of an examination, examiners review a banking organization's intercompany transactions for compliance with these statutes and Regulation W.

The Federal Reserve establishes standards designed to ensure that banking organizations operate in a safe and sound manner and in accordance with applicable law.

Regulatory Functions

As a bank regulator, the Federal Reserve establishes standards designed to ensure that banking organizations operate in a safe and sound manner and in accordance with applicable law. These standards may take the form of regulations, rules, policy guidelines, or supervisory interpretations and may be established under specific provisions of a law or under more general legal authority. Regulatory standards may be either restrictive (limiting the scope of a banking organization's activities) or permissive (authorizing banking organizations to engage in certain activities). (For a complete list of Federal Reserve regulations, see appendix A.)

In many cases, the Federal Reserve Board's regulations are adopted to implement specific legislative initiatives or requirements passed by Congress. These statutory provisions may have been adopted by Congress to respond to past crises or problems or to update the nation's banking laws to respond to changes in the marketplace. For example, in response to the savings and loan crisis and financial difficulties in the banking industry in the late 1980s and early 1990s, Congress enacted several laws to improve the condition of individual institutions and of the overall banking industry, including the Competitive Equality Banking Act of 1987; the Financial Institutions Reform, Recovery, and Enforcement Act of 1989; and the Federal Deposit Insurance Corporation Improvement Act of 1991. These legislative initiatives restricted banking practices, limited supervisors' discretion in dealing with weak banks, imposed new regulatory requirements—including prompt corrective action—and strengthened supervisory oversight overall.

More recently, Congress has adopted other laws to respond to the growing integration of banking markets, both geographically and functionally, and the increasing convergence of banking, securities, and insurance activities. The Riegle-Neal Interstate Banking and Branching Efficiency Act of 1994 significantly reduced the legal barriers that had restricted the ability of banks and bank holding companies to expand their activities across state lines. In 1999, Congress passed the GLB Act, which repealed certain Depression-era banking laws and permitted banks to affiliate with securities and insurance firms within financial holding companies.

Acquisitions and Mergers

Under the authority assigned to the Federal Reserve by the Bank Holding Company Act of 1956 as amended, the Bank Merger Act of 1960, and the Change in Bank Control Act of 1978, the Federal Reserve Board maintains broad authority over the structure of the banking system in the United States.

The Bank Holding Company Act assigned to the Federal Reserve primary responsibility for supervising and regulating the activities of bank holding companies. Through this act, Congress sought to achieve two basic objectives: (1) to avoid the creation of a monopoly or the restraint of trade in the banking industry through the acquisition of additional banks by bank holding companies and (2) to keep banking and commerce separate by restricting the nonbanking activities of bank holding companies. Historically, bank holding companies could engage only in banking activities and other activities that the Federal Reserve determined to be closely related to banking. But since the passage of the GLB Act, a bank holding company that qualifies to become a financial holding company may engage in a broader range of financially related activities, including full-scope securities underwriting and dealing, insurance underwriting and sales, and merchant banking. A bank holding company seeking financial holding company status must file a written declaration with the Federal Reserve System, certifying that the company meets the capital, managerial, and other requirements to be a financial holding company.

Bank Acquisitions

Under the Bank Holding Company Act, a firm that seeks to become a bank holding company must first obtain approval from the Federal Reserve. The act defines a *bank holding company* as any company that directly or indirectly owns, controls, or has the power to vote 25 percent or more of any class of the voting shares of a bank; controls in any manner the election of a majority of the directors or trustees of a bank; or is found to exercise a controlling influence over the management or policies of a bank. A bank holding company must obtain the approval of the Federal

Reserve before acquiring more than 5 percent of the shares of an additional bank or bank holding company. All bank holding companies must file certain reports with the Federal Reserve System.

When considering applications to acquire a bank or a bank holding company, the Federal Reserve is required to take into account the likely effects of the acquisition on competition, the convenience and needs of the communities to be served, the financial and managerial resources and future prospects of the companies and banks involved, and the effectiveness of the company's policies to combat money laundering. In the case of an interstate bank acquisition, the Federal Reserve also must consider certain other factors and may not approve the acquisition if the resulting organization would control more than 10 percent of all deposits held by insured depository institutions. When a foreign bank seeks to acquire a U.S. bank, the Federal Reserve also must consider whether the foreign banking organization is subject to comprehensive supervision or regulation on a consolidated basis by its home-country supervisor.

The Federal Reserve is responsible for changes in the control of bank holding companies and state member banks.

Bank Mergers

Another responsibility of the Federal Reserve is to act on proposed bank mergers when the resulting institution would be a state member bank. The Bank Merger Act of 1960 sets forth the factors to be considered in evaluating merger applications. These factors are similar to those that must be considered in reviewing bank acquisition proposals by bank holding companies. To ensure that all merger applications are evaluated in a uniform manner, the act requires that the responsible agency request reports from the Department of Justice and from the other approving banking agencies addressing the competitive impact of the transaction.

Other Changes in Bank Control

The Change in Bank Control Act of 1978 authorizes the federal bank regulatory agencies to deny proposals by a single "person" (which includes an individual or an entity), or several persons acting in concert, to acquire control of an insured bank or a bank holding company. The Federal Reserve is responsible for approving changes in the control of bank holding companies and state member banks, and the FDIC and the OCC are responsible for approving changes in the control of insured state nonmember and national banks, respectively. In considering a proposal under the act, the Federal Reserve must review several factors, including the financial condition, competence, experience, and integrity of the acquiring person or group of persons; the effect of the transaction on competition; and the adequacy of the information provided by the acquiring party.

Formation and Activities of Financial Holding Companies

As authorized by the GLB Act, the Federal Reserve Board's regulations allow a bank holding company or a foreign banking organization to become a financial holding company and engage in an expanded array of financial activities if the company meets certain capital, managerial, and other criteria. Permissible activities for financial holding companies include conducting securities underwriting and dealing, serving as an insurance agent and underwriter, and engaging in merchant banking. Other permissible activities include those that the Federal Reserve Board, after consulting with the Secretary of the Treasury, determines to be financial in nature or incidental to financial activities. Financial holding companies also may engage to a limited extent in a nonfinancial activity if the Board determines that the activity is complementary to one or more of the company's financial activities and would not pose a substantial risk to the safety or soundness of depository institutions or the financial system.

Capital Adequacy Standards

A key goal of banking regulation is to ensure that banks maintain sufficient capital to absorb reasonably likely losses.

A key goal of banking regulation is to ensure that banks maintain sufficient capital to absorb reasonably likely losses. In 1989, the federal banking regulators adopted a common standard for measuring capital adequacy that is broadly based on the risks of an institution's investments. This common standard, in turn, was based on the 1988 agreement "International Convergence of Capital Measurement and Capital Standards" (commonly known as the Basel Accord) developed by the Basel Committee on Banking Supervision. This committee, which is associated with the Bank for International Settlements headquartered in Switzerland, is composed of representatives of the central banks or bank supervisory authorities from Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Spain, Sweden, Switzerland, the United Kingdom, and the United States.

The risk-based capital standards require institutions that assume greater risk to hold higher levels of capital. Moreover, these standards take into account risks associated with activities that are not included on a bank's balance sheet, such as the risks arising from commitments to make loans. Because they have been accepted by the bank supervisory authorities of most of the countries with major international banking centers, these standards promote safety and soundness and reduce competitive inequities among banking organizations operating within an increasingly global market.

Recognizing that the existing risk-based capital standards were in need of significant enhancements to address the activities of complex bank-

ing organizations, the Basel Committee began work to revise the Basel Accord in 1999 and, in June 2004, endorsed a revised framework, which is referred to as Basel II. Basel II has three "pillars" that make up the framework for assessing capital adequacy. Pillar I, minimum regulatory capital requirements, more closely aligns banking organizations' capital levels with their underlying risks. Pillar II, supervisory oversight, requires supervisors to evaluate banking organizations' capital adequacy and to encourage better risk-management techniques. Pillar III, market discipline, calls for enhanced public disclosure of banking organizations' risk exposures.

Financial Disclosures by State Member Banks

State member banks that issue securities registered under the Securities Exchange Act of 1934 must disclose certain information of interest to investors, including annual and quarterly financial reports and proxy statements. By statute, the Federal Reserve administers these requirements and has adopted financial disclosure regulations for state member banks that are substantially similar to the SEC's regulations for other public companies.

Securities Credit

The Securities Exchange Act of 1934 requires the Federal Reserve to regulate the extension of credit used in connection with the purchase of securities. Through its regulations, the Board establishes the minimum amount the buyer must put up when purchasing a security. This minimum amount is known as the margin requirement. In fulfilling its responsibility under the act, the Federal Reserve limits the amount of credit that may be provided by securities brokers and dealers (Regulation T) and the amount of securities credit extended by banks and other lenders (Regulation U). These regulations generally apply to credit-financed purchases of securities traded on securities exchanges and certain securities traded over the counter when the credit is collateralized by such securities. In addition, Regulation X prohibits borrowers who are subject to U.S. laws from obtaining such credit overseas on terms more favorable than could be obtained from a domestic lender.

In general, compliance with the Federal Reserve's margin regulations is enforced by several federal regulatory agencies. The federal agencies that regulate financial institutions check for Regulation U compliance during examinations. The Federal Reserve checks for Regulation U compliance on the part of securities credit lenders not otherwise regulated by federal agencies. Compliance with Regulation T is verified during examinations of broker-dealers by the securities industry's self-regulatory organizations under the general oversight of the SEC.

6 Consumer and Community Affairs

The number of federal laws intended to protect consumers in credit and other financial transactions has been growing since the late 1960s. Congress has assigned to the Federal Reserve the duty of implementing many of these laws to ensure that consumers receive comprehensive information and fair treatment.

Among the Federal Reserve's responsibilities in this area are

- writing and interpreting regulations to carry out many of the major consumer protection laws,
- reviewing bank compliance with the regulations,
- investigating complaints from the public about state member banks' compliance with consumer protection laws,
- addressing issues of state and federal jurisdiction,
- testifying before Congress on consumer protection issues, and
- conducting community development activities.

In carrying out these responsibilities, the Federal Reserve is advised by its Consumer Advisory Council, whose members represent the interests of consumers, community groups, and creditors nationwide. Meetings of the council, which take place three times a year at the Federal Reserve Board in Washington, D.C., are open to the public.

Consumer Protection

Most financial transactions involving consumers are covered by consumer protection laws. These include transactions involving credit, charge, and debit cards issued by financial institutions and credit cards issued by retail establishments; automated teller machine transactions and other electronic fund transfers; deposit account transactions; automobile leases; mortgages and home equity loans; and lines of credit and other unsecured credit.

Writing and Interpreting Regulations

The Federal Reserve Board writes regulations to implement many of the major consumer protection laws. These regulations may cover not only banks but also certain businesses, including finance companies, mortgage brokers, retailers, and automobile dealers. For example, Congress passed

the Truth in Lending Act to ensure that consumers have adequate information about credit. The Board implemented that law by writing Regulation Z, which requires banks and other creditors to provide detailed information to consumers about the terms and cost of consumer credit for mortgages, car loans, credit and charge cards, and other credit products. The Board also revises and updates its regulations to address new products or changes in technology, to implement changes to existing legislation, or to address problems encountered by consumers.

Educating Consumers about Consumer Protection Laws

Well-educated consumers are the best consumer protection in the market.

Well-educated consumers are the best consumer protection in the market. They know their rights and responsibilities, and they use the information provided in disclosures to shop and compare. The Federal Reserve Board maintains a consumer information web site with educational materials related to the consumer protection regulations developed by the Board (www.federalreserve.gov/consumers.htm). In addition, the Federal Reserve staff uses consumer surveys and focus groups to learn more about what issues are important to consumers and to develop and test additional educational resources.

Enforcing Consumer Protection Laws

The Federal Reserve has a comprehensive program to examine financial institutions and other entities that it supervises to ensure compliance with consumer protection laws and regulations. Its enforcement responsibilities generally extend only to state-chartered banks that are members of the Federal Reserve System and to certain foreign banking organizations. Other federal regulators are responsible for examining banks, thrift institutions, and credit unions under their jurisdictions and for taking enforcement action.

Each Reserve Bank has specially trained examiners who regularly evaluate banks' compliance with consumer protection laws and their Community Reinvestment Act (CRA) performance. Most banks are evaluated every forty-eight months, although large banks are examined every twenty-four months and poorly rated banks are examined more frequently.

To make the most effective and efficient use of resources while ensuring compliance with consumer protection laws and regulations, the Federal Reserve uses a risk-focused approach to supervision, focusing most intensely on those areas involving the greatest compliance risk. Examinations always include a comprehensive assessment of an institution's CRA performance in order to present to the public a full and fair portrait of the institution's efforts. Examiners also assess the broad range of large complex banking organizations' activities to determine the level and trend of compliance risk in the area of consumer protection.

In accordance with the Community Reinvestment Act of 1977, the Federal Reserve reviews a bank's efforts to meet the credit and community development needs of its entire community, including low- and moderate-income neighborhoods; for example, it looks at the extent to which a bank has programs that contribute to the building of affordable housing and to other aspects of community development. When deciding whether to approve an application for a bank acquisition or merger or for the formation of a bank holding company, the Federal Reserve takes into account an institution's performance under the CRA. An important aspect of the process is that it gives the public the opportunity to submit written comments on the proposal. These comments, which often provide insight into a financial institution's CRA performance, are reviewed by Federal Reserve staff and considered by the Board when it evaluates an application.

The Federal Reserve reviews a bank's efforts to meet the credit and community development needs of its entire community.

At the end of this chapter is a list of the consumer protection laws for which the Federal Reserve has rule-writing or enforcement responsibility, the dates the laws were enacted, and the highlights of the laws' provisions.

Consumer Complaint Program

The Federal Reserve responds to inquiries and complaints from the public about the policies and practices of financial institutions involving consumer protection issues. Each Reserve Bank has staff whose primary responsibility is to investigate consumer complaints about state member banks and refer complaints about other institutions to the appropriate regulatory agencies. The Federal Reserve's responses not only address the concerns raised but also educate consumers about financial matters.

The Federal Reserve Board maintains information on consumer inquiries and complaints in a database, which it regularly reviews to identify potential problems at individual financial institutions and, as required by the Federal Trade Commission Improvement Act, to uncover potentially unfair or deceptive practices within the banking industry. Complaint data are a critical component of the risk-focused supervisory program and are used as a risk factor to assess a bank's compliance with consumer regulations. Data about consumer complaints are also used to determine the need for future regulations or educational efforts.

Community Affairs

Community affairs programs at the Board and the twelve Federal Reserve Banks promote community development and fair and impartial access to credit. Community affairs offices at the Board and Reserve Banks engage in a wide variety of activities to help financial institutions, community-based organizations, government entities, and the public understand and

address financial services issues that affect low- and moderate-income people and geographic regions. Each office responds to local needs in its District and establishes its own programs to

- foster depository institutions' active engagement in providing credit and other banking services to their entire communities, particularly traditionally underserved markets;
- encourage mutually beneficial cooperation among community organizations, government agencies, financial institutions, and other community development practitioners;
- develop greater public awareness of the benefits and risks of financial products and of the rights and responsibilities that derive from community investment and fair lending regulations; and
- promote among policy makers, community leaders, and private-sector decision makers a better understanding of the practices, processes, and resources that result in successful community development programs.

Each Federal Reserve Bank develops specific products and services to meet the informational needs of its region. The community affairs offices issue a wide array of publications, sponsor a variety of public forums, and provide technical information on community and economic development and on fair and equal access to credit and other banking services.

The Fair Housing Act prohibits discrimination in the extension of housing credit.

Consumer Protection Laws

- ***Fair Housing Act (1968)***
  Prohibits discrimination in the extension of housing credit on the basis of race, color, religion, national origin, sex, handicap, or family status.
- ***Truth in Lending Act (1968)***
  Requires uniform methods for computing the cost of credit and for disclosing credit terms. Gives borrowers the right to cancel, within three days, certain loans secured by their residences. Prohibits the unsolicited issuance of credit cards and limits cardholder liability for unauthorized use. Also imposes limitations on home equity loans with rates or fees above a specified threshold.
- ***Fair Credit Reporting Act (1970)***
  Protects consumers against inaccurate or misleading information in credit files maintained by credit-reporting agencies; requires credit-reporting agencies to allow credit applicants to correct erroneous reports.
- ***Flood Disaster Protection Act of 1973***
  Requires flood insurance on property in a flood hazard area that comes under the National Flood Insurance Program.
- ***Fair Credit Billing Act (1974)***
  Specifies how creditors must respond to billing-error complaints from consumers; imposes requirements to ensure that creditors handle ac-

counts fairly and promptly. Applies primarily to credit and charge card accounts (for example, store card and bank card accounts). Amended the Truth in Lending Act.

- ***Equal Credit Opportunity Act (1974)***
  Prohibits discrimination in credit transactions on several bases, including sex, marital status, age, race, religion, color, national origin, the receipt of public assistance funds, or the exercise of any right under the Consumer Credit Protection Act. Requires creditors to grant credit to qualified individuals without requiring cosignature by spouses, to inform unsuccessful applicants in writing of the reasons credit was denied, and to allow married individuals to have credit histories on jointly held accounts maintained in the names of both spouses. Also entitles a borrower to a copy of a real estate appraisal report.
- ***Real Estate Settlement Procedures Act of 1974***
  Requires that the nature and costs of real estate settlements be disclosed to borrowers. Also protects borrowers against abusive practices, such as kickbacks, and limits the use of escrow accounts.
- ***Home Mortgage Disclosure Act of 1975***
  Requires mortgage lenders to annually disclose to the public data about the geographic distribution of their applications, originations, and purchases of home-purchase and home-improvement loans and refinancings. Requires lenders to report data on the ethnicity, race, sex, income of applicants and borrowers, and other data. Also directs the Federal Financial Institutions Examination Council, of which the Federal Reserve is a member, to make summaries of the data available to the public.
- ***Consumer Leasing Act of 1976***
  Requires that institutions disclose the cost and terms of consumer leases, such as automobile leases.
- ***Fair Debt Collection Practices Act (1977)***
  Prohibits abusive debt collection practices. Applies to banks that function as debt collectors for other entities.
- ***Community Reinvestment Act of 1977***
  Encourages financial institutions to help meet the credit needs of their entire communities, particularly low- and moderate-income neighborhoods.
- ***Right to Financial Privacy Act of 1978***
  Protects bank customers from the unlawful scrutiny of their financial records by federal agencies and specifies procedures that government authorities must follow when they seek information about a customer's financial records from a financial institution.
- ***Electronic Fund Transfer Act (1978)***
  Establishes the basic rights, liabilities, and responsibilities of consumers who use electronic fund transfer services and of financial institutions that offer these services. Covers transactions conducted at automated teller machines, at point-of-sale terminals in stores, and through tele-

The Community Reinvestment Act encourages financial institutions to help meet the credit needs of their entire communities.

phone bill-payment plans and preauthorized transfers to and from a customer's account, such as direct deposit of salary or Social Security payments.

- ***Federal Trade Commission Improvement Act (1980)***
  Authorizes the Federal Reserve to identify unfair or deceptive acts or practices by banks and to issue regulations to prohibit them. Using this authority, the Federal Reserve has adopted rules substantially similar to those adopted by the FTC that restrict certain practices in the collection of delinquent consumer debt, for example, practices related to late charges, responsibilities of cosigners, and wage assignments.
- ***Expedited Funds Availability Act (1987)***
  Specifies when depository institutions must make funds deposited by check available to depositors for withdrawal. Requires institutions to disclose to customers their policies on funds availability.
- ***Women's Business Ownership Act of 1988***
  Extends to applicants for business credit certain protections afforded consumer credit applicants, such as the right to an explanation for credit denial. Amended the Equal Credit Opportunity Act.
- ***Fair Credit and Charge Card Disclosure Act of 1988***
  Requires that applications for credit cards that are sent through the mail, solicited by telephone, or made available to the public (for example, at counters in retail stores or through catalogs) contain information about key terms of the account. Amended the Truth in Lending Act.
- ***Home Equity Loan Consumer Protection Act of 1988***
  Requires creditors to provide consumers with detailed information about open-end credit plans secured by the consumer's dwelling. Also regulates advertising of home equity loans and restricts the terms of home equity loan plans.
- ***Truth in Savings Act (1991)***
  Requires that depository institutions disclose to depositors certain information about their accounts—including the annual percentage yield, which must be calculated in a uniform manner—and prohibits certain methods of calculating interest. Regulates advertising of savings accounts.
- ***Home Ownership and Equity Protection Act of 1994***
  Provides additional disclosure requirements and substantive limitations on home-equity loans with rates or fees above a certain percentage or amount. Amended the Truth in Lending Act.
- ***Gramm-Leach-Bliley Act, title V, subpart A, Disclosure of Nonpublic Personal Information (1999)***
  Describes the conditions under which a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties, provides a method for consumers to opt out of information sharing with nonaffiliated third parties, and requires a financial institution to notify consumers about its privacy policies and practices.

The Fair Credit and Charge Card Disclosure Act requires that applications for credit cards contain information about key terms of the account.

- ***Fair and Accurate Credit Transaction Act of 2003***
  Enhances consumers' ability to combat identity theft, increases the accuracy of consumer reports, allows consumers to exercise greater control over the type and amount of marketing solicitations they receive, restricts the use and disclosure of sensitive medical information, and establishes uniform national standards in the regulation of consumer reporting. Amended the Fair Credit Reporting Act.

7 The Federal Reserve in the U.S. Payments System

The Federal Reserve plays an important role in the U.S. payments system. The twelve Federal Reserve Banks provide banking services to depository institutions and to the federal government. For depository institutions, they maintain accounts and provide various payment services, including collecting checks, electronically transferring funds, and distributing and receiving currency and coin. For the federal government, the Reserve Banks act as fiscal agents, paying Treasury checks; processing electronic payments; and issuing, transferring, and redeeming U.S. government securities.

By creating the Federal Reserve System, Congress intended to eliminate the severe financial crises that had periodically swept the nation, especially the sort of financial panic that occurred in 1907. During that episode, payments were disrupted throughout the country because many banks and clearinghouses refused to clear checks drawn on certain other banks, a practice that contributed to the failure of otherwise solvent banks. To address these problems, Congress gave the Federal Reserve System the authority to establish a nationwide check-clearing system. The System, then, was to provide not only an elastic currency—that is, a currency that would expand or shrink in amount as economic conditions warranted—but also an efficient and equitable check-collection system.

Bank panic of 1907

Congress was also concerned about some banks' paying less than the full amount of checks deposited by their customers because some paying banks charged fees to presenting banks to pay checks. To avoid paying presentment fees, many collecting banks routed checks through banks that were not charged presentment fees by paying banks. This practice, called circuitous routing, resulted in extensive delays and inefficiencies in the check-collection system. In 1917, Congress amended the Federal Reserve Act to prohibit banks from charging the Reserve Banks presentment fees and to authorize nonmember banks as well as member banks to collect checks through the Federal Reserve System.

In passing the Monetary Control Act of 1980, Congress reaffirmed its intention that the Federal Reserve should promote an efficient nationwide payments system. The act subjects all depository institutions, not just member commercial banks, to reserve requirements and grants them equal access to Reserve Bank payment services. It also encourages competition between the Reserve Banks and private-sector providers of payment services by requiring the Reserve Banks to charge fees for certain payments services listed in the act and to recover the costs of providing these services over the long run.

The Federal Reserve performs an important role as an intermediary in clearing and settling interbank payments.

More recent congressional action has focused increasingly on improving the efficiency of the payments system by encouraging increased use of technology. In 1987, Congress enacted the Expedited Funds Availability Act (EFAA), which gave the Board, for the first time, the authority to regulate the payments system in general, not just those payments made through the Reserve Banks. The Board used its authority under the EFAA to revamp the check-return system, improve the presentment rights of private-sector banks, and establish rules governing the time that banks can hold funds from checks deposited into customer accounts before making the funds available for withdrawal. In 2003, Congress enacted the Check Clearing for the 21st Century Act, which further enhanced the efficiency of the payments system by reducing legal and practical impediments to check truncation and the electronic collection of checks, services that speed up check collection and reduce associated costs.

Financial Services

The U.S. payments system is the largest in the world. Each day, millions of transactions, valued in the trillions of dollars, are conducted between sellers and purchasers of goods, services, or financial assets. Most of the payments underlying those transactions flow between depository institutions, a large number of which maintain accounts with the Reserve Banks. The Federal Reserve therefore performs an important role as an intermediary in clearing and settling interbank payments. The Reserve

Banks settle payment transactions efficiently by debiting the accounts of the depository institutions making payments and by crediting the accounts of depository institutions receiving payments. Moreover, as the U.S. central bank, the Federal Reserve is immune from liquidity problems—not having sufficient funds to complete payment transactions—and credit problems that could disrupt its clearing and settlement activities.

The Federal Reserve plays a vital role in both the nation's retail and wholesale payments systems, providing a variety of financial services to depository institutions. Retail payments are generally for relatively small-dollar amounts and often involve a depository institution's retail clients—individuals and smaller businesses. The Reserve Banks' retail services include distributing currency and coin, collecting checks, and electronically transferring funds through the automated clearinghouse system. By contrast, wholesale payments are generally for large-dollar amounts and often involve a depository institution's large corporate customers or counterparties, including other financial institutions. The Reserve Banks' wholesale services include electronically transferring funds through the Fedwire Funds Service and transferring securities issued by the U.S. government, its agencies, and certain other entities through the Fedwire Securities Service. Because of the large amounts of funds that move through the Reserve Banks every day, the System has policies and procedures to limit the risk to the Reserve Banks from a depository institution's failure to make or settle its payments.

An important function of the Federal Reserve is ensuring that enough cash is in circulation to meet the public's demand.

Retail Services

Currency and Coin

An important function of the Federal Reserve is ensuring that enough cash—that is, currency and coin—is in circulation to meet the public's demand. When Congress established the Federal Reserve, it recognized that the public's demand for cash is variable. This demand increases or decreases seasonally and as the level of economic activity changes. For example, in the weeks leading up to a holiday season, depository institutions increase their orders of currency and coin from Reserve Banks to meet their customers' demand. Following the holiday season, depository institutions ship excess currency and coin back to the Reserve Banks, where it is credited to their accounts.

Each of the twelve Reserve Banks is authorized by the Federal Reserve Act to issue currency, and the Department of Treasury is authorized to issue coin. The Secretary of the Treasury approves currency designs, and the Treasury's Bureau of Engraving and Printing prints the notes. The Federal Reserve Board places an annual printing order with the bureau

and pays the bureau for the cost of printing. The Federal Reserve Board coordinates shipments of currency to the Reserve Banks around the country. The Reserve Banks, in turn, issue the notes to the public through depository institutions. Federal Reserve notes are obligations of the Reserve Banks. The Reserve Banks secure the currency they issue with legally authorized collateral, most of which is in the form of U.S. Treasury securities held by the Reserve Banks. Coin, unlike currency, is issued by the Treasury, not the Reserve Banks. The Reserve Banks order coin from the Treasury's Bureau of the Mint and pay the Mint the full face value of coin, rather than the cost to produce it. The Reserve Banks then distribute coin to the public through depository institutions.

Demand Treasury note, 1861

Silver certificate, 1880

Although the issuance of paper money in this country dates back to 1690, the U.S. government did not issue paper currency with the intent that it circulate as money until 1861, when Congress approved the issuance of demand Treasury notes. All currency issued by the U.S. government since then remains legal tender, including silver certificates, which have a blue seal for the Department of the Treasury; United States notes, which have a red seal; and national bank notes, which have a brown seal. Today, nearly all currency in circulation is in the form of Federal Reserve notes, which

were first issued in 1914 and have a green Treasury seal. Currency is redesigned periodically to incorporate new anti-counterfeiting features. When currency is redesigned, all previous Federal Reserve notes remain valid.

National bank note, Winters National Bank of Dayton, Ohio, 1901

When currency flows back to the Reserve Banks, each deposit is counted, verified, and authenticated. Notes that are too worn for recirculation (unfit notes) and those that are suspected of being counterfeit are culled out. Suspect notes are forwarded to the United States Secret Service, and unfit notes are destroyed at the Reserve Banks on behalf of the Treasury. Notes that can be recirculated to the public are held in Reserve Bank vaults, along with new notes, until they are needed to meet demand. Coin that is received by Reserve Banks is verified by weight rather than piece-counted, as currency is.

Today, currency and coin are used primarily for small-dollar transactions and thus account for only a small proportion of the total dollar value of all monetary transactions. During 2003, Reserve Banks delivered to depository institutions about 36.6 billion notes having a value of $633.4 billion and received from depository institutions about 35.7 billion notes having a value of $596.9 billion. Of the total received by Reserve Banks, 7.4 billion notes, with a face value of $101.3 billion, were deemed to be unfit to continue to circulate and were destroyed. The difference between the amount of currency paid to depository institutions and the amount of currency received from circulation equals the change in demand for currency resulting from economic activity. In 2003, the increase in demand was $36.5 billion.

Over the past five decades, the value of currency and coin in circulation has risen dramatically—from $31.2 billion in 1955 to $724.2 billion in 2003 (table 7.1).[1] The total number of notes in circulation (24.8 billion at

1. Current data on currency and coin can be found on the Board's web site (www.federalreserve.gov), under "Payment Systems."

the end of 2003) and the demand for larger denominations ($20, $50, and $100 notes) has also increased (table 7.2). In 1960, these larger denominations accounted for 64 percent of the total value of currency in circulation; by the end of 2003, they accounted for 95 percent. Because the U.S. dollar is highly regarded throughout the world as a stable and readily negotiable currency, much of the increased demand for larger-denomination notes has arisen outside of the United States. Although the exact value of U.S. currency held outside the country is unknown, Federal Reserve economists estimate that from one-half to two-thirds of all U.S. currency circulates abroad.

Table 7.1

Value of currency and coin in circulation, selected years, 1955–2003

Millions of dollars

Year	Currency*	Coin	Total
1955	29,242	1,916	31,158
1960	30,442	2,426	32,868
1965	38,029	4,027	42,056
1970	45,915	5,986	51,901
1975	68,059	8,285	76,344
1980	109,515	11,641	121,156
1985	182,003	15,456	197,459
1990	268,206	18,765	286,971
1995	401,517	22,727	424,244
2000	563,970	29,724	593,694
2001	612,273	31,028	643,301
2002	654,785	32,733	687,518
2003	690,267	33,927	724,194

* Currency in circulation includes Federal Reserve notes, silver certificates, United States notes, and national bank notes.

Table 7.2

Estimated value of currency in circulation by denomination, selected years, 1960–2003

Billions of dollars

Year	Denomination								Total
	1	2	5	10	20	50	100	Other*	
1960	1.5	.1	2.2	6.7	10.5	2.8	6.0	.6	30.4
1970	2.1	.1	2.9	8.4	16.6	4.4	10.9	.5	45.9
1980	3.1	.7	4.1	11.0	36.4	12.2	41.6	.4	109.5
1990	5.1	.8	6.3	12.6	69.0	33.9	140.2	.3	268.2
2000	7.7	1.2	8.9	14.5	98.6	55.1	377.7	.3	564.0
2003	8.2	1.4	9.7	15.2	107.8	59.9	487.8	.3	690.3

* Other denominations include the $500, $1,000, $5,000, and $10,000 notes. No denominations larger than $100 have been printed since 1946 or issued since 1969. The majority of these notes are held by private collectors, currency dealers, and financial institutions for display.

Check Processing

While cash is convenient for small-dollar transactions, for larger-value transactions individuals, businesses, and governments generally use checks or electronic funds transfers. Measured by the number used, checks continue to be the preferred noncash payment method; however, their use has begun to decline in favor of electronic methods. In 2001, the Federal Reserve conducted an extensive survey on the use of checks and other noncash payment instruments in the United States and compared the results with a 1979 study of noncash payments and similar data collected in 1995. The survey results indicated that check usage peaked sometime during the mid-1990s and has declined since then. For example, the survey found that checks represented 59.5 percent of retail noncash payments in 2000, compared with 77.1 percent just five years earlier and 85.7 percent in 1979. The total value of checks paid declined from an estimated $50.7 trillion in 1979 to $39.3 trillion in 2000 (both in 2000 dollars).[2]

In 2004, the Federal Reserve conducted another study to determine the changes in noncash payments from 2000 to 2003. That study found that the number of noncash payments had grown since 2000 and that checks were the only payment instrument being used less frequently than in 2000

2. See Gerdes, Geoffrey R., and Jack K. Walton II, "The Use of Checks and Other Noncash Payment Instruments in the United States," *Federal Reserve Bulletin,* vol. 88 (August 2002), pp. 360–74.

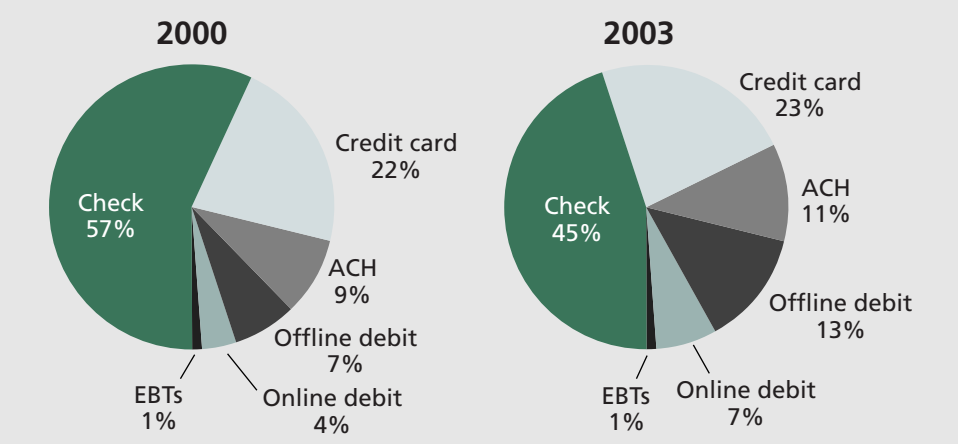
(table 7.3). Chart 7.1 illustrates the changes in the distribution of noncash payments from 2000 to 2003.

Table 7.3
Number of noncash payments, 2000 and 2003

	2000 estimate (billions)	2003 estimate (billions)	CAGR*
Noncash payments	72.5	81.2	38%
Check	41.9	36.7	–4.3%
Credit card	15.6	19.0	6.7%
ACH	6.2	9.1	13.4%
Offline debit	5.3	10.3	24.9%
Online debit	3.0	5.3	21.0%
Electronic benefits transfers (EBTs)	0.5	0.8	15.4%

* Compound annual growth rate.

Chart 7.1
Distribution of number of noncash payments, 2000 and 2003



Of the estimated 36.7 billion checks paid in 2003, approximately 8.7 billion were "on-us checks," that is, checks deposited in the same institution on which they were drawn. In 2003, the Reserve Banks processed more than 58 percent of interbank checks, checks not drawn on the institution at which they were deposited. Depository institutions cleared the remaining checks through private arrangements among themselves. These private arrangements include sending checks directly to the depository institution on which they are drawn, depositing the checks for collection with a correspondent bank, or delivering the checks to a clearinghouse for exchange. Processing interbank checks requires a mechanism for

exchanging the checks as well as for the related movement of funds, or settlement, among the depository institutions involved.

For checks collected through the Reserve Banks, the account of the collecting institution is credited for the value of the deposited checks in accordance with the availability schedules maintained by the Reserve Banks. These schedules reflect the time normally needed for the Reserve Banks to receive payments from the institutions on which the checks are drawn. Credit is usually given on the day of deposit or the next business day. In 2003, the Reserve Banks collected 16 billion checks with a value of $15.8 trillion (table 7.4).

Table 7.4

Number and value of checks collected by the Reserve Banks, selected years, 1920–2003

Number in millions; value in millions of dollars

Year	Number	Value
1920	424	149,784
1930	905	324,883
1940	1,184	280,436
1950	1,955	856,953
1960	3,419	1,154,121
1970	7,158	3,331,733
1980	15,716	8,038,026
1990	18,598	12,519,171
2000	16,994	13,849,084
2003	16,271	15,768,877

NOTE: In 2003, the Reserve Banks, acting as fiscal agents for the United States, also paid 267 million Treasury checks and 198 million postal money orders.

Since it was established, the Federal Reserve has worked with the private sector to improve the efficiency and cost-effectiveness of the check-collection system. Toward that end, the Federal Reserve and the banking industry developed bank routing numbers in the 1940s. These numbers are still printed on checks to identify the institution on which a check is drawn and to which the check must be presented for payment. In the 1950s, the magnetic ink character recognition (MICR) system for encoding pertinent data on checks was developed so that the data could be read electronically. The MICR system contributed significantly to the automation of check processing.

In the 1970s, the Federal Reserve introduced a regional check-processing program to further improve the efficiency of check clearing, which resulted in an increase in the number of check-processing facilities throughout the country. In response to the recent decline in overall check usage, the

Reserve Banks began an initiative to better align Reserve Bank check-processing operations with the changing demand for those services. As part of the initiative, the Reserve Banks standardized check processing, consolidated some operations, and reduced the overall number of their check-processing sites.

Other improvements in check collection have focused on when a customer has access to funds deposited in a bank. Until the late 1980s, depository institutions were not required to make funds from check deposits available for withdrawal within specific time frames. In 1988, the Federal Reserve Board adopted Regulation CC, Availability of Funds and Collection of Checks, which implemented the Expedited Funds Availability Act. Regulation CC established maximum permissible hold periods for checks and other deposits, after which banks must make funds available for withdrawal. It also established rules to speed the return of unpaid checks. In late 1992, the Federal Reserve Board amended Regulation CC to permit all depository institutions to demand settlement in same-day funds from paying banks without paying presentment fees, provided presenting banks meet certain conditions.

Substitute check

In addition to processing paper checks more efficiently, the Federal Reserve has also encouraged check truncation, which improves efficiency by eliminating the need to transfer paper checks physically between institutions. To that end, the Federal Reserve worked with Congress on the Check Clearing for the 21st Century Act, commonly known as Check 21, which be-

came effective October 28, 2004. Check 21 facilitates check truncation by creating a new negotiable instrument called a substitute check, which is the legal equivalent of an original check. A substitute check is a paper reproduction of an original check that contains an image of the front and back of the original check and is suitable for automated processing, just as the original check is. Check 21 allows depository institutions to truncate original checks, process check information electronically, and deliver substitute checks to depository institutions if they require paper checks. In 2004, the Board amended Regulation CC to implement Check 21.

The Automated Clearinghouse

The automated clearinghouse (ACH) is an electronic payment system, developed jointly by the private sector and the Federal Reserve in the early 1970s as a more-efficient alternative to checks. Since then, the ACH has evolved into a nationwide mechanism that processes credit and debit transfers electronically. ACH credit transfers are used to make direct deposit payroll payments and corporate payments to vendors. ACH debit transfers are used by consumers to authorize the payment of insurance premiums, mortgages, loans, and other bills from their account. The ACH is also used by businesses to concentrate funds at a primary bank and to make payments to other businesses. In 2003, the Reserve Banks processed 6.5 billion ACH payments with a value of $16.8 trillion (table 7.5).

Table 7.5

Number and value of ACH transactions processed by the Reserve Banks, selected years, 1975–2003

Number in millions; value in millions of dollars

Year	Number	Value
1975	6	92,868
1980	227	286,600
1990	1,435	4,660,476
2000	4,651	14,024,445
2003	6,502	16,761,883

The use of the ACH has evolved over time. The ACH is now used to make certain payments initiated by telephone or over the Internet. In addition, merchants that receive checks at the point of sale and banks that receive bill-payment checks in the mail are increasingly converting those checks into ACH payments.

In 2001, the Reserve Banks began a cross-border ACH service. Legal and operational differences between countries have presented challenges to the rapid growth of the cross-border service; however, the Reserve Banks

are continuing to work with financial institutions and ACH operators in other nations to address these challenges.

Depository institutions transmit ACH payments to the Reserve Banks in batches, rather than individually. ACH funds transfers are generally processed within one to two days, according to designated schedules, and are delivered to receiving institutions several times a day, as they are processed. The Reserve Banks offer ACH operator services to all depository institutions. A private-sector processor also provides ACH operator services in competition with the Reserve Banks. The Reserve Banks and the private-sector operator deliver ACH payments to participants in each other's system in order to maintain a national ACH payment system.

Both the government and the commercial sectors use ACH payments. Compared with checks, ACH transfers are less costly to process and provide greater certainty of payment to the receiver. Initially, the federal government was the dominant user of the ACH and promoted its use for Social Security and payroll payments. Since the early 1980s, commercial ACH volume has grown rapidly, and in 2003 it accounted for 86 percent of total ACH volume (table 7.6).

Table 7.6

ACH volume by type, selected years 1975–2003

Number in millions

Year	Number of commercial payments	Number of government payments	Commercial payments as a percentage of total (percent)
1975	5.8	.2	97
1980	64.5	162.5	28
1990	915.3	519.5	64
2000	3,812.0	839.0	82
2003	5,588.0	914.0	86

Wholesale Services

Fedwire Funds Service

The Fedwire Funds Service provides a real-time gross settlement system in which more than 9,500 participants are able to initiate electronic funds transfers that are immediate, final, and irrevocable. Depository institutions that maintain an account with a Reserve Bank are eligible to use the service to send payments directly to, or receive payments from, other participants. Depository institutions can also use a correspondent relationship with a Fedwire participant to make or receive transfers indirectly through

the system. Participants generally use Fedwire to handle large-value, time-critical payments, such as payments to settle interbank purchases and sales of federal funds; to purchase, sell, or finance securities transactions; to disburse or repay large loans; and to settle real estate transactions. The Department of the Treasury, other federal agencies, and government-sponsored enterprises also use the Fedwire Funds Service to disburse and collect funds. In 2003, the Reserve Banks processed 123 million Fedwire payments having a total value of $436.7 trillion (table 7.7).

Table 7.7

Number and value of Fedwire funds transactions processed by the Federal Reserve, selected years, 1920–2003

Number in millions; value in millions of dollars

Year	Number	Value
1920	.5	30,857
1930	1.9	198,881
1940	.8	92,106
1950	1.0	509,168
1960	3.0	2,428,083
1970	7.0	12,332,001
1980	43.0	78,594,862
1990	62.6	199,067,200
2000	108.3	379,756,389
2003	123.0	436,706,269

Fedwire funds transfers are processed individually, rather than in batches as ACH transfers are. The Federal Reserve uses secure, sophisticated data-communications and data-processing systems to ensure that each transfer is authorized by the sender and that it is not altered while it is under the control of a Reserve Bank. Although a few depository institutions use the telephone to initiate Fedwire payments, more than 99 percent of all Fedwire funds transfers are initiated electronically. The Federal Reserve processes Fedwire funds transfers in seconds, electronically debiting the account of the sending institution and crediting the account of the receiving institution. The Federal Reserve guarantees the payment, assuming any risk that the institution sending the payment has insufficient funds in its Federal Reserve account to complete the transfer.

Fedwire Securities Service

The Fedwire Securities Service provides safekeeping, transfer, and settlement services for securities issued by the Treasury, federal agencies, gov-

ernment-sponsored enterprises, and certain international organizations. The Reserve Banks perform these services as fiscal agents for these entities. Securities are safekept in the form of electronic records of securities held in custody accounts. Securities are transferred according to instructions provided by parties with access to the system. Access to the Fedwire Securities Service is limited to depository institutions that maintain accounts with a Reserve Bank, and a few other organizations, such as federal agencies, government-sponsored enterprises, and state government treasurer's offices (which are designated by the U.S. Treasury to hold securities accounts). Other parties, specifically brokers and dealers, typically hold and transfer securities through depository institutions that are Fedwire participants and that provide specialized government securities clearing services. In 2003, the Fedwire Securities Service processed 20.4 million securities transfers with a value of $267.6 trillion (table 7.8).

Table 7.8

Number and value of book-entry securities transfers processed by the Federal Reserve, selected years, 1970–2003

Number in millions; value in millions of dollars

Year	Number	Value
1970	.3	258,200
1980	4.1	13,354,100
1990	10.9	99,861,205
2000	13.6	188,133,178
2003	20.4	267,644,194

Fedwire securities are processed individually, in much the same way that Fedwire funds transfers are processed, and participants initiate securities transfers in the same manner, using either a computer connection or the telephone. When the Federal Reserve receives a request to transfer a security, for example as a result of the sale of securities, it determines that the security is held in safekeeping for the institution requesting the transfer and withdraws the security from the institution's safekeeping account. It then electronically credits the proceeds of the sale to the account of the depository institution, deposits the book-entry security into the safekeeping account of the receiving institution, and electronically debits that institution's account for the purchase price. Most securities transfers involve the delivery of securities and the simultaneous exchange of payment, which is referred to as delivery versus payment. The transfer of securities ownership and related funds is final at the time of transfer, and the Federal Reserve guarantees payment to institutions that initiate such securities transfers.

National Settlement Service

The National Settlement Service allows participants in private-sector clearing arrangements to do multilateral funds settlements on a net basis using balances in their Federal Reserve accounts. The service provides an automated mechanism for submitting settlement information to the Reserve Banks. It improves operational efficiency and controls for this process and reduces settlement risk to participants by granting settlement finality for movements of funds on settlement day. The service also enables the Federal Reserve to manage and limit the financial risk posed by these arrangements because it incorporates risk controls that are as stringent as those used in the Fedwire Funds Service. Approximately seventy arrangements use the National Settlement Service—primarily check clearinghouse associations, but also other types of arrangements.

Fiscal Agency Services

As fiscal agents of the United States, the Reserve Banks function as the U.S. government's bank.

As fiscal agents of the United States, the Reserve Banks function as the U.S. government's bank and perform a variety of services for the Treasury, other government agencies, government-sponsored enterprises, and some international organizations. Often the fiscal agent services performed by the Reserve Banks are the same, or similar to, services that the Reserve Banks provide to the banking system. Services performed for the Treasury include maintaining the Treasury's bank account; processing payments; and issuing, safekeeping, and transferring securities. Fiscal services performed for other entities are generally securities-related. The Treasury and other entities reimburse the Reserve Banks for the expenses incurred in providing these services.

One of the unique fiscal agency functions that the Reserve Banks provide to the Treasury is a program through which the Reserve Banks invest Treasury monies until needed to fund the government's operations. The Treasury receives funds from two principal sources: tax receipts and borrowings. The funds that flow into and out of the government's account vary in amount throughout the year; for example, the account balance tends to be relatively high during the April tax season. The Treasury directs the Reserve Banks to invest funds in excess of a previously agreed-upon minimum amount in special collateralized accounts at depository institutions nationwide. The Federal Reserve monitors these balances for compliance with collateral requirements and returns the funds to the Treasury when they are needed.

This investment facility, in which excess funds are invested in accounts at depository institutions, also facilitates the implementation of monetary policy. When funds flow from depository institutions into the Treasury's

account at the Federal Reserve, the supply of Federal Reserve balances to depository institutions decreases. The reverse occurs when funds flow from the Treasury's Federal Reserve account to the Treasury's accounts at depository institutions. A stable balance in the Treasury's account at the Federal Reserve mitigates the effect of Treasury's receipts and disbursements on the supply of Federal Reserve balances to depository institutions.

The Reserve Banks make disbursements from the government's account through Fedwire funds transfers or ACH payments, or to a limited extent, by check. Fedwire disbursements are typically associated with, but not limited to, the redemption of Treasury securities. Certain recurring transactions, such as Social Security benefit payments and government employee salary payments, are processed mainly by the ACH and electronically deposited directly to the recipients' accounts at their depository institutions. Other government payments may be made using Treasury checks drawn on the government's account at the Reserve Banks. The Treasury continues to work to move the remaining government payments away from Treasury checks toward electronic payments, primarily the ACH, in an effort to improve efficiency and reduce the costs associated with government payments.

The Federal Reserve plays an important role when the Treasury needs to raise money to finance the government or to refinance maturing Treasury securities. The Reserve Banks handle weekly, monthly, and quarterly auctions of Treasury securities, accepting bids, communicating them to the Treasury, issuing the securities in book-entry form to the winning bidders, and collecting payment for the securities. Over the past several years, the auction process has become increasingly automated, which further ensures a smooth borrowing process. For example, automation has reduced to only minutes the time between the close of bidding and the announcement of the results of a Treasury securities auction.

Treasury securities are maintained in book-entry form in either the Reserve Banks' Fedwire Securities Service or the Treasury's TreasuryDirect system, which is also operated by the Reserve Banks. Even though TreasuryDirect holds less than 2 percent of all outstanding Treasury securities, it provides a convenient way for individuals to hold their securities directly, rather than with a third party such as a depository institution. Individuals purchase Treasury securities either directly from the Treasury when they are issued or on the secondary market, and they instruct their broker that the securities be delivered to their TreasuryDirect account. Once the securities are deposited there, the ACH directly deposits any interest or principal payments owed to the account holder to the account holder's account at a depository institution. A Reserve Bank, if requested, will sell securities held in TreasuryDirect for a fee on the secondary market, even though this is a service intended for individuals who hold Treasury securities to maturity.

The Federal Reserve also provides support for the Treasury's savings bonds program. Although savings bonds represent less than 5 percent of the federal debt, they are a means for individuals to invest in government securities with a small initial investment, currently $25. The Reserve Banks issue, service, and redeem tens of millions of U.S. savings bonds each year on behalf of the Treasury. As authorized by the Treasury, the Reserve Banks also qualify depository institutions and corporations to serve as issuing agents and paying agents for savings bonds.[3]

International Services

As the central bank of the United States, the Federal Reserve performs services for foreign central banks and for international organizations such as the International Monetary Fund and the International Bank for Reconstruction and Development. The Reserve Banks provide several types of services to these organizations, including maintaining non-interest-bearing deposit accounts (in U.S. dollars), securities safekeeping accounts, and accounts for safekeeping gold. Some foreign official institutions direct a portion of their daily receipts and payments in U.S. dollars through their funds accounts at the Federal Reserve. If an account contains excess funds, the foreign official institution may request that these funds be invested overnight in repurchase agreements with the Reserve Banks. If investments are needed for longer periods, the foreign official institution may provide instructions to buy securities to be held in safekeeping. Conversely, the foreign institution may provide instructions to sell securities held in safekeeping, with the proceeds deposited in its account. The Reserve Banks charge foreign official institutions for these services.

Gold vault, Federal Reserve Bank of New York

Federal Reserve Intraday Credit Policy

Each day, the Reserve Banks process a large number of payment transactions resulting from the Banks' role in providing payment services to depository institutions. Because depository institutions in the aggregate generally hold a relatively small amount of funds overnight in their Reserve Bank accounts, the Reserve Banks extend intraday credit, commonly referred to as daylight credit or daylight-overdraft credit, to facilitate the settlement of payment transactions and to ensure the smooth functioning of the U.S. payments system. To address the risk of providing this credit, the Federal Reserve has developed a policy that balances the goals of ensuring smooth functioning of the payments system and managing the Federal Reserve's direct credit risk from institutions' use of Federal Reserve intraday credit.

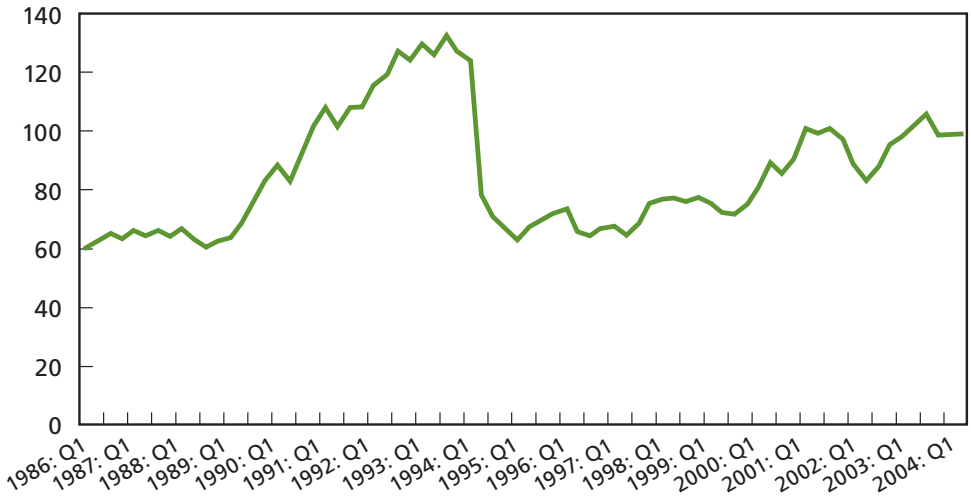
3. Savings bonds are now available in book-entry form from the Treasury, through www.TreasuryDirect.gov.

Institutions incur daylight overdrafts in their Reserve Bank accounts because of the mismatch in timing between the settlement of payments owed and the settlement of payments due. The Federal Reserve uses a schedule of rules, referred to as daylight-overdraft posting rules, to determine whether a daylight overdraft has occurred in an institution's account. The daylight-overdraft posting rules define the time of day that debits and credits for transactions processed by the Reserve Banks will be posted to an institution's account. The Federal Reserve relies on an automated system to measure an institution's intraday account activity, to monitor its compliance with the Federal Reserve's policy, and to calculate the institution's daylight-overdraft charges. The Reserve Banks' daylight-overdraft exposure can be significant. For example, in 2003 daylight overdrafts across depository institutions peaked at levels over $100 billion per day (chart 7.2).

Chart 7.2

Average peak daylight overdrafts of depository institutions, 1986:Q1–2004:Q2

Billions of dollars



NOTE: The Federal Reserve measures each depository institution's account balance at the end of each minute during the business day. An institution's peak daylight overdraft for a given day is its largest negative end-of-minute balance. The System peak daylight overdraft for a given day is determined by adding the negative account balances of all depository institutions at the end of each minute and then selecting the largest negative end-of-minute balance. The quarterly average peak is the sum of daily System peaks for a quarter divided by the number of days in that quarter.

The Federal Reserve's policy establishes various measures to control the risks associated with daylight overdrafts. Beginning in 1985, the policy set a maximum limit, or net debit cap, on depository institutions' daylight-overdraft positions. In order to adopt a net debit cap greater than zero, an institution must be in sound financial condition. Certain institutions may

be eligible to obtain additional daylight-overdraft capacity above their net debit caps by pledging collateral, subject to Reserve Bank approval. Institutions must have regular access to the Federal Reserve's discount window so that they can borrow overnight from their Reserve Bank to cover any daylight overdrafts that are not eliminated before the end of the day. Those that lack regular access to the discount window are prohibited from incurring daylight overdrafts in their Reserve Bank accounts and are subject to additional risk controls. Beginning in 1994, the Reserve Banks also began charging fees to depository institutions for their use of daylight overdrafts as an economic incentive to reduce the overdrafts, thereby reducing direct Federal Reserve credit risk and contributing to economic efficiency.

Federal Reserve policy allows Reserve Banks to apply additional risk controls to an account holder's payment activity, if necessary to limit risk. These risk controls include unilaterally reducing an account holder's net debit cap, placing real-time controls on the account holder's payment activity so that requested payments are rejected, or requiring the account holder to pledge collateral to cover its daylight overdrafts.

A Appendix: Federal Reserve Regulations

A **Extensions of Credit by Federal Reserve Banks**
Governs borrowing by depository institutions and others at the Federal Reserve discount window

B **Equal Credit Opportunity**
Prohibits lenders from discriminating against credit applicants, establishes guidelines for gathering and evaluating credit information, and requires written notification when credit is denied

C **Home Mortgage Disclosure**
Requires certain mortgage lenders to disclose data regarding their lending patterns

D **Reserve Requirements of Depository Institutions**
Sets uniform requirements for all depository institutions to maintain reserves either with their Federal Reserve Bank or as cash in their vaults

E **Electronic Funds Transfers**
Establishes the rights, liabilities, and responsibilities of parties in electronic funds transfers and protects consumers when they use such systems

F **Limitations on Interbank Liabilities**
Prescribes standards to limit the risks that the failure of a depository institution would pose to an insured depository institution

G **Disclosure and Reporting of CRA-Related Agreements**
Implements provisions of the Gramm-Leach-Bliley Act that require reporting and public disclosure of written agreements between (1) insured depository institutions or their affiliates and (2) nongovernmental entities or persons, made in connection with fulfillment of Community Reinvestment Act requirements

H **Membership of State Banking Institutions in the Federal Reserve System**
Defines the requirements for membership of state-chartered banks in the Federal Reserve System; sets limitations on certain investments and requirements for certain types of loans; describes rules pertaining to securities-related activities; establishes the minimum ratios of capital to assets that banks must maintain and procedures

for prompt corrective action when banks are not adequately capitalized; prescribes real estate lending and appraisal standards; sets out requirements concerning bank security procedures, suspicious-activity reports, and compliance with the Bank Secrecy Act; and establishes rules governing banks' ownership or control of financial subsidiaries

I Issue and Cancellation of Capital Stock of Federal Reserve Banks
Sets out stock-subscription requirements for all banks joining the Federal Reserve System

J Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers through Fedwire
Establishes procedures, duties, and responsibilities among (1) Federal Reserve Banks, (2) the senders and payors of checks and other items, and (3) the senders and recipients of Fedwire funds transfers

K International Banking Operations
Governs the international banking operations of U.S. banking organizations and the operations of foreign banks in the United States

L Management Official Interlocks
Generally prohibits a management official from serving two nonaffiliated depository institutions, depository institution holding companies, or any combination thereof, in situations where the management interlock would likely have an anticompetitive effect

M Consumer Leasing
Implements the consumer leasing provisions of the Truth in Lending Act by requiring meaningful disclosure of leasing terms

N Relations with Foreign Banks and Bankers
Governs relationships and transactions between Federal Reserve Banks and foreign banks, bankers, or governments

O Loans to Executive Officers, Directors, and Principal Shareholders of Member Banks
Restricts credit that a member bank may extend to its executive officers, directors, and principal shareholders and their related interests

P Privacy of Consumer Financial Information
Governs how financial institutions use nonpublic personal information about consumers

Q **Prohibition against Payment of Interest on Demand Deposits**
Prohibits member banks from paying interest on demand deposits

S **Reimbursement to Financial Institutions for Assembling or Providing Financial Records; Recordkeeping Requirements for Certain Financial Records**
Establishes rates and conditions for reimbursement to financial institutions for providing customer records to a government authority and prescribes recordkeeping and reporting requirements for insured depository institutions making domestic wire transfers and for insured depository institutions and nonbank financial institutions making international wire transfers

T **Credit by Brokers and Dealers**
Governs extension of credit by securities brokers and dealers, including all members of national securities exchanges (See also Regulations U and X.)

U **Credit by Banks and Persons Other Than Brokers and Dealers for the Purpose of Purchasing or Carrying Margin Stock**
Governs extension of credit by banks or persons other than brokers or dealers to finance the purchase or the carrying of margin securities (See also Regulations T and X.)

V **Fair Credit Reporting**
Implements the provisions of the Fair Credit Reporting Act applicable to financial institutions regarding obtaining and using consumer reports and other information about consumers, sharing such information among affiliates, furnishing information to consumer reporting agencies, and preventing identity theft

W **Transactions Between Member Banks and Their Affiliates**
Implements sections 23A and 23B of the Federal Reserve Act, which establish certain restrictions on and requirements for transactions between a member bank and its affiliates

X **Borrowers of Securities Credit**
Applies the provisions of Regulations T and U to borrowers who are subject to U.S. laws and who obtain credit within or outside the United States for the purpose of purchasing securities

Y **Bank Holding Companies and Change in Bank Control**
Regulates the acquisition of control of banks and bank holding companies by companies and individuals, defines and regulates the nonbanking activities in which bank holding companies (includ-

ing financial holding companies) and foreign banking organizations with United States operations may engage, and establishes the minimum ratios of capital to assets that bank holding companies must maintain

Z **Truth in Lending**
Prescribes uniform methods for computing the cost of credit, for disclosing credit terms, and for resolving errors on certain types of credit accounts

AA **Unfair or Deceptive Acts or Practices**
Establishes consumer complaint procedures and defines unfair or deceptive practices in extending credit to consumers

BB **Community Reinvestment**
Implements the Community Reinvestment Act and encourages banks to help meet the credit needs of their entire communities

CC **Availability of Funds and Collection of Checks**
Governs the availability of funds deposited in checking accounts and the collection and return of checks

DD **Truth in Savings**
Requires depository institutions to provide disclosures to enable consumers to make meaningful comparisons of deposit accounts

EE **Netting Eligibility for Financial Institutions**
Defines financial institutions to be covered by statutory provisions that validate netting contracts, thereby permitting one institution to pay or receive the net, rather than the gross, amount due, even if the other institution is insolvent

B Appendix: Glossary of Terms

This glossary gives basic definitions of terms used in the text. Readers looking for more comprehensive explanations may want to consult textbooks in economics, banking, and finance.

A

agreement corporation
Corporation chartered by a state to engage in international banking; so named because the corporation enters into an "agreement" with the Board of Governors to limit its activities to those permitted an Edge Act corporation. Typically organized as a subsidiary of a bank, an agreement corporation may conduct activities abroad that are permissible to foreign banks abroad but that may not otherwise be permissible for U.S. banks.

automated clearinghouse (ACH)
Electronic clearing and settlement system for exchanging electronic credit and debit transactions among participating depository institutions. The Federal Reserve Banks operate an automated clearinghouse, as do private organizations.

B

balances
See **Federal Reserve balances**.

Bank for International Settlements (BIS)
International organization established in 1930 and based in Basel, Switzerland, that serves as a forum for central banks for collecting information, developing analyses, and cooperating on a wide range of policy-related matters; also provides certain financial services to central banks.

bank holding company
Company that owns, or has controlling interest in, one or more banks. The Board of Governors is responsible for regulating and supervising bank holding companies, even if the bank owned by the holding company is under the primary supervision of a different federal agency (the Comptroller of the Currency or the Federal Deposit Insurance Corporation).

Bank Holding Company Act of 1956
Federal legislation that establishes the legal framework under which bank

holding companies operate and places the formation of bank holding companies and their acquisition of banking and nonbanking interests under the supervision of the Federal Reserve.

banking organization
A bank holding company (consolidated to include all of its subsidiary banks and nonbank subsidiaries) or an independent bank (a bank that is not owned or controlled by a bank holding company).

bank regulation
Actions to make and issue rules and regulations and enforce those rules and other laws governing the structure and conduct of banking.

bank supervision
Oversight of individual banks to ensure that they are operated prudently and in accordance with applicable statutes and regulations.

Basel Committee on Banking Supervision
An international committee of bank supervisors, associated with the BIS, that is headquartered in Basel, Switzerland, and is composed of bank supervisors from Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Spain, Sweden, Switzerland, the United Kingdom, and the United States.

Basel I
Informal name for the 1988 agreement—the International Convergence of Capital Measurement and Capital Standards—under which national bank supervisors for the first time agreed on an international framework for capital adequacy guidelines. Also known as the Basel Accord.

Basel II
Informal name for the 2004 agreement updating the Basel Accord. Also known as the New Basel Accord, Basel II has three pillars: minimum capital requirements, supervisory oversight, and market discipline.

Board of Governors
Central, governmental agency of the Federal Reserve System, located in Washington, D.C., and composed of seven members, who are appointed by the President and confirmed by the Senate. The Board, with other components of the System, has responsibilities associated with the conduct of monetary policy, the supervision and regulation of certain banking organizations, the operation of much of the nation's payments system, and the administration of many federal laws that protect consumers in credit transactions. The Board also supervises the Federal Reserve Banks.

book-entry securities
Securities that are recorded in electronic records, called book entries, rather than as paper certificates. (*Compare* **definitive securities**.)

C

Call Report
Informal name for quarterly Reports of Condition and Income.

capital
In banking, the funds invested in a bank that are available to absorb loan losses or other problems and therefore protect depositors. Capital includes all equity and some types of debt. Bank regulators have developed two definitions of capital for supervisory purposes: tier 1 capital, which can absorb losses while a bank continues operating, and tier 2 capital, which may be of limited life and may carry an interest obligation or other characteristics of a debt obligation, and therefore provides less protection to depositors than tier 1 capital.

capital market
The market in which corporate equity and longer-term debt securities (those maturing in more than one year) are issued and traded. (*Compare* **money market**.)

cash
U.S. paper currency plus coin.

central bank
Principal monetary authority of a nation, which performs several key functions, including conducting monetary policy to stabilize the economy and level of prices. The Federal Reserve is the central bank of the United States.

check clearing
The movement of a check from the depository institution at which it was deposited back to the institution on which it was written, the movement of funds in the opposite direction, and the corresponding credit and debit to the accounts involved. Check clearing also encompasses the return of a check (for insufficient funds, for example) from the bank on which it was written to the bank at which it was deposited, and the corresponding movement of funds. The Federal Reserve Banks operate a nationwide check-clearing system.

check truncation
The practice of removing an original paper check from the check-clearing process and sending in its place an alternative paper or electronic version of the essential information on the check.

clearing
General term that may refer to check clearing or to the process of matching trades between the sellers and buyers of securities and other financial instruments and contracts.

commercial bank
Bank that offers a variety of deposit accounts, including checking, savings, and time deposits, and extends loans to individuals and businesses. Commercial banks can be contrasted with investment banking firms, which generally are involved in arranging for the sale of corporate or municipal securities, and broker-dealer firms, which buy and sell securities for themselves and others. (*Compare* **savings bank**.)

commercial paper
Short-term, unsecured promissory note issued by an industrial or commercial firm, a financial company, or a foreign government.

Consumer Advisory Council
Group, created under the Federal Reserve Act, composed of thirty members who represent the interests of a broad range of consumers and creditors. The council meets with the Board of Governors three times a year on matters concerning consumers and the consumer protection laws administered by the Board.

corporate bond
Interest-bearing or discounted debt obligation issued by a private corporation.

contractual clearing balance
An amount a depository institution may contract to maintain in its account at a Federal Reserve Bank in addition to any reserve balance requirement. This amount helps ensure that the institution can meet its daily transaction obligations without overdrawing its account. Balances maintained to satisfy the contractual clearing balance earn credits that can be used to pay for services provided by the Federal Reserve Banks.

correspondent bank
Bank that accepts the deposits of, and performs services for, another bank (called a respondent bank).

credit risk
The risk that economic loss will result from the failure of an obligor to repay financial institutions according to the terms and conditions of a contract or agreement.

credit union
Financial cooperative organization whose membership consists of individuals who have a common bond, such as place of employment or residence or membership in a labor union. Credit unions accept deposits from members, pay interest (in the form of dividends) on the deposits out of earnings, and use their funds mainly to provide consumer installment loans to members.

currency
Paper money that consists mainly of Federal Reserve notes. Other types of currency that were once issued by the United States include silver certificates, United States notes, and national bank notes.

D

daylight overdraft
A negative balance in an institution's Federal Reserve Bank account at any time during the operating hours of the Fedwire Funds Service.

daylight-overdraft posting rules
A schedule used to determine the timing of debits and credits to an institution's Federal Reserve Bank account for various transactions processed by the Reserve Banks.

definitive securities
Securities that are recorded on engraved paper certificates and payable to the bearers or to specific, registered owners. (*Compare* **book-entry securities**.)

demand deposit
A deposit that the depositor has a right to withdraw at any time without prior notice to the depository institution. By law, no interest can be paid on such deposits. Demand deposits are commonly offered in the form of checking accounts.

depository institution
Financial institution that makes loans and obtains its funds mainly through accepting deposits from the public; includes commercial banks, savings and loan associations, savings banks, and credit unions.

derivative
A financial instrument whose value depends upon the characteristics and value of an underlying commodity, currency, or security.

discounting
Practice of extending credit in which the borrower endorses a negotiable instrument or other commercial paper in the borrower's portfolio over to the lender in exchange for funds from the lender in the amount of the instrument's face value less the interest due over the term of the loan, that is, the "discounted" value.

discount rate
Officially the primary credit rate, it is the interest rate at which an eligible depository institution may borrow funds, typically for a short period, directly from a Federal Reserve Bank. The law requires that the board of directors of each Reserve Bank establish the discount rate every fourteen days, subject to review and determination by the Board of Governors.

discount window (the window)
Figurative expression for the Federal Reserve facility that extends credit directly to eligible depository institutions (those subject to reserve requirements); so named because, in the early days of the Federal Reserve System, bankers would come to a Reserve Bank teller window to obtain credit.

discount window credit
Credit extended by a Federal Reserve Bank to an eligible depository institution. All discount window borrowing must be secured by collateral. Three types of discount window credit are available to eligible depository institutions:

- **primary credit**
  Credit extended to generally sound depository institutions at a rate above the target federal funds rate on a very short-term basis as a backup source of funding.
- **seasonal credit**
  Credit extended by a Federal Reserve Bank to depository institutions that have difficulty raising funds in national money markets to help meet temporary needs for funds resulting from regular, seasonal fluctuations in loans and deposits. The interest rate charged is based on market rates.
- **secondary credit**
  Credit extended to depository institutions ineligible for primary credit, at a rate above the primary credit rate, either on a very short-term basis (when consistent with a timely return to market sources of funds) or for a longer term (to facilitate the orderly resolution of serious financial difficulties).

E

easing
Federal Reserve action to lower the federal funds rate. The action is undertaken when economic activity needs to be stimulated. (*Compare* **tightening**.)

Edge Act corporation (or Edge corporation)
Corporation chartered by the Federal Reserve to engage in international banking. The Board of Governors acts on applications to establish Edge Act corporations and also examines the corporations and their subsidiaries. Typically organized as a subsidiary of a bank, an Edge Act corporation may conduct activities abroad that are permissible to foreign banks abroad but that may not otherwise be permissible to U.S. banks. Named after Senator Walter Edge of New Jersey, who sponsored the original legislation to permit formation of such organizations. (*Compare* **agreement corporation**.)

elastic currency
Currency that can, by the actions of the central monetary authority, expand or contract in amount warranted by economic conditions.

electronic funds transfer (EFT)
Transfer of funds electronically rather than by check or cash. The Federal Reserve's Fedwire Funds Service and automated clearinghouse services are EFT systems. (EFTs subject to the Electronic Funds Transfer Act are more narrowly defined.)

Eurocurrency liabilities
A generic term referring to liabilities in a bank located in a country other than the one that issues the currency in which the liability is denominated. Despite its name, Eurocurrency need not be a liability of a European banking office nor denominated in European currency. Not to be confused with the euro, the name of the common currency of twelve (as of 2004) European Union countries.

Eurodollar deposits
Dollar-denominated deposits in banks and other financial institutions outside the United States; includes deposits at banks not only in Europe, but in all parts of the world.

excess reserves
Amount of funds held by an institution in its account at a Federal Reserve Bank in excess of its required reserve balance and its contractual clearing balance.

F

Federal Advisory Council
Advisory group made up of one representative (in most cases a banker) from each of the twelve Federal Reserve Districts. Established by the Federal Reserve Act, the council meets periodically with the Board of Governors to discuss business and financial conditions and to make recommendations.

federal agency securities
Interest-bearing obligations issued by federal agencies and government-sponsored entities, such as the Federal Home Loan Banks, the Federal Farm Credit Banks, the Federal National Mortgage Association (Fannie Mae), the Federal Home Loan Mortgage Corporation (Freddie Mac), and the Tennessee Valley Authority. Some federal agency securities are backed by the U.S. government while others are not.

Federal Financial Institutions Examination Council (FFIEC)
Group of representatives of the federal banking regulatory agencies—the Board of Governors, the Office of Thrift Supervision, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the National Credit Union Administration—established to help maintain uniform standards for examining and supervising federally insured depository institutions.

federal funds transactions
Short-term transactions in immediately available funds—between depository institutions and certain other institutions that maintain accounts with the Federal Reserve—that involve lending balances at the Federal Reserve; usually not collateralized.

federal funds rate
Rate charged by a depository institution on an overnight loan of federal funds to another depository institution; rate may vary from day to day and from bank to bank.

Federal Open Market Committee (FOMC, or the Committee)
Twelve-voting-member committee made up of the seven members of the Board of Governors; the president of the Federal Reserve Bank of New York; and, on a rotating basis, the presidents of four other Reserve Banks. Nonvoting Reserve Bank presidents also participate in Committee deliberations and discussion. The FOMC generally meets eight times a year in Washington, D.C., to set the nation's monetary policy. It also establishes policy relating to System operations in the foreign exchange markets.

Federal Reserve Act
Federal legislation, enacted in 1913, that established the Federal Reserve System.

Federal Reserve balances
The amount of funds held by a depository institution in its account at its Federal Reserve Bank.

Federal Reserve Bank
One of the twelve operating arms of the Federal Reserve System, located throughout the nation, that together with their Branches carry out various System functions, including providing payment services to depository institutions, distributing the nation's currency and coin, supervising and regulating member banks and bank holding companies, and serving as fiscal agent for the U.S. government.

Federal Reserve District (Reserve District, or District)
One of the twelve geographic regions served by a Federal Reserve Bank.

Federal Reserve float
Float is credit that appears on the books of the depository institution of both the check writer (the payor) and the check receiver (the payee) while a check is being processed. Federal Reserve float is float present during the Federal Reserve Banks' check-clearing process. To promote efficiency in the payments system and provide certainty about the date that deposited funds will become available to the receiving depository institution (and the payee), the Federal Reserve Banks credit the accounts of banks that deposit checks according to a fixed schedule. However, processing certain checks and collecting funds from the banks on which these checks are written may take more time than the schedule allows. Therefore, the accounts of some banks may be credited before the Federal Reserve Banks are able to collect payment from other banks, resulting in Federal Reserve float.

Federal Reserve note
Paper currency issued by the Federal Reserve Banks. Nearly all the nation's circulating currency is in the form of Federal Reserve notes, which are printed by the Bureau of Engraving and Printing, a bureau of the U.S. Department of the Treasury. Federal Reserve notes are obligations of the Federal Reserve Banks and legal tender for all debts.

Federal Reserve Regulatory Service
Monthly subscription service that includes all statutes and regulations for which the Federal Reserve has responsibility, Board of Governors interpretations and rulings, official staff commentaries, significant staff opinions, and procedural rules under which the Board operates.

Federal Reserve System
The central bank of the United States, created by the Federal Reserve Act and made up of a seven-member Board of Governors in Washington, D.C., twelve regional Federal Reserve Banks, and Branches of the Federal Reserve Banks.

Fedwire Funds Service
Electronic funds transfer network operated by the Federal Reserve Banks. It is usually used to transfer large amounts of funds from one institution's account at the Federal Reserve to another institution's account. It is also used by the U.S. Department of the Treasury, other federal agencies, and government-sponsored enterprises to collect and disburse funds.

Fedwire Securities Service
Electronic vault that stores records of book-entry securities holdings and a transfer and settlement mechanism used by depository institutions to transfer custody of book-entry securities from one depository institution to another. The securities on the Fedwire Securities Service include U.S. Treasury securities, U.S. agency securities, mortgage-backed securities issued by government-sponsored enterprises, and securities of certain international organizations.

financial holding company
A bank holding company that has met the capital, managerial, and other requirements to take advantage of the expanded affiliations allowed under the Gramm-Leach-Bliley Act.

financial institution
Institution that uses its funds chiefly to purchase financial assets, such as loans or securities (as opposed to tangible assets, such as real estate). Financial institutions can be separated into two major groups according to the nature of the principal claims they issue: (1) depository institutions (also called depository intermediaries), such as commercial banks, savings and loan associations, savings banks, and credit unions, which obtain funds largely by accepting deposits from the public and (2) nondepositories (sometimes called nondepository intermediaries), such as life insurance and property–casualty insurance companies and pension funds, whose claims are the policies they sell or their promise to provide income after retirement.

fiscal agency services
Services performed by the Federal Reserve Banks for the U.S. government and other organizations, including maintaining accounts for the U.S. Department of the Treasury, paying checks and making electronic payments on behalf of the Treasury, and selling and redeeming marketable Treasury securities and savings bonds.

fiscal policy
Federal government policy regarding taxation and spending, set by Congress and the President.

flexible exchange rates
Arrangements in which the rate of exchange between countries' currencies (the foreign exchange rate) is allowed to fluctuate in response to market forces of supply and demand.

foreign currency operations
Transactions in the foreign exchange markets involving the purchase of the currency of one nation with that of another. Also called foreign exchange transactions.

foreign exchange intervention
A foreign currency operation (*see* above) designed to influence the value of the dollar against foreign currencies, typically with the aim of stabilizing disorderly markets.

foreign exchange markets
Markets in which foreign currencies are purchased and sold.

foreign exchange rate
Price of the currency of one nation in terms of the currency of another nation.

G

government securities
Securities issued by the U.S. Treasury or federal agencies.

Gramm-Leach-Bliley Act
Federal legislation that allowed affiliations among banks, securities firms, and insurance companies under a financial holding company structure. The act reaffirmed the Federal Reserve's role as "umbrella supervisor" over organizations that control banks, while also requiring that bank regulators and functional regulators supervise subsidiaries within a financial holding company.

gross domestic product (GDP)
Total value of goods and services produced by labor and property located in the United States during a specific period.

Group of Seven (G-7)
International group made up of seven leading industrial nations—Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States—whose finance ministers and central bank governors meet occasionally to discuss economic policy.

I

interest-rate risk
Risk of gain or loss in the value of a portfolio as a result of changes in market interest rates.

international banking facility
Specially designated activities of a bank located in the United States that are treated as those of an offshore bank by U.S. regulatory authorities. Dollar deposits in such a facility are considered to be Eurodollars.

International Monetary Fund (IMF)
International organization established for lending funds to member nations to promote international monetary cooperation among nations, to facilitate the expansion and balanced growth of international trade, and to finance temporary balance-of-payments deficits, usually in conjunction with macroeconomic adjustment programs.

L

liquidity
Quality that makes an asset easily convertible into cash with relatively little loss of value in the conversion process. Sometimes used more broadly to encompass cash and credit in hand and promises of credit to meet needs for cash.

liquidity risk
In banking, the risk that a depository institution will not have sufficient cash or liquid assets to meet the claims of depositors and other creditors.

M

M1
Measure of the U.S. money stock that consists of currency held by the public, traveler's checks, demand deposits, and other checkable deposits.

M2
Measure of the U.S. money stock that consists of M1, savings deposits (including money market deposit accounts), time deposits in amounts of less than $100,000, and balances in retail money market mutual funds. Excludes individual retirement account (IRA) and Keough balances at depository institutions and retail money funds.

M3
Measure of the U.S. money stock that consists of M2, time deposits of $100,000 or more at all depository institutions, repurchase agreements in amounts of $100,000 or more, Eurodollars, and balances held in institutional money market mutual funds.

margin requirement
Buying on margin refers to buying stocks or securities with borrowed money (usually borrowed from a brokerage firm or bank). The margin requirement is the minimum amount (expressed as a percentage) the buyer must put up (rather than borrow). The Federal Reserve Board sets margin requirements.

market interest rates
Rates of interest determined by the interaction of the supply of and demand for funds in freely functioning markets.

market risk
The risk that a banking organization may incur losses due to the change in market value of an asset or liability on its balance sheet.

member bank
Depository institution that is a member of the Federal Reserve System. All national banks are automatically members of the System; state-chartered banks may choose to apply to join the System.

monetary aggregates
Aggregate measures through which the Federal Reserve monitors the nation's monetary assets: M1, M2, and M3.

monetary policy
A central bank's actions to influence the availability and cost of money and credit, as a means of helping to promote national economic goals. Tools of monetary policy include open market operations, direct lending to depository institutions, and reserve requirements.

monetize
Action in which a central bank purchases an object that is not money (for example, gold) and pays for it by creating balances at the central bank. The action permits an increase in the money stock.

money
Anything that serves as a generally accepted medium of exchange, a standard of value, and a means of saving or storing purchasing power. In the United States, currency (the bulk of which is Federal Reserve notes) and coin as well as funds in deposit accounts at depository institutions are examples of money.

money market
Figurative expression for the informal network of dealers and investors over which short-term debt securities are purchased and sold. Money market securities generally are highly liquid securities that mature in less than one year, often less than ninety days. (*Compare* **capital market**.)

money stock
Total quantity of money available for transactions and investment; measures of the U.S. money stock include M1, M2, and M3. (Also referred to as the money supply or, simply, money.)

mutual savings bank
Savings bank owned by its depositors (contrasted with a stock savings bank, which issues common stock to the public).

N

national bank
A commercial bank that is chartered by the Office of the Comptroller of the Currency, which is a bureau of the U.S. Department of the Treasury; by law, national banks are members of the Federal Reserve System.

net debit cap
The maximum uncollateralized daylight-overdraft position that a depository institution is permitted to incur in its Federal Reserve Bank account at any point in the day, or on average over a two-week period.

nominal interest rates
Current stated rates of interest paid or earned. (*Compare* **real interest rates**.)

nonmember bank
State-chartered commercial bank that is not a member of the Federal Reserve System.

nonpersonal time deposit
Time deposit held by a depositor other than an individual (for example, a corporation).

O

official foreign exchange reserves
Assets denominated in foreign currencies held by a country's monetary authorities (in the United States, held by the Federal Reserve System and the Treasury Department).

open market
Freely competitive market.

open market operations
Purchases and sales of securities, typically U.S. Treasury securities, in the open market, by the Open Market Trading Desk at the Federal Reserve Bank of New York as directed by the Federal Open Market Committee, to influence interest rates. Purchases increase the supply of Federal Reserve balances to depository institutions; sales do the opposite.

outright transaction
"Permanent" purchase or sale of securities in the open market, or the redemption of securities, by the Federal Reserve to adjust the supply of balances at the Federal Reserve Banks over the long term. (Contrasts with transactions intended to adjust the supply of balances only temporarily. *See* **repurchase agreement** *and* **reverse repurchase agreement**.)

over the counter
Figurative term for the means of trading securities that are not listed on an organized stock exchange such as the New York Stock Exchange. Over-the-counter trading is done by broker-dealers who communicate by telephone and computer networks.

P

paper
General term for short-term debt instruments such as commercial paper.

payments system
Collective term for mechanisms (both paper-based and electronic) for moving funds, payments, and money among financial institutions throughout the nation. The Federal Reserve plays a major role in the nation's payments system through distribution of currency and coin, pro-

cessing of checks, and electronic transfer of funds; various private organizations also perform payments system functions.

portfolio
Collection of loans or assets, classified by type of borrower or asset. For example, a bank's portfolio might include loans, investment securities, and assets managed in trust; the loan portfolio might include commercial, mortgage, and consumer installment loans.

presentment fee
Fee that a bank receiving a check imposes on the bank collecting payment.

prompt corrective action
Supervisory framework, created under the Federal Deposit Insurance Corporation Improvement Act of 1991, that links enforcement actions closely to the level of capital held by banks.

R

real interest rates
Interest rates adjusted for the expected erosion of purchasing power resulting from inflation. Technically defined as nominal interest rates minus the expected rate of inflation. (*Compare* **nominal interest rates**.)

reciprocal currency (swap) arrangements
Short-term reciprocal arrangements between a Federal Reserve Bank and individual foreign central banks. By drawing on a swap the foreign central bank obtains dollars that can be used to conduct foreign exchange intervention in support of its currency or to lend to its domestic banking system to satisfy temporary liquidity demands. For the duration of the swap, the Federal Reserve Bank obtains an equivalent amount of foreign currency along with a commitment from the foreign central bank to repurchase the foreign currency at a preset exchange rate.

Reports of Condition and Income
Quarterly financial report that all banks, savings and loan associations, Edge and agreement corporations, and certain other types of organizations must file with a federal regulatory agency. Informally called a Call Report.

repurchase agreement (RP or repo)
A transaction in which the Federal Reserve enters into an agreement with a primary dealer to acquire securities from the dealer for a specified

principal amount at an agreed-upon interest rate and to return the securities on a specified future date. The maturity date may be the next day or many days later, with the maximum length set by the FOMC. These transactions permit the Federal Reserve to increase the supply of Federal Reserve balances for the length of the agreement.

required reserve balance

That portion of its required reserves that a depository institution must hold in an account at a Federal Reserve Bank. This portion is the difference between the institution's reserve requirement and its vault cash.

required reserve ratio

The percentage of reservable liabilities that depository institutions must set aside in the form of reserves.

required reserves

Funds that a depository institution is required to maintain in the form of vault cash or, if vault cash is insufficient to meet the requirement, in the form of a balance maintained directly with a Reserve Bank or indirectly with a pass-through correspondent bank. The required amount varies according to the required reserve ratios set by the Board and the amount of reservable liabilities held by the institution.

reservable liabilities

Those obligations on a depository institution's balance sheet that are subject to reserve requirements. Transaction deposits, nonpersonal time deposits, and Eurocurrency liabilities are all subject to reserve requirements; however, the required reserve ratios for nonpersonal time deposits and Eurocurrency liabilities are zero.

reserve requirements

Requirements set by the Board of Governors for the amounts of certain liabilities that depository institutions must set aside in the form of reserves.

reverse repurchase agreement

A transaction—the opposite of a repurchase agreement—in which the Federal Reserve enters into an agreement with a primary dealer to sell securities from the System portfolio for a specified principal amount at an agreed-upon interest rate and to receive the securities back from the dealer on a specified future date. The maturity date may be the next day or many days later, with the maximum length set by the FOMC. These transactions permit the Federal Reserve to decrease the supply of Federal Reserve balances for the length of the agreement.

S

savings and loan association (S&L)
Historically, depository institution that accepted deposits mainly from individuals and invested heavily in residential mortgage loans; although still primarily residential lenders, S&Ls now have many of the powers of commercial banks.

savings bank
Depository institution historically engaged primarily in accepting consumer savings deposits and in originating and investing in residential mortgage loans; now may offer checking-type deposits and make a wider range of loans. (*Compare* **commercial bank**.)

savings bond
A nonmarketable debt obligation of the U.S. government. Savings bonds are available in both paper and book-entry form and can be purchased with an initial investment of as little as $25. Investors can purchase paper savings bonds in person from many depository institutions, by mail from a Reserve Bank or the Treasury, or online. Book-entry bonds are available from the Treasury online.

securities
Paper certificates (definitive securities) or electronic records (book-entry securities) evidencing ownership of equity (stocks) or debt obligations (bonds).

securitization
The process of packaging and selling similar financial instruments, such as loans and other receivables, in the form of "asset-backed" securities that can be traded on secondary markets. Securitization allows financial institutions to transfer some of the risks of ownership to parties more willing or able to manage them.

self-regulatory organizations
Associations of broker-dealers or others that have responsibility, under the oversight of the Securities and Exchange Commission, to regulate their own members through the adoption and enforcement of rules of conduct for fair, ethical, and efficient practices. Examples include the National Association of Securities Dealers and the New York Stock Exchange.

settlement
In banking, the process of recording the debit and credit positions of two parties in a transfer of funds. Also, the delivery of securities by a seller and the payment by the buyer.

shock
Unanticipated or unusual event that has a noticeable impact on the economy or a financial system.

special drawing rights (SDRs)
Type of international reserve asset created by the International Monetary Fund and allocated, on occasion, to the nations that are members of the IMF.

state bank
Bank that is chartered by a state; may or may not be a member of the Federal Reserve System.

subsidiary
Company that is controlled by another corporation (called the parent corporation), typically through stock ownership or voting control.

substitute check
A paper reproduction of an original check that contains an image of the front and back of the original check and is suitable for automated processing, just as the original check is. The Check Clearing for the 21st Century Act, commonly known as Check 21, allows depository institutions to truncate original checks, process check information electronically, and deliver substitute checks to depository institutions if they require paper checks.

swap
An agreement between two parties to exchange cash flows of underlying securities. For example, in an interest rate swap, the most common type of swap, one party agrees to pay a fixed interest rate in return for receiving a variable rate from the other party.

swap arrangement
See **reciprocal currency arrangement**.

System Open Market Account
The Federal Reserve's portfolio of U.S. Treasury securities. Purchases and sales in this account—open market operations—are under the overall supervision of the manager of the System Open Market Account, subject to the policies and rules of the Federal Open Market Committee.

systemic risk
Risk that a disruption at a firm, in a market segment, to a settlement system, or in a similar setting will cause widespread difficulties at other firms, in other market segments, or in the financial system as a whole.

T

thrift institution
A general term encompassing savings banks, savings and loan associations, and credit unions.

Thrift Institutions Advisory Council
Group established by the Board of Governors to obtain information and opinions on the needs and problems of thrift institutions. Made up of representatives of savings and loan associations, savings banks, and credit unions.

tightening
Federal Reserve action to raise interest rates. Undertaken when inflation is a concern. (*Compare* **easing**.)

time deposit
Funds deposited in an account that has a fixed term to maturity and technically cannot be withdrawn before maturity without advance notice (for example, a certificate of deposit). Time deposits may earn interest.

Trading Desk (the Desk)
The group at the Federal Reserve Bank of New York that conducts open market operations for the Federal Reserve System and intervenes in foreign currency markets for the Federal Reserve and Treasury.

transaction account
A checking account or similar deposit account from which transfers of funds can be made. Demand deposit accounts, NOW (negotiable order of withdrawal) accounts, and credit union share draft accounts are examples of transaction accounts.

U

U.S. Treasury securities
Obligations of the U.S. government issued by the U.S. Department of the Treasury as a means of borrowing money to meet government expenditures not covered by tax revenues. All marketable Treasury securities have a minimum purchase amount of $1,000 and are issued in $1,000 increments. There are three types of marketable Treasury securities: bills, notes, and bonds.

- **Treasury bill (T-bill)**
  Short-term U.S. Treasury security having a maturity of up to one year. T-bills are sold at a discount. Investors purchase a bill at a price lower than the face value (for example, the investor might buy a

$10,000 bill for $9,700); the return is the difference between the price paid and the amount received when the bill is sold or it matures (if held to maturity, the return on the T-bill in the example would be $300).

- **Treasury note**
  Intermediate-term security having a maturity of one to ten years. Notes pay interest semiannually, and the principal is payable at maturity.
- **Treasury bond**
  Long-term security having a maturity of longer than ten years. Bonds pay interest semiannually, and the principal is payable at maturity.

The Treasury Department also issues several types of nonmarketable securities, including savings bonds.

V

vault cash
Cash on hand at a depository institution to meet day-to-day business needs, such as cashing checks for customers. Can be used to satisfy the institution's reserve requirement.

W

wire transfer
Electronic transfer of funds; usually involves large-dollar payments.

Index

D

E

F

G

H

I

M

S

Board of Governors
www.federalreserve.gov

Federal Reserve Bank of Atlanta
www.frbatlanta.org

Federal Reserve Bank of Boston
www.bos.frb.org

Federal Reserve Bank of Chicago
www.chicagofed.org

Federal Reserve Bank of Cleveland
www.clevelandfed.org

Federal Reserve Bank of Dallas
www.dallasfed.org

Federal Reserve Bank of Kansas City
www.kansascityfed.org

Federal Reserve Bank of Minneapolis
www.minneapolisfed.org

Federal Reserve Bank of New York
www.newyorkfed.org

Federal Reserve Bank of Philadelphia
www.philadelphiafed.org

Federal Reserve Bank of Richmond
www.rich.frb.org

Federal Reserve Bank of San Francisco
www.frbsf.org

Federal Reserve Bank of St. Louis
www.stlouisfed.org

Published by the Board of Governors of the Federal Reserve System on behalf of the Federal Reserve System.

Board Members

Print

Janet L. Yellen, *Chair*
Stanley Fischer, *Vice Chairman*
Daniel K. Tarullo
Jerome H. Powell
Lael Brainard

Members since 1913

The seven members of the Board of Governors of the Federal Reserve System are nominated by the President and confirmed by the Senate. A full term is fourteen years. One term begins every two years, on February 1 of even-numbered years. A member who serves a full term may not be reappointed. A member who completes an unexpired portion of a term may be reappointed. All terms end on their statutory date regardless of the date on which the member is sworn into office.

The Chairman and the Vice Chairman of the Board are named by the President from among the members and are confirmed by the Senate. They serve a term of four years. A member's term on the Board is not affected by his or her status as Chairman or Vice Chairman.

Board Member Assignments - Board Committees

Committee on Board Affairs
Governor Powell, Chairman
Vice Chairman Fischer

Committee on Consumer and Community Affairs
Governor Brainard, Chair
Governor Tarullo

Committee on Economic and Financial Monitoring and Research
Vice Chairman Fischer, Chairman
Governor Brainard

Committee on Financial Stability
Vice Chairman Fischer, Chairman
Governor Tarullo
Governor Brainard

Committee on Federal Reserve Bank Affairs
Governor Powell, Chairman
Governor Brainard

Committee on Bank Supervision
Governor Tarullo, Chairman
Governor Powell
Governor Brainard

Subcommittee on Smaller Regional and Community Banking
Governor Powell, Chairman
Governor Brainard

Committee on Payments, Clearing, and Settlement
Governor Powell, Chairman
Governor Tarullo

Employer Information Report EEO-1

Current | Archive: 2011 GO

Federal Reserve Board, 2011 Employer Information Report

Percentage

Occupational Categories	Total Employees			RACE/ETHNICITY													
				Hispanic or Latino		Non- Hispanic or Latino											
						White		Black or African American		Asian		Native Hawaiian or Other Pacific Islander		American Indian or Alaska Native		Two or more races	
	All	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female
1.1 Exec. Sr. Lvl Mgrs Governors, Officers, FR-29 & FR-28																	
By total	343	201	142	3	4	170	107	15	20	11	9	2	1	0	0	0	1
By percent	100.00%	58.60%	41.40%	0.87%	1.17%	49.56%	31.20%	4.37%	5.83%	3.21%	2.62%	0.58%	0.29%	0.00%	0.00%	0.00%	0.29%
1.2 1st / Mid Lvl																	
By total	81	38	43	1	0	19	25	15	16	3	2	0	0	0	0	0	0
By percent	100.00%	46.91%	53.09%	1.23%	0.00%	23.46%	30.86%	18.52%	19.75%	3.70%	2.47%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Officials & Managers Total																	
By total	424	239	185	4	4	189	132	30	36	14	11	2	1	0	0	0	1
By percent	100.00%	56.37%	43.63%	0.94%	0.94%	79.08%	31.13%	7.08%	8.49%	3.30%	2.59%	0.47%	0.24%	0.00%	0.00%	0.00%	0.24%
2. Professionals																	
By total	1,459	775	684	36	37	521	338	80	180	119	114	14	14	1	0	4	1
By percent	100.00%	53.12%	46.88%	2.47%	2.54%	67.23%	23.17%	5.48%	12.34%	8.16%	7.81%	0.96%	0.96%	0.07%	0.00%	0.27%	0.07%
3. Technicians																	
By total	6	2	4	0	0	0	2	2	2	0	0	0	0	0	0	0	0
By percent	100.00%	33.33%	66.67%	0.00%	0.00%	0.00%	33.33%	33.33%	33.33%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
4. Sales Workers																	
By total	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
By percent	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
5. Administrative Support Workers																	
By total	154	27	127	1	5	7	12	19	104	0	4	0	0	0	2	0	0
By percent	100.00%	17.53%	82.47%	0.65%	3.25%	4.55%	7.79%	12.34%	67.53%	0.00%	2.60%	0.00%	0.00%	0.00%	1.30%	0.00%	0.00%
6. Craft Workers																	
By total	42	41	1	0	0	23	0	14	1	3	0	1	0	0	0	0	0
By percent	100.00%	97.62%	2.38%	0.00%	0.00%	54.76%	0.00%	33.33%	2.38%	7.14%	0.00%	2.38%	0.00%	0.00%	0.00%	0.00%	0.00%
7. Operatives																	
By total	12	12	0	0	0	1	0	11	0	0	0	0	0	0	0	0	0
By percent	100.00%	100.00%	0.00%	0.00%	0.00%	8.33%	0.00%	91.67%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
8. Laborers and Helpers																	
By total	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
By percent	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
9. Service Workers																	
By total	177	142	35	7	0	47	4	83	29	5	1	0	1	0	0	0	0

Occupational Categories	Total Employees			RACE/ETHNICITY													
				Hispanic or Latino		Non- Hispanic or Latino											
						White		Black or African American		Asian		Native Hawaiian or Other Pacific Islander		American Indian or Alaska Native		Two or more races	
	All	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female
By percent	100.00%	80.23%	19.77%	3.95%	0.00%	26.55%	2.26%	46.89%	16.38%	2.82%	0.56%	0.00%	0.56%	0.00%	0.00%	0.00%	0.00%
Total Workforce																	
By total	2,274	1,238	1,036	48	46	788	488	239	352	141	130	17	16	1	2	4	2
By percent	100%	54.44%	45.56%	2.11%	2.02%	34.65%	21.46%	10.51%	15.48%	6.20%	5.72%	0.75%	0.70%	0.04%	0.09%	0.18%	0.09%

Last update: August 2, 2013

Federal Reserve Act

Print

Section 10. Board of Governors of the Federal Reserve System

1. Appointment and qualification of members

The Board of Governors of the Federal Reserve System (hereinafter referred to as the "Board") shall be composed of seven members, to be appointed by the President, by and with the advice and consent of the Senate, after the date of enactment of the Banking Act of 1935, for terms of fourteen years except as hereinafter provided, but each appointive member of the Federal Reserve Board in office on such date shall continue to serve as a member of the Board until February 1, 1936, and the Secretary of the Treasury and the Comptroller of the Currency shall continue to serve as members of the Board until February 1, 1936. In selecting the members of the Board, not more than one of whom shall be selected from any one Federal Reserve district, the President shall have due regard to a fair representation of the financial, agricultural, industrial, and commercial interests, and geographical divisions of the country. The members of the Board shall devote their entire time to the business of the Board and shall each receive an annual salary of $15,000, payable monthly, together with actual necessary traveling expenses.

[12 USC 241. As amended by acts of June 3, 1922 (42 Stat. 620); Aug. 23, 1935 (49 Stat. 704). Prior to the enactment of the Banking Act of 1935, approved Aug. 23, 1935, the Board of Governors of the Federal Reserve System was known as the Federal Reserve Board. See note to the third paragraph of section 1. The portion of this paragraph dealing with salaries of Board members has in effect been amended numerous times, most recently by Executive Order. Prior to the act of December 27, 2000, section 1002 of which revised the executive schedule, the salary of the chairman of the Board was set at executive schedule level 2 and the salary of other members at level 3. The salary of the chairman of the Board is now set at executive schedule level I, and the salary of other members at level II (see 2 USC 358 and 5 USC 5313 and 5314).]

Back to Top

2. Members ineligible to serve member banks; term of office; chairman and vice chairman

The members of the Board shall be ineligible during the time they are in office and for two years thereafter to hold any office, position, or employment in any member bank, except that this restriction shall not apply to a member who has served the full term for which he was appointed. Upon the expiration of the term of any appointive member of the Federal Reserve Board in office on the date of enactment of the Banking Act of 1935, the President shall fix the term of the successor to such member at not to exceed fourteen years, as designated by the President at the time of nomination, but in such manner as to provide for the expiration of the term of not more than one member in any two-year period, and thereafter each member shall hold office for a term of fourteen years from the expiration of the term of his predecessor, unless sooner removed for cause by the President. Of the persons thus appointed, 1 shall be designated by the President, by and with the advice and consent of the Senate, to serve as Chairman of the Board for a term of 4 years, and 2 shall be designated by the President, by and with the advice and consent of the Senate, to serve as Vice Chairmen of the Board, each for a term of 4 years, 1 of whom shall serve in the absence of the Chairman, as provided in the fourth undesignated paragraph of this section, and 1 of whom shall be designated Vice Chairman for Supervision. The Vice Chairman for Supervision shall develop policy recommendations for the Board regarding supervision and regulation of depository institution holding companies and other financial firms supervised by the Board, and shall oversee the supervision and regulation of such firms. The chairman of the Board, subject to its supervision, shall be its active executive officer. Each member of the Board shall within fifteen days after notice of appointment make and subscribe to the oath of office. Upon the expiration of their terms of office, members of the Board shall continue to serve until their successors are appointed and have qualified. Any person appointed as a member of the Board after the date of enactment of the Banking Act of 1935 shall not be eligible for reappointment as such member after he shall have served a full term of fourteen years.

[12 USC 242. As amended by acts of March 3, 1919 (40 Stat. 1315); June 3, 1922 (42 Stat. 620); June 16, 1933 (48 Stat. 166); Aug. 23, 1935 (49 Stat. 704); November 16, 1977 (91 Stat. 1388); and act of July 21, 2010 (124 Stat. 2126). The Banking Act of 1935, referred to in this paragraph, became effective Aug. 23, 1935. Prior to the enactment of that act, the chairman and vice chairman of the Board of Governors of the Federal Reserve System were known as the governor and vice governor of the Federal Reserve Board, respectively. See note to the third paragraph of section 1. The act of November 16, 1977, amended the second sentence of this paragraph. The amendment takes effect on Jan. 1, 1979, and applies to individuals who are designated by the President on or after such date to serve as chairman or vice chairman. The act of July 21, 2010, designated a new Vice Chairman for Supervision.]

Back to Top

3. Assessments on Federal reserve banks

The Board of Governors of the Federal Reserve System shall have power to levy semiannually upon the Federal reserve banks, in proportion to their capital stock and surplus, an assessment sufficient to pay its estimated expenses and the salaries of its members and employees for the half year succeeding the levying of such assessments, together with any deficit carried forward from the preceding half year, and such assessments may include amounts sufficient to provide for the acquisition by the Board in its own name of such site or building in the District of Columbia as in its judgment alone shall be necessary for the purpose of providing suitable and adequate quarters for the performance of its functions. After September 1, 2000, the Board may also use such assessments to acquire, in its own name, a site or building (in addition to the facilities existing on such date) to provide for the performance of the functions of the Board. After approving such plans, estimates, and specifications as it shall have caused to be prepared, the Board may, notwithstanding any other provision of law, cause to be constructed on any site so acquired by it a building or buildings suitable and adequate in its judgment for

its purposes and proceed to take all such steps as it may deem necessary or appropriate in connection with the construction, equipment, and furnishing of such building or buildings. The Board may maintain, enlarge, or remodel any building or buildings so acquired or constructed and shall have sole control of such building or buildings and space therein.

[12 USC 243. As reenacted without change by act of June 3, 1922 (42 Stat. 621); and amended by acts of June 19, 1934 (48 Stat. 1108) and Dec. 27, 2000 (114 Stat. 3027). By act approved June 27, 1935 (49 Stat. 425), provision was made for the furnishing of steam from the central heating plant to the Federal Reserve Board, now the Board of Governors of the Federal Reserve System.]

Back to Top

4. Principal offices; expenses; deposit of funds; members not to be officers or stockholders of banks

The principal offices of the Board shall be in the District of Columbia. At meetings of the Board the chairman shall preside, and, in his absence, the vice chairman shall preside. In the absence of the chairman and the vice chairman, the board shall elect a member to act as chairman pro tempore. The Board shall determine and prescribe the manner in which its obligations shall be incurred and its disbursements and expenses allowed and paid, and may leave on deposit in the Federal Reserve banks the proceeds of assessments levied upon them to defray its estimated expenses and the salaries of its members and employees, whose employment, compensation, leave, and expenses shall be governed solely by the provisions of this Act, specific amendments thereof, and rules and regulations of the Board not inconsistent therewith; and funds derived from such assessments shall not be construed to be Government funds or appropriated moneys. No member of the Board of Governors of the Federal Reserve System shall be an officer or director of any bank, banking institution, trust company, or Federal Reserve bank or hold stock in any bank, banking institution, or trust company; and before entering upon his duties as a member of the Board of Governors of the Federal Reserve System he shall certify under oath that he has complied with this requirement, and such certification shall be filed with the secretary of the Board. Whenever a vacancy shall occur, other than by expiration of term, among the six members of the Board of Governors of the Federal Reserve System appointed by the President as above provided, a successor shall be appointed by the President, by and with the advice and consent of the Senate, to fill such vacancy, and when appointed he shall hold office for the unexpired term of his predecessor.

[12 USC 244. As amended by acts of June 3, 1922 (42 Stat. 621); June 16, 1933 (48 Stat. 167); Aug. 23, 1935 (49 Stat. 705). The reference to "the six members" of the Board of Governors is an apparent error in the law and should read "the seven members." See section 10, first paragraph, this act.]

Back to Top

5. Vacancies during recess of Senate

The President shall have power to fill all vacancies that may happen on the Board of Governors of the Federal Reserve System during the recess of the Senate by granting commissions which shall expire with the next session of the Senate.

[12 USC 245. As amended by act of June 3, 1922 (42 Stat. 621).]

Back to Top

6. Reservation of powers of Secretary of Treasury

Nothing in this Act contained shall be construed as taking away any powers heretofore vested by law in the Secretary of the Treasury which relate to the supervision, management, and control of the Treasury Department and bureaus under such department, and wherever any power vested by this Act in the Board of Governors of the Federal Reserve System or the Federal reserve agent appears to conflict with the powers of the Secretary of the Treasury, such powers shall be exercised subject to the supervision and control of the Secretary.

[12 USC 246. As reenacted without change by act of June 3, 1922 (42 Stat. 621).]

Back to Top

7. Annual report

The Board of Governors of the Federal Reserve System shall annually make a full report of its operations to the Speaker of the House of Representatives, who shall cause the same to be printed for the information of the Congress. The report required under this paragraph shall include the reports required under section 707 of the Equal Credit Opportunity Act, section 18(f)(7) of the Federal Trade Commission Act, section 114 of the Truth in Lending Act, and the tenth undesignated paragraph of this section.

[12 USC 247. As reenacted without change by act of June 3, 1922 (42 Stat. 621) and amended by acts of June 3, 1922, and Dec. 27, 2000 (114 Stat. 3030).]

Back to Top

8. Office of the Comptroller of the Currency

Section three hundred and twenty-four of the Revised Statutes of the United States shall be amended so as to read as follows:

(a) Office Of The Comptroller Of The Currency Established. There is established in the Department of the Treasury a bureau to be known as the “Office of the Comptroller of the Currency” which is charged with assuring the safety and soundness of, and compliance with laws and regulations, fair access to financial services, and fair treatment of customers by, the institutions and other persons subject to its jurisdiction.

(b) Comptroller Of The Currency.

1. **In General.** The chief officer of the Office of the Comptroller of the Currency shall be known as the Comptroller of the Currency. The Comptroller of the Currency shall perform the duties of the Comptroller of the Currency under the general direction of the Secretary of the Treasury. The Secretary of the Treasury may not delay or prevent the issuance of any rule or the promulgation of any regulation by the Comptroller of the Currency, and may not intervene in any matter or proceeding before the Comptroller of the Currency (including agency enforcement actions), unless otherwise specifically provided by law.
2. **Additional Authority.** The Comptroller of the Currency shall have the same authority with respect to functions

transferred to the Comptroller of the Currency under the Enhancing Financial Institution Safety and Soundness Act of 2010 as was vested in the Director of the Office of Thrift Supervision on the transfer date, as defined in section 311 of that Act.

[12 USC 1. As reenacted without change by act of June 3, 1922 (42 Stat. 621); and amended by acts of May 20, 1966 (80 Stat. 161), Sept. 23, 1994 (108 Stat. 2232), and July 21, 2010 (124 Stat. 1523).]

Back to Top

9. Branch Federal Reserve bank buildings

No Federal Reserve bank may authorize the acquisition or construction of any branch building, or enter into any contract or other obligation for the acquisition or construction of any branch building, without the approval of the Board.

[12 USC 522. As added by act of June 3, 1922 (42 Stat. 622); and amended by acts of Feb. 6, 1923 (42 Stat. 1223); July 30, 1947 (61 Stat. 520); May 29, 1953 (67 Stat. 41); Aug. 31, 1962 (76 Stat. 418); Oct. 28, 1974 (88 Stat. 1505); and Oct. 24, 1992 (106 Stat. 3144).]

Back to Top

10. Record of open market and other policies

The Board of Governors of the Federal Reserve System shall keep a complete record of the action taken by the Board and by the Federal Open Market Committee upon all questions of policy relating to open-market operations and shall record therein the votes taken in connection with the determination of open-market policies and the reasons underlying the action of the Board and the Committee in each instance. The Board shall keep a similar record with respect to all questions of policy determined by the Board, and shall include in its annual report to the Congress a full account of the action so taken during the preceding year with respect to open-market policies and operations and with respect to the policies determined by it and shall include in such report a copy of the records required to be kept under the provisions of this paragraph.

[12 USC 247a. As added by act of Aug. 23, 1935 (49 Stat. 705).]

Back to Top

12. Appearances before Congress*

The Vice Chairman for Supervision shall appear before the Committee on Banking, Housing, and Urban Affairs of the Senate and the Committee on Financial Services of the House of Representatives and at semi-annual hearings regarding the efforts, activities, objectives, and plans of the Board with respect to the conduct of supervision and regulation of depository institution holding companies and other financial firms supervised by the Board.

[12 USC 247b. As added by act of July 21, 2010 (124 Stat. 2126).]

* The act of July 21, 2010, added paragraph 12 without adding paragraph 11.

Back to Top

Report to the Congress on the Office of Minority and Women Inclusion

Print

Preface: Implementing the Dodd-Frank Act
Introduction
Equal Employment of Minorities and Women
Inclusion of Minority-Owned and Women-Owned Businesses
Financial Literacy Activities
Diversity Policies and Practices of Regulated Entities
Appendix A

Other Formats
- Full Report (PDF)

Stay Connected
Twitter YouTube
Flickr RSS Feeds
Subscribe

Financial Literacy Activities

During 2013, the Board continued to participate in community and Federal Reserve System outreach events and programs, examples of which are listed below.

- *Congressional Black Caucus Annual Legislative Conference*: In September 2013, the Board, in conjunction with the Federal Reserve System, sponsored a booth at the 43rd Annual Legislative Conference. Financial education materials and information were distributed to conference attendees. The Board also provided support for the Financial Education Youth Summit convened by the Congressional Black Caucus held at the U.S. Capitol Visitor Center and Trinity Washington University.
- *FedEd Program*: During 2013, research assistants from divisions within the Board continued to implement a program developed to work with local high school students to improve their understanding of personal finances and the role of the Federal Reserve System in the economy. Subjects covered include the importance of saving, budgeting, using credit, establishing financial goals, and the impact of Federal Reserve policy on those subjects. More than 40 presentations were made to middle and high school students in the Washington metropolitan area. Presentations were made at ten schools in the District of Columbia: Roosevelt High School; Wilson High School; Coolidge High School; Dunbar High School; Anacostia High School; Ballou High School; Washington Latin Public Charter School; Edmund Burke School; KIPP DC Charter School; and St. Albans School. Presentations were made at two schools in Virginia--Annandale High School and Marshall High School--and one school in Maryland--Stone Ridge School of the Sacred Heart. Presentations were also made at the District of Columbia Public Schools Central Office to preview the FedEd Program for the New Heights Providers Meeting, the Sumner School for the DC Future Business Leaders of America, and the Heights School.
- *Federal Reserve Financial Literacy Day*: On October 23, 2013, the Board and the Federal Reserve System held training programs and seminars around the country on such topics as saving, budgeting, credit use, and the establishment of financial goals. Board research assistants presented the program to classes at two schools in the District of Columbia: Cardozo High School and the Columbia Heights Education Campus.
- *Math x Economics*: On May 23, 2013, the Board hosted the Math x Economics program for a second year in a row. The goal of the program was to introduce students to economics as a potential course of study in college and as a future career option. The Board's recruitment efforts targeted groups who are underrepresented in the field of economics, including minorities and females, especially from underserved schools. A total of 29 students from Washington metropolitan area schools attended. The students completed a survey at the end of the program; all 29 participants said they would recommend the program to other students. The descriptive statistics of the respondents are listed below.

Distribution of participants	Percent
Female	56
Male	44
Juniors	78
Seniors	22
African American	25.9
Hispanic	18.5
Asian	18.5
White	18.5
More than one ethnicity	14.8
Did not specify ethnicity	3.7

- *Education and Training Materials Distribution*: During 2013, the Board continued to provide financial literacy materials to consumer education and financial literacy groups, including the University of Maryland Extension Family and Consumer Sciences Center, the YMCA of Metropolitan Washington, Operation HOPE, and It Takes a Community to Raise a Child (located in New York City).

- *Professional Outreach*: On April 3, 2013, Chairman Bernanke delivered remarks to the 13th Annual Redefining Investment Strategy Education (RISE) Forum. His remarks highlighted the importance of promoting economic and financial knowledge among people of all ages and walks of life. He stated that the Board and the 12 Federal Reserve Banks are all deeply involved in economic education and in supporting the work of teachers, schools, and national organizations.

  On November 13, 2013, Chairman Bernanke hosted the annual Teacher Town Hall Meeting at the Federal Reserve Board. Federal Reserve Banks also held gatherings around the country to provide educators the opportunity to listen to the Chairman and ask questions. His remarks covered the origins, history, and role of the Federal Reserve, and how it has helped shape the nation's economy and financial system.

Last update: Apr 8, 2014

October 30, 2014
Federal Reserve Board
Washington, D.C.

Sponsored by:
Federal Reserve Board

National Summit on Diversity in the Economics Profession

Print

About | Conference Program

About

The National Summit on Diversity in the Economics Profession, hosted by the Board of Governors of the Federal Reserve System in partnership with the American Economic Association, will be held at the Federal Reserve Board on October 30, 2014 in Washington, D.C. This conference brings together presidents and research directors of the Federal Reserve Banks and chairs of economics departments from around the country to open a profession-wide dialogue about diversity. Speakers and panelists will discuss the state of diversity in the economics profession and examples of successful diversity initiatives in academia. A hallmark of the conference will be the opportunity for collegial learning, discussion, and sharing among faculty peers to develop practical ideas about what can be accomplished in our profession.

Please note that attendance at the conference is by invitation only. Conference attendees and media representatives must register in advance.

Watch the online webcast of the event at http://www.ustream.tv/federalreserve

Organizers

- Janice Shack-Marquez
- Amanda Bayer

No FEAR Act Data

No FEAR Act Notice

PDF

The Notification and Federal Employee Anti-discrimination and Retaliation Act (No FEAR Act) of 2002 increases federal agency accountability for acts of discrimination or reprisal against employees.

The No FEAR Act requires agencies to post on their public websites statistical data relating to equal employment opportunity complaints filed against the respective agencies.

The Federal Reserve Board's public website contains statistical data in accordance with the No FEAR Act.

Information updated as 1st Quarter 2015 for period ending December 31, 2014

Complaint activity	Comparative data Previous fiscal year data					Fiscal Year 2015 thru 12/31
	2010	2011	2012	2013	2014	
Number of complaints filed	7	10	12	6	10	2
Number of complainants	7	10	12	6	10	2
Repeat filers	0	0	0	0	0	0

Return to top

Complaints by basis Note: Complaints can be filed alleging multiple bases. The sum of the bases may not equal total complaints filed	Comparative data Previous fiscal year data					Fiscal Year 2015 thru 12/31
	2010	2011	2012	2013	2014	
Race	6	10	16	15	15	1
Color	1	2	3	4	5	0
Religion	0	0	2	2	3	1
Reprisal	2	5	11	8	9	2
Sex	5	8	11	11	12	0
National origin	2	3	3	1	3	1
Equal Pay Act	0	0	1	3	3	0
Age	6	8	15	9	10	1
Disability	3	2	5	2	5	0
Non EEO	0	0	0	0	0	0

Return to top

Complaints by issue	Comparative data Previous fiscal year data	Fiscal Year 2015

Note: Complaints can be filed alleging multiple issues. The sum of the issues may not equal total complaints filed	2010	2011	2012	2013	2014	thru 12/31
Appointment/hire	0	0	0	0	1	0
Assignment of duties	2	3	4	4	4	2
Awards	0	0	0	0	0	0
Conversion to full-time	0	0	0	0	0	0
Disciplinary action						
Demotion	0	0	0	0	0	0
Reprimand	0	0	1	2	1	0
Removal	2	2	2	1	3	0
Suspension	0	0	0	0	0	0
Other	0	0	1	1	0	0
Duty hours	1	0	0	0	1	0
Evaluation appraisal	1	2	4	3	5	2
Examination/test	0	0	0	0	0	0
Harassment						
Nonsexual	4	8	11	10	13	2
Sexual	1	2	1	1	0	0
Medical examination	0	0	0	0	0	0
Pay (including overtime)	1	1	1	3	3	0
Promotion/nonselection	5	6	10	10	10	1
Reassignment						
Denied	0	0	0	0	0	0
Directed	0	0	0	0	0	0
Reasonable accommodation	1	1	3	2	4	0
Reinstatement	0	0	0	0	0	0
Retirement	0	0	0	0	0	0
Termination	0	2	2	0	0	0
Terms/conditions of employment	2	2	9	5	6	0
Time and attendance	0	0	0	0	0	0
Training	0	0	0	1	1	0
Other	3	4	1	2	2	2

Return to top

Processing time	Comparative data Previous fiscal year data					Fiscal Year 2015 thru 12/31
	2010	2011	2012	2013	2014	
Complaints pending during fiscal year						
Average number of days in investigation stage	68	151	133	228	148	197
Average number of days in final action stage	28	36	53	26	0	0
Complaints pending during fiscal year where hearing was requested						
Average number of days in investigation stage	93	183	148	151	211	108
Average number of days in final action stage	28	36	47	27	0	0
Complaints pending during fiscal year where hearing was not requested						
Average number of days in investigation stage	87	0	93	220	55	0
Average number of days in final action stage	62	0	92	24	0	0

Return to top

Complaints dismissed by agency	Comparative data Previous fiscal year data					Fiscal Year 2015 thru 12/31
	2010	2011	2012	2013	2014	
Total complaints dismissed by agency	0	1	0	1	0	0
Average days pending prior to dismissal	0	531	0	27	0	0
Complaints withdrawn by complainants						
Total complaints withdrawn by complainants	1	0	0	1	1	1

Return to top

Total final actions finding discrimination	Comparative data Previous fiscal year data										Fiscal Year 2015 thru 12/31	
	2010		2011		2012		2013		2014			
	#	%	#	%	#	%	#	%	#	%	#	%
Total number findings	0		0		0		0		0		0	
Without hearing	0	0	0	0	0	0	0	0	0	0	0	0
With hearing	0	0	0	0	0	0	0	0	0	0	0	0

Return to top

Findings of discrimination rendered by basis Note: Complaints can be filed alleging multiple bases. The sum of the bases may not equal total complaints and findings	Comparative data Previous fiscal year data										Fiscal Year 2015 thru 12/31	
	2010		2011		2012		2013		2014			
	#	%	#	%	#	%	#	%	#	%	#	%
Total number findings	0		0		0		0		0		0	
Race	0	0	0	0	0	0	0	0	0	0	0	0
Color	0	0	0	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0	0	0	0
Reprisal	0	0	0	0	0	0	0	0	0	0	0	0
Sex	0	0	0	0	0	0	0	0	0	0	0	0
National origin	0	0	0	0	0	0	0	0	0	0	0	0
Equal Pay Act	0	0	0	0	0	0	0	0	0	0	0	0
Age	0	0	0	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0	0	0	0
Non EEO	0	0	0	0	0	0	0	0	0	0	0	0
Findings after hearing	0	0	0	0	0	0	0	0	0	0	0	0
Race	0	0	0	0	0	0	0	0	0	0	0	0
Color	0	0	0	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0	0	0	0
Reprisal	0	0	0	0	0	0	0	0	0	0	0	0
Sex	0	0	0	0	0	0	0	0	0	0	0	0
National origin	0	0	0	0	0	0	0	0	0	0	0	0
Equal Pay Act	0	0	0	0	0	0	0	0	0	0	0	0
Age	0	0	0	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0	0	0	0
Non EEO	0	0	0	0	0	0	0	0	0	0	0	0
Findings without hearing	0	0	0	0	0	0	0	0	0	0	0	0
Race	0	0	0	0	0	0	0	0	0	0	0	0
Color	0	0	0	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0	0	0	0
Reprisal	0	0	0	0	0	0	0	0	0	0	0	0
Sex	0	0	0	0	0	0	0	0	0	0	0	0
National origin	0	0	0	0	0	0	0	0	0	0	0	0
Equal Pay Act	0	0	0	0	0	0	0	0	0	0	0	0
Age	0	0	0	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0	0	0	0
Non EEO	0	0	0	0	0	0	0	0	0	0	0	0

Return to top

Findings of discrimination rendered by issue	Comparative data Previous fiscal year data										Fiscal Year 2015 thru 12/31	
	2010		2011		2012		2013		2014			
	#	%	#	%	#	%	#	%	#	%		%

Findings of discrimination rendered by issue	Comparative data Previous fiscal year data										Fiscal Year 2015 thru 12/31	
	2010		2011		2012		2013		2014			
	#	%	#	%	#	%	#	%	#	%		%
Total number findings	0		0		0		0		0		0	
Appointment/hire	0	0	0	0	0	0	0	0	0	0	0	0
Assignment of duties	0	0	0	0	0	0	0	0	0	0	0	0
Awards	0	0	0	0	0	0	0	0	0	0	0	0
Conversion to full-time	0	0	0	0	0	0	0	0	0	0	0	0
Disciplinary action	0	0	0	0	0	0	0	0	0	0	0	0
Demotion	0	0	0	0	0	0	0	0	0	0	0	0
Reprimand	0	0	0	0	0	0	0	0	0	0	0	0
Suspension	0	0	0	0	0	0	0	0	0	0	0	0
Removal	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0
Duty hours	0	0	0	0	0	0	0	0	0	0	0	0
Evaluation appraisal	0	0	0	0	0	0	0	0	0	0	0	0
Examination/test	0	0	0	0	0	0	0	0	0	0	0	0
Harassment	0	0	0	0	0	0	0	0	0	0	0	0
Nonsexual	0	0	0	0	0	0	0	0	0	0	0	0
Sexual	0	0	0	0	0	0	0	0	0	0	0	0
Medical examination	0	0	0	0	0	0	0	0	0	0	0	0
Pay (including overtime)	0	0	0	0	0	0	0	0	0	0	0	0
Promotion/nonselection	0	0	0	0	0	0	0	0	0	0	0	0
Reassignment	0	0	0	0	0	0	0	0	0	0	0	0
Denied	0	0	0	0	0	0	0	0	0	0	0	0
Directed	0	0	0	0	0	0	0	0	0	0	0	0
Reasonable accommodation	0	0	0	0	0	0	0	0	0	0	0	0
Reinstatement	0	0	0	0	0	0	0	0	0	0	0	0
Retirement	0	0	0	0	0	0	0	0	0	0	0	0
Termination	0	0	0	0	0	0	0	0	0	0	0	0
Terms/conditions of employment	0	0	0	0	0	0	0	0	0	0	0	0
Time and attendance	0	0	0	0	0	0	0	0	0	0	0	0
Training	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0
Findings after hearing												
Appointment/hire	0	0	0	0	0	0	0	0	0	0	0	0
Assignment of duties	0	0	0	0	0	0	0	0	0	0	0	0
Awards	0	0	0	0	0	0	0	0	0	0	0	0
Conversion to full-time	0	0	0	0	0	0	0	0	0	0	0	0
Disciplinary action	0	0	0	0	0	0	0	0	0	0	0	0
Demotion	0	0	0	0	0	0	0	0	0	0	0	0
Reprimand	0	0	0	0	0	0	0	0	0	0	0	0
Suspension	0	0	0	0	0	0	0	0	0	0	0	0
Removal	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0
Duty hours	0	0	0	0	0	0	0	0	0	0	0	0
Evaluation appraisal	0	0	0	0	0	0	0	0	0	0	0	0
Examination/test	0	0	0	0	0	0	0	0	0	0	0	0
Harassment	0	0	0	0	0	0	0	0	0	0	0	0
Nonsexual	0	0	0	0	0	0	0	0	0	0	0	0
Sexual	0	0	0	0	0	0	0	0	0	0	0	0
Medical examination	0	0	0	0	0	0	0	0	0	0	0	0
Pay (including overtime)	0	0	0	0	0	0	0	0	0	0	0	0
Promotion/nonselection	0	0	0	0	0	0	0	0	0	0	0	0
Reassignment	0	0	0	0	0	0	0	0	0	0	0	0
Denied	0	0	0	0	0	0	0	0	0	0	0	0

Findings of discrimination rendered by issue	Comparative data Previous fiscal year data										Fiscal Year 2015 thru 12/31	
	2010		2011		2012		2013		2014			
	#	%	#	%	#	%	#	%	#	%		%
Directed	0	0	0	0	0	0	0	0	0	0	0	0
Reasonable accommodation	0	0	0	0	0	0	0	0	0	0	0	0
Reinstatement	0	0	0	0	0	0	0	0	0	0	0	0
Retirement	0	0	0	0	0	0	0	0	0	0	0	0
Termination	0	0	0	0	0	0	0	0	0	0	0	0
Terms/conditions of employment	0	0	0	0	0	0	0	0	0	0	0	0
Time and attendance	0	0	0	0	0	0	0	0	0	0	0	0
Training	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0
Findings without hearing	0	0	0	0	0	0	0	0	0	0	0	0
Appointment/hire	0	0	0	0	0	0	0	0	0	0	0	0
Assignment of duties	0	0	0	0	0	0	0	0	0	0	0	0
Awards	0	0	0	0	0	0	0	0	0	0	0	0
Conversion to full-time	0	0	0	0	0	0	0	0	0	0	0	0
Disciplinary action	0	0	0	0	0	0	0	0	0	0	0	0
Demotion	0	0	0	0	0	0	0	0	0	0	0	0
Reprimand	0	0	0	0	0	0	0	0	0	0	0	0
Suspension	0	0	0	0	0	0	0	0	0	0	0	0
Removal	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0
Duty hours	0	0	0	0	0	0	0	0	0	0	0	0
Evaluation appraisal	0	0	0	0	0	0	0	0	0	0	0	0
Examination/test	0	0	0	0	0	0	0	0	0	0	0	0
Harassment	0	0	0	0	0	0	0	0	0	0	0	0
Nonsexual	0	0	0	0	0	0	0	0	0	0	0	0
Sexual	0	0	0	0	0	0	0	0	0	0	0	0
Medical examination	0	0	0	0	0	0	0	0	0	0	0	0
Pay (including overtime)	0	0	0	0	0	0	0	0	0	0	0	0
Promotion/nonselection	0	0	0	0	0	0	0	0	0	0	0	0
Reassignment	0	0	0	0	0	0	0	0	0	0	0	0
Denied	0	0	0	0	0	0	0	0	0	0	0	0
Directed	0	0	0	0	0	0	0	0	0	0	0	0
Reasonable accommodation	0	0	0	0	0	0	0	0	0	0	0	0
Reinstatement	0	0	0	0	0	0	0	0	0	0	0	0
Retirement	0	0	0	0	0	0	0	0	0	0	0	0
Termination	0	0	0	0	0	0	0	0	0	0	0	0
Terms/conditions of employment	0	0	0	0	0	0	0	0	0	0	0	0
Time and attendance	0	0	0	0	0	0	0	0	0	0	0	0
Training	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0

Return to top

Pending complaints filed in previous fiscal years by status	Comparative data Previous fiscal year data					Fiscal Year 2015 thru 12/31
	2010	2011	2012	2013	2014	
Total complaints from previous fiscal years	2	10	10	14	13	23
Number complaints pending						
Investigation	0	0	0	0	3	4
Hearing	1	1	6	4	8	11
Final action	0	0	0	0	0	1
Appeal with EEOC Office of Federal Operations	1	1	0	1	2	4
Class Certification with EEOC Office of Federal Operations	0	0	1	4	0	0

Pending complaints filed in previous fiscal years by status	Comparative data Previous fiscal year data					Fiscal Year 2015 thru 12/31
	2010	2011	2012	2013	2014	
District Court	0	0	2	2	0	1

Return to top

Complaint investigations	Comparative data Previous fiscal year data					Fiscal Year 2015 thru 12/2014
	2010	2011	2012	2013	2014	
Pending complaints where investigations exceed required time frames	3	0	2	8	6	1

Return to top

For further information, please contact the Diversity & Inclusion Director.

Diversity & Inclusion Director, Stop 156
Board of Governors of the Federal Reserve System
20th and Constitution Avenue, N.W.
Washington, D.C. 20551

Last update: January 29, 2015

OFFICE OF INSPECTOR GENERAL

Audit Report 2013-AE-B-013

The Board Can Benefit from Implementing an Agency-Wide Process for Maintaining and Monitoring Administrative Internal Control

September 5, 2013

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU

Report Contributors

Silvia Vizcarra, OIG Manager
Brian Murphy, Auditor
Jackie Ogle, Auditor
Amanda Sundstrom, Auditor
Cynthia Gray, Senior OIG Manager for Financial Management and Internal Controls
Melissa Heist, Associate Inspector General for Audits and Evaluations

Abbreviations

Board	Board of Governors of the Federal Reserve System
COSO	Committee of Sponsoring Organizations of the Treadway Commission
FMFIA	Federal Managers' Financial Integrity Act of 1982
GAO	Government Accountability Office
OIG	Office of Inspector General
OMB	Office of Management and Budget

Executive Summary:

The Board Can Benefit from Implementing an Agency-Wide Process for Maintaining and Monitoring Administrative Internal Control

2013-AE-B-013 **September 5, 2013**

Purpose

Our objective for this audit was to determine the processes for establishing, maintaining, and monitoring internal control within the Board of Governors of the Federal Reserve System (Board). We focused on internal control over the effectiveness and efficiency of operations and compliance with laws and regulations, i.e., administrative internal control. Our scope does not include internal control over financial reporting or information systems because the Board issues a management assertion on internal control over financial reporting and complies with the Federal Information Security Management Act of 2002, which requires agencies to establish and maintain an information security program to protect information and information systems.

Background

Internal control is an integral part of managing an organization and is critical to improving organizational effectiveness and accountability. It comprises the plans, methods, and procedures used to meet the organization's mission, goals, and objectives. Internal control is the first line of defense in safeguarding assets and preventing and detecting errors and fraud and, thus, helps organizations achieve desired results through effective stewardship of public resources.

The Federal Managers' Financial Integrity Act of 1982 (FMFIA) requires that each executive agency establish internal accounting and administrative controls in compliance with standards established by the Government Accountability Office and prepare an annual statement on internal control based on an evaluation performed using Office of Management and Budget guidelines. Although the Board is not subject to FMFIA, the Board decided to voluntarily comply with the spirit and intent of FMFIA shortly after its enactment. The Board's approach to FMFIA remains unchanged.

Findings

We found that the Board's divisions have processes for establishing administrative internal control that are tailored to their specific responsibilities. These controls generally utilize best practices and are designed to increase efficiency and react to changing environments. The Board's processes for maintaining and monitoring these controls can be enhanced. Specifically, we found that the Board does not have an agency-wide process for maintaining and monitoring its administrative internal control.

Although the Board is not subject to FMFIA, the Board decided to voluntarily comply with the spirit and intent of FMFIA. The Board's approach to addressing the provisions of FMFIA does not require management to assess and monitor administrative internal control. We believe that an agency-wide process that maintains, monitors, and reports on administrative internal control can assist the Board in effectively and efficiently achieving its mission, goals, and objectives, as well as address the organizational challenges outlined in the Board's 2012–2015 strategic framework.

Recommendation

We recommend that the Chief Operating Officer (COO) designate responsible officials or an office to develop and implement an agency-wide policy and process to more closely follow the spirit and intent of FMFIA and develop a training program to increase staff awareness about maintaining and monitoring administrative internal control.

In its response to a draft of our report, the COO stated that the Board concurred with the recommendation's intent. The COO also stated that the Board has already implemented, or is in the process of implementing, several enhanced administrative processes. He added that, given the priorities and budgetary constraints underlying the Board's new strategic framework, Board management will evaluate whether, and in what form, an agency-wide framework makes sense and will coordinate with the Executive Committee of the Board to implement any additional requirements.

Access the full report: http://www.federalreserve.gov/oig/files/FRB_Administrative_Internal_Control_full_Sep2013.pdf
For more information, contact the OIG at 202-973-5000 or visit http://www.federalreserve.gov/oig.

Summary of Recommendation, OIG Report No. 2013-AE-B-013

Rec. no.	Report page no.	Recommendation	Responsible office
1	10	Designate responsible officials or an office to a. develop and implement an agency-wide policy and process to more closely follow the spirit and intent of the Federal Managers' Financial Integrity Act of 1982. b. develop a training program to increase staff awareness about maintaining and monitoring administrative internal control.	Chief Operating Officer

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

September 5, 2013

MEMORANDUM

TO: Donald Hammond
Chief Operating Officer
Board of Governors of the Federal Reserve System

FROM: Melissa Heist
Associate Inspector General for Audits and Evaluations

SUBJECT: OIG Report No. 2013-AE-B-013: *The Board Can Benefit from Implementing an Agency-Wide Process for Maintaining and Monitoring Administrative Internal Control*

Attached is the Office of Inspector General's (OIG's) final report on the subject audit. We conducted this audit to determine the processes for establishing, maintaining, and monitoring internal control within the Board of Governors of the Federal Reserve System (Board). We focused on internal control over the effectiveness and efficiency of operations and compliance with laws and regulations, i.e., administrative internal control.

We provided you with a copy of our draft report for review and comment. In your response, you stated that you concurred with the intent of our recommendation, and that you planned to evaluate whether, and in what form, an agency-wide framework makes sense and that you will coordinate with the Executive Committee of the Board to implement any additional requirements. The Inspector General Act, as amended, requires that we report in our Semiannual Report to Congress on recommendations for which no management decision has been made. The act defines a management decision as the issuance of a final decision by management concerning its response to audit findings and recommendations, including actions concluded to be necessary. Since your response indicates that you have not yet determined the final actions you will take to address our report's findings we request that you provide to us within 90 calendar days a final management decision describing the actions you have taken or that you plan to take to address our recommendation. We have included your response as appendix B to our report.

We appreciate the cooperation that we received from the Board's Office of the Chief Operating Officer and the divisions with which we met. Please contact Cynthia Gray, Senior OIG Manager, or me if you would like to discuss this report or any related issues.

Attachment

cc: Michelle A. Smith, Office of Board Members
Michael S. Gibson, Division of Banking Supervision and Regulation
Sandra F. Braunstein, Division of Consumer and Community Affairs
William Mitchell, Division of Financial Management
Steven B. Kamin, Division of International Finance
Sharon Mowry, Division of Information Technology
Scott G. Alvarez, Legal Division
William English, Division of Monetary Affairs
Michell Clark, Management Division
Nellie Liang, Office of Financial Stability Policy and Research
Robert deV. Frierson, Office of the Secretary
David Wilcox, Division of Research and Statistics
Louise L. Roseman, Division of Reserve Bank Operations and Payment Systems

Contents

Introduction

Objective

Our objective for this audit was to determine the processes for establishing, maintaining, and monitoring internal control within the Board of Governors of the Federal Reserve System (Board). Our audit focused on the internal control over the effectiveness and efficiency of operations and compliance with laws and regulations, i.e., administrative internal control. Administrative controls address programmatic, operational, and administrative areas. Our scope does not include internal control over financial reporting or information systems because the Board issues a management assertion on internal control over financial reporting and complies with the Federal Information Security Management Act of 2002, which requires agencies to establish and maintain an information security program to protect information and information systems. Additional detail on our scope and methodology is in appendix A.

Background

Internal control is an integral part of managing an organization and is critical to improving organizational effectiveness and accountability. It comprises the plans, methods, and procedures used to meet the organization's mission, goals, and objectives. Internal control is the first line of defense in safeguarding assets and preventing and detecting errors and fraud and, thus, helps organizations achieve desired results through effective stewardship of public resources. Internal control should provide reasonable assurance that the objectives of the organization are being achieved in the following categories: (1) effectiveness and efficiency of operations, (2) reliability of financial reporting, and (3) compliance with applicable laws and regulations.

The Board's long-standing mission is to foster stability, integrity, and efficiency in the nation's monetary, financial, and payment systems in pursuit of optimal macroeconomic performance. In carrying out its mission, the Board has stated that it is continually aware that its operations are supported primarily by public funds, it is accountable and responsive to the public, and it recognizes its obligation to manage resources efficiently and effectively while providing transparency and accountability.[1]

1. The Board is an independent federal government agency that does not receive funding appropriated by Congress. The Federal Reserve System's income is derived primarily from the interest on U.S. government securities that it has acquired through open market operations. After paying its expenses, the Federal Reserve System turns the rest of its earnings over to the U.S. Treasury.

Federal Managers' Financial Integrity Act of 1982

Congress has long recognized the importance that internal control plays in achieving organizational effectiveness and accountability. In 1982, when faced with several highly publicized internal control breakdowns, including disclosures of waste, loss, unauthorized use, and misappropriation of funds across a wide spectrum of government operations, Congress passed the Federal Managers' Financial Integrity Act of 1982 (FMFIA) to help reduce fraud, waste, and abuse, as well as to enhance the management of federal government operations through improved internal control.

FMFIA requires the Government Accountability Office (GAO) to establish internal control standards (*Standards for Internal Control in the Federal Government*) and the Office of Management and Budget (OMB) to issue guidelines (*Circular A-123—Management's Responsibility for Internal Control*) for agencies to follow in assessing and reporting on their internal control. In addition, FMFIA requires that each executive agency establish internal accounting and administrative controls in compliance with GAO's standards and evaluate and report annually on internal control using OMB guidelines.

Under its long-standing legal interpretation, the Board is not required to comply with FMFIA because it is a financially related statute that is made inapplicable to the Board by section 10 of the Federal Reserve Act.[2] However, in 1983, shortly after the enactment of FMFIA, the Board's Controller issued a memorandum to the Board's Staff Director for Management stating that it would be in the Board's best interest to comply with the spirit and intent of FMFIA.[3] The Board's approach to addressing FMFIA was described in this memorandum as well as in later correspondence in 1984 and 1988. The Board's approach to addressing FMFIA remains unchanged since the correspondence from the 1980s.

Standards for Internal Control

In accordance with FMFIA, GAO issued *Standards for Internal Control in the Federal Government* in 1983. To address changes in information technology and financial systems, GAO revised and reissued its standards in November 1999. The revised standards include five standards for internal control and provide the overall framework for establishing and maintaining internal control and for identifying and addressing major performance challenges and areas at greater risk for fraud, waste, abuse, and mismanagement (figure 1).

The revised GAO standards also incorporate the private sector's *Internal Control—Integrated Framework* published by the Committee of Sponsoring Organizations of the Treadway

2. Section 10 of the Federal Reserve Act empowers the Board to "determine and prescribe the manner in which its obligations shall be incurred and its disbursements and expenses allowed and paid." 12 U.S.C. § 244.

3. The positions of Controller and Staff Director for Management no longer exist within the current Board organizational structure.

Commission (COSO).[4] The COSO framework was recently updated to include enhancements and clarifications that are intended to increase ease of use and broaden application. The new COSO framework provides clarity for understanding requirements for effective internal control and expands reporting to include nonfinancial and internal reporting. It also reflects changes in the business and operating environments, including governance oversight, demands and complexities in laws and regulations, and expectations for competencies and accountabilities.

Figure 1: GAO's *Standards for Internal Control in the Federal Government*

Control Environment: Sets a positive and supportive attitude toward internal control and conscientious management.

Risk Assessment: Provides for an assessment of the risks the agency faces from both external and internal sources.

Control Activities: Help ensure that management's directives are carried out.

Information & Communication: Ensure that information is recorded and communicated to management and others within the entity to enable them to carry out their internal control and other responsibilities.

Monitoring: Assesses the quality of internal control performance over time and ensures that the findings of audits and other reviews are promptly resolved.

4. COSO's internal control framework is widely used and recognized as a leading framework for designing, implementing, and evaluating the effectiveness of internal control. It integrates various internal control concepts into a framework in which a common definition is established and control components are identified. COSO's internal control framework was updated in May 2013 with a transition period ending December 15, 2014.

Responsibility for Internal Control

In anticipation of FMFIA's enactment, OMB issued Circular A-123, then titled *Internal Control Systems*, in 1981. In 1982, following FMFIA's enactment, OMB issued the assessment guidelines required by FMFIA. Circular A-123 has been periodically updated over the years and is now titled *Management's Responsibility for Internal Control*. The updated circular emphasizes the need for agencies to integrate and coordinate internal control assessments with other internal control–related activities. The circular provides information on improving the accountability and effectiveness of programs and operations by establishing, assessing, correcting, and reporting on internal control. Internal control guidance can be found in GAO's *Standards for Internal Control in the Federal Government,* OMB's Circular A-123, as well as COSO's *Internal Control—Integrated Framework.* Below are excerpts from those documents.

Establishing Internal Control

Management is responsible for developing and maintaining effective internal control. Management sets the objectives, defines organizational programs and operations, performs risk assessments to identify the most significant areas within those programs and operations, communicates the objectives of internal control to the organization, and implements the control activities to minimize risks. Some examples of internal control activities are

- policies and procedures
- segregation of duties
- reviews by management at the functional or activity level
- appropriate documentation of transactions and internal control
- access restrictions to and accountability for resources and records

As part of this process, management should take systematic and proactive measures to develop and implement appropriate, cost-effective internal control.

While management is responsible for developing and maintaining effective internal control, internal control is accomplished by all personnel in an organization. Internal control recognizes that personnel do not always understand, communicate, or perform consistently. Accordingly, a clear and close linkage must exist between personnel's duties and the way in which they are carried out, as well as between personnel's duties and the organization's objectives. Personnel should know their responsibilities and the limits of their authority. Further, internal control should be clearly documented, and the documentation should be readily available for examination. All documentation and records should be properly managed and maintained.

Maintaining and Monitoring Internal Control

Managers should continually assess and evaluate internal control. Once-effective procedures can become less effective over time, or the application of controls may change. Such changes can result from the arrival of new personnel, the variability of training and supervision, time and resource constraints, or other factors. Monitoring ensures that internal control continues to operate effectively and is accomplished by (1) appropriate personnel assessing the design and

operation of controls on a suitably timely basis and (2) management taking necessary actions to address any issues.

Monitoring can be done through ongoing activities or separate evaluations. Ongoing monitoring occurs during the course of normal operations; separate evaluations of specific processes take place after the processes have been performed. Ongoing monitoring is effective because it is performed on a real-time basis, it reacts dynamically to changing conditions, and it is ingrained in the organization. However, separate evaluations provide an opportunity to consider the continued effectiveness of ongoing monitoring. Therefore, a combination of ongoing monitoring and separate evaluations will usually ensure that the internal control maintains its effectiveness over time.

The final stage of monitoring involves reporting findings and deficiencies on a timely basis to appropriate personnel. Reporting enables the results of monitoring to either confirm previously established expectations about the effectiveness of internal control or highlight identified deficiencies for possible corrective action. The basis for reporting on internal control can include a variety of information sources including Office of Inspector General (OIG) and GAO reports, management reviews, and annual evaluations pursuant to statutory requirements; however, management should use its own judgment to assess and report on internal control and use other sources of information as supplements.

Finding: The Board Does Not Have an Agency-Wide Process for Maintaining and Monitoring Administrative Internal Control

We found that the Board's divisions have processes for establishing administrative internal control that are tailored to their specific responsibilities. These controls generally utilize best practices and are designed to increase efficiency and react to changing environments. A few of the divisions' functional areas formally maintain and monitor their controls. However, the Board's processes for maintaining and monitoring these internal controls can be enhanced. Specifically, we found that the Board does not have an agency-wide process for maintaining, monitoring, and reporting on its administrative internal control. Although the Board is not subject to FMFIA, the Board decided to voluntarily comply with the spirit and intent of FMFIA. The Board's approach to addressing the provisions of FMFIA does not require management to assess and monitor administrative internal control. GAO has emphasized the benefits of internal control, and during our audit we performed benchmarking against other independent agencies that voluntarily follow FMFIA as a best practice. We believe that an agency-wide process that maintains, monitors, and reports on administrative internal control can assist the Board in effectively and efficiently achieving its mission, goals, and objectives, as well as address organizational challenges outlined in the Board's 2012–2015 strategic framework.

The Board Has Not Implemented an Agency-Wide Process for Maintaining and Monitoring Administrative Internal Control

During our audit, we found that the Board's functional areas have processes for establishing internal control. The types of internal controls implemented differ by functional area because they are tailored to their specific responsibilities. For example, we found that some functional areas have implemented automated processes to increase efficiency while others have documented their procedures to ensure consistency as environments may change. In general, we found that functional areas developed their internal controls as they recognized the need to mitigate risks.

Although the Board's divisions have processes for establishing internal controls, we found that the Board does not have an agency-wide process for maintaining, monitoring, and reporting on administrative internal control. A few of the divisions' functional areas do formally maintain and monitor their controls through regular updates to policies and procedures, continuous evaluation of a process, or internal business reviews. For example, functional areas in multiple divisions that are responsible for providing economic analyses to support monetary policy decisionmaking have created a committee to periodically review their process and ensure that it is up-to-date. Other functional areas have set schedules for reviewing their procedures to ensure they are up-to-date. Some of these functional areas maintain and monitor their controls because they are reviewed periodically by outside agencies. Two of these functional areas perform and submit self-assessments to those outside agencies. However, we found that the majority of the functional areas do not formally maintain and monitor their administrative internal controls. The functional areas that do not maintain and monitor their administrative internal controls update them on an

as-needed basis, such as when a process changes or new guidance is issued, rather than as a result of monitoring.

The Board's Approach to Complying with FMFIA in Spirit and Intent Does Not Require Management to Assess and Monitor Administrative Internal Control

In a series of correspondence from 1983 to 1988, the Board stated its intent to comply with the spirit and intent of FMFIA. Since that time, the Board's approach to addressing the provisions of FMFIA has relied on work already being conducted, such as the examination of the Board's financial statements by independent auditors as well as independent reviews by the OIG and GAO. In addition, the Board stated that its approach to meeting the reporting provisions of FMFIA is through reports the Board provides to Congress, such as the Board's annual report and the OIG's semiannual reports. However, this approach does not require any action by the Board's divisions and does not include maintaining, monitoring, and reporting on administrative internal control.

FMFIA guidance states that management has primary responsibility for assessing and monitoring controls associated within their programs and should use other sources as a supplement to, not a replacement for, its own judgment when assessing and reporting on internal control. The guidance also states that continuous monitoring and other periodic assessments should provide the basis for the agency's assessment of its internal control. Therefore, although the OIG and GAO perform independent reviews of the Board's programs and operations, their reports should not replace Board management's own judgment for assessing and reporting on administrative internal control.

Complying with FMFIA Is a Best Practice

GAO has emphasized the benefits of internal control. GAO monitored and reported on initial FMFIA implementation efforts across the government in a series of reports as well as in numerous reports targeting specific agencies and programs. Specifically, GAO reported that agencies noted moderate or better senior management support for a strong internal control review process and for reporting weaknesses identified and making the needed improvements as a result of implementing FMFIA. GAO also reported that federal managers generally perceived that positive impacts, such as improved internal control and program efficiency and effectiveness, have resulted from FMFIA. In February 2005, GAO testified before Congress that controls at agencies had improved and that agencies had implemented logical, cohesive, and coordinated agency-wide approaches to identifying and correcting internal control problems.

During our benchmarking, we met with management at one executive agency that is required to comply with FMFIA (Agency 1) and two independent agencies that voluntarily follow FMFIA as

a best practice (Agency 2 and Agency 3).[5] Management from Agencies 2 and 3 stated to us that they recognize the importance of internal control and therefore decided to follow FMFIA. Both of the agencies stated that accountability was recognized as one of the benefits of following FMFIA. Agency 2 also stated that its FMFIA process allows business units to proactively focus on their areas of highest risk.

We found only minor differences in the approach of the agency required to comply with FMFIA as compared with the agencies that voluntarily follow FMFIA. Specifically, we found that all three agencies have developed an agency-wide process for evaluating and reporting on internal control. For example, all three agencies have designated officials responsible for FMFIA compliance at the agency level. Within these agencies, each business unit performs internal control reviews and provides an assurance statement to the head of the agency concerning the adequacy of their internal control, including deficiencies identified during their assessments. In addition, using the assurance statements provided by the business units, the heads of each of the three agencies publicly issue a consolidated assurance statement on the adequacy of the agency's internal control. One of the agencies that voluntarily follows FMFIA has also implemented a policy for FMFIA compliance and has established a senior oversight council. The other agency stated that it is planning to implement a policy for FMFIA compliance and establish a senior oversight council in the near future. Both agencies placed great emphasis on the importance of educating their staffs regarding internal control.

A comparison of the FMFIA implementation approaches of the benchmarked agencies is in table 1.

Table 1: Benchmarking Summary, FMFIA Section 2[a]

FMFIA Implementation	Agency 1	Agency 2	Agency 3
Required to comply with FMFIA	Yes	No	No
Designated officials responsible for FMFIA compliance	Yes	Yes	Yes
Developed an agency-wide policy regarding FMFIA compliance	Yes	Yes	No[b]
Established an oversight council	Yes	Yes	No[c]
Conduct internal control reviews and program evaluations of the business lines	Yes	Yes	Yes
Provide an assurance statement concerning the adequacy of business units' internal control to the agency head	Yes	Yes	Yes
Include all the deficiencies identified throughout the unit in the assurance letter, which is forwarded to the agency head	Yes	Yes	Yes
Publicly issues an annual assurance statement	Yes	Yes	Yes

Source: OIG compilation of benchmarking results.

[a]Section 2 of FMFIA deals with accounting and administrative internal controls.
[b]During our interview, agency officials stated that they were planning to develop an agency policy for FMFIA compliance.
[c]During our interview, agency officials stated that they were planning to create an oversight council in the future.

5. Agency 1 is required to comply with FMFIA and was included in our benchmarking to gain an understanding of how an executive agency implemented FMFIA. This agency was used as the basis of comparison to the agencies that voluntarily comply with FMFIA.

Maintaining and Monitoring Administrative Internal Control Can Help the Board Achieve Its Mission, Goals, and Objectives

Maintaining and monitoring administrative internal control can help the Board respond to shifting environments and evolving demands and priorities by ensuring that the control activities being used are effective and updated when necessary. While the Board's broad mission of fostering stability, integrity, and efficiency in the nation's monetary, financial, and payment system remains essentially unchanged, the 2007–2009 financial crisis fundamentally changed how the Board operates within its functional disciplines. To address these changes, the Board developed a strategic framework for 2012–2015 that addresses the most critical organizational challenges, such as retaining the right mix of skills and expertise, data governance, and facilities upgrades. As the Board's programs change to meet the strategic framework goals, established control activities can become less effective due to changing conditions. Maintaining and monitoring established control activities to address organizational challenges can help the Board ensure that the internal controls implemented are adequately designed and continue to work over time and that control failures and risks are identified, corrected, and mitigated on a timely basis.

We believe that an agency-wide process for maintaining, monitoring, and reporting on internal control can assist the Board in achieving its mission, goals, and objectives; lead to organizational efficiencies; and help avoid and address potential and actual problems that might prevent the Board from carrying out its mission effectively and efficiently or complying with laws and regulations. Prior OIG work products have identified internal control weaknesses at the Board, including noncompliance with policies and procedures, inadequate access control, and the premature release of confidential information. Although these internal control weaknesses did not prevent the Board from carrying out its mission or achieving its strategic objectives, they introduced operational and reputational risks. An agency-wide process for maintaining and monitoring administrative internal control can allow the Board to (1) identify and prevent or correct internal control weaknesses in a timely manner; (2) reduce costs because problems are identified and addressed in a proactive, rather than reactive, manner; (3) produce more accurate and reliable information for use in decisionmaking; and (4) provide periodic assertions on the effectiveness of internal control.

Conclusion

Recognizing the importance of FMFIA, the Board decided to voluntarily comply with the spirit and intent of the legislation. However, the Board's approach to FMFIA compliance does not include an agency-wide process for evaluating and reporting on administrative internal control. During our benchmarking, we found that other agencies that are not required to follow FMFIA have developed an agency-wide process for evaluating and reporting on administrative internal control. Maintaining and monitoring administrative internal control can provide management with reasonable assurance that the Board is effectively and efficiently achieving its mission, goals, and objectives and complying with laws and regulations. We believe an agency-wide approach that more closely follows and addresses the spirit and intent of FMFIA would allow the Board to maximize the benefit from its internal control and could contribute to the Board's ongoing commitment to accountability and effective and efficient operations.

Recommendation

We recommend that the Chief Operating Officer

1. Designate responsible officials or an office to

   a. develop and implement an agency-wide policy and process to more closely follow the spirit and intent of FMFIA.

   b. develop a training program to increase staff awareness about maintaining and monitoring administrative internal control.

Management's Response

Regarding our recommendation, the Board's Chief Operating Officer (COO) stated the following:

> Concur with the recommendation's intent. We agree that effectively establishing, maintaining, and monitoring administrative internal controls can assist the Board in achieving its goals and objectives and in complying with laws and regulations. We also agree that there are opportunities to enhance our current practices related to administrative internal controls. To that end, we have already implemented, or are in the process of implementing, several enhanced administrative processes. For example, we are establishing within the Division of Financial Management a central tracking point for all audit, inspection, evaluation, or other similar reports pertaining to any Board functional area. This will allow us to better monitor findings across the organization and identify trends and opportunities to more broadly strengthen administrative internal controls. We have also established a comprehensive process for regularly reviewing and updating all of our management policies to ensure that the policies and the underlying practices and associated controls remain up-to-date; I receive regular reports on the status of this activity.
>
> The audit report notes that shortly after FMFIA was enacted, as well as in later correspondence in 1984 and 1988, staff recommended that the Board comply with the spirit and intent of FMFIA. It is unclear, however, from this correspondence whether the Board officially adopted this recommendation or exactly what staff intended in establishing a FMFIA-compliant program. Given the priorities and budgetary constraints underlying the Board's new strategic framework, we believe that creating additional infrastructure to develop and implement policies and processes, to include developing a training program, must be carefully balanced with other competing resource priorities. We will evaluate whether, and in what form, an agency-wide framework makes sense and coordinate with the Executive Committee of the Board to implement any additional requirements.

OIG Comment

The COO acknowledged that there are opportunities to enhance the Board's current practices related to administrative internal controls and provided two examples of enhancements that have been implemented or are in the process of being implemented. The COO stated that the Board has established a comprehensive process for regularly reviewing and updating all management policies. We agree that this is a method of maintaining and monitoring internal control over those management policies; however, this process addresses only one of the Board's functions. We believe that this is a good example of a method by which other functional areas in other divisions can keep their policies and procedures up to date. In addition, the COO stated that the Division of Financial Management is establishing a central tracking point for all audit, inspection, evaluation, and other similar reports. While a tracking system will assist the Board in monitoring the areas that have been reviewed by others, FMFIA and COSO guidance state that management should continually assess and evaluate internal control and should use other sources as a supplement to, not as a replacement for, its own judgment when assessing and reporting on internal control.

The COO also stated in his response that it is unclear whether the Board officially adopted a staff recommendation included in the correspondence from the 1980s to comply with the spirit and intent of FMFIA. Further, the COO stated in his response that it is unclear what the staff recommendation intended regarding the establishment of a FMFIA-compliant program. While we did not find evidence that the Board officially adopted a staff recommendation to comply with the spirit and intent of FMFIA, correspondence from the 1980s from the Vice Chairman of the Board and others indicate support for complying with the spirit and intent of FMFIA.

Concerning our audit recommendation, the COO stated that implementing policies and processes, to include developing a training program, must be balanced with other competing resource priorities as detailed in the Board's new strategic framework. He plans to evaluate whether, and in what form, an agency-wide framework makes sense and coordinate with the Executive Committee of the Board to implement any additional requirements. We recognize that the Board has priorities and resource constraints, but we believe that an agency-wide process for maintaining and monitoring administrative internal control can help the Board manage changes that may result from implementing the strategic framework and further the Board's goal of increasing the efficiencies of its operations. As we stated in our report, change can decrease the effectiveness of the Board's control activities. Therefore, maintaining and monitoring established control activities to address organizational challenges can help the Board ensure that the internal controls implemented are adequately designed and continue to work over time and that control failures and risks are identified, corrected, and mitigated in a timely manner. Based on our benchmarking and the emphasis on the benefits of internal control throughout the federal government, we strongly believe it is in the Board's best interest to more closely follow the spirit and intent of FMFIA.

The Inspector General Act, as amended, requires that we report in our Semiannual Report to Congress on recommendations for which no management decision has been made. The act defines a management decision as the issuance of a final decision by management concerning its response to audit findings and recommendations, including actions concluded to be necessary. Since the COO's response indicated that he had not yet determined the final actions he would take to address our report's findings, we are requesting that he provide us within 90 calendar days a final management decision describing the actions taken or planned to address our recommendation.

Appendix A
Scope and Methodology

To accomplish our objective, we reviewed FMFIA and applicable guidance, including GAO's *Standards for Internal Control in the Federal Government*, GAO's Internal Control and Management Evaluation Tool, OMB Circular A-123, and COSO publications. We also reviewed previous audit reports issued by our office as well as by GAO.

We met with personnel in 12 of the 14 Board divisions to provide background information on internal control and the process for maintaining and monitoring internal control, and to gain a high-level understanding of administrative internal control processes in place in the divisions.[6] Following the initial meetings, the divisions provided the audit team with points of contact in a variety of functional areas in each of the divisions. The audit team held over 70 meetings across the 12 divisions, including follow-up meetings with points of contact in functional areas for each division, to determine their administrative internal control processes. We then reviewed documentation of those administrative internal controls. Although we reviewed the internal control documentation, we did not test any of the controls in place nor did we make a determination on the adequacy of the controls.

We discussed the process for establishing internal control with selected functional areas. We also benchmarked with three federal agencies to gain an understanding of their processes for maintaining and monitoring their internal controls. One of these agencies is required to comply with FMFIA, while the other two follow it voluntarily.

Our audit addressed section 2 of FMFIA (internal accounting and administrative control) and not section 4 (financial accounting systems). We focused on internal control over the effectiveness and efficiency of operations and compliance with laws and regulations, i.e., administrative controls, because the Board voluntarily complies with Sarbanes-Oxley section 404, which requires management to assert that it is responsible for creating, maintaining, and assessing the effectiveness of internal control over financial reporting. Further, we did not assess internal control over information systems because the Board complies with the Federal Information Security Management Act of 2002, which requires agencies to establish and maintain an information security program and implement controls to protect information and information systems that support the operations and assets of the agency.

We conducted our audit fieldwork from March 2012 to May 2013. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We

6. We did not include the OIG in the scope of this audit because we are not independent with regard to the OIG's internal control activities. We did not meet with the Division of Financial Management because it was created during our fieldwork phase.

believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix B
Management's Response

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
WASHINGTON, DC 20551

OFFICE OF THE
CHIEF OPERATING OFFICER

DATE: July 15, 2013

TO: Melissa Heist

FROM: Don Hammond

SUBJECT: Response to the OIG's OIG Draft Report: *The Board Can Benefit from Implementing an Agency-wide Process for Maintaining and Monitoring Administrative Internal Control*

We appreciate the opportunity to comment on the draft report of the OIG's audit work related to the processes for establishing, maintaining, and monitoring internal control within the Board of Governors of the Federal Reserve System (Board). As the report notes, the Board's divisions have developed processes for establishing administrative internal controls that are tailored to their specific responsibilities. We are pleased that the report found that these controls generally utilize best practices and are designed to increase efficiency and react to changing environments. The following comments provide additional perspective on the report's recommendation and management's planned actions to further enhance our processes.

Recommendation 1: We recommend that the Chief Operating Officer designate responsible officials or an office to:

a. develop and implement an agency-wide policy and process to more closely follow the spirit and intent of the Federal Managers' Financial Integrity Act (FMFIA), and
b. develop a training program to increase staff awareness about maintaining and monitoring administrative internal control.

COO Response:

Concur with the recommendation's intent. We agree that effectively establishing, maintaining, and monitoring administrative internal controls can assist the Board in achieving its goals and objectives and in complying with laws and regulations. We also agree that there are opportunities to enhance our current practices related to administrative internal controls. To that end, we have already implemented, or are in the process of implementing, several enhanced administrative processes. For example, we are establishing within the Division of Financial Management a central tracking point for all audit, inspection, evaluation, or other similar reports pertaining to any Board functional area. This will allow us to better monitor findings across the organization and identify trends and opportunities to more broadly strengthen administrative internal

www.federalreserve.gov

controls. We have also established a comprehensive process for regularly reviewing and updating all of our management policies to ensure that the policies and the underlying practices and associated controls remain up-to-date; I receive regular reports on the status of this activity.

The audit report notes that shortly after FMFIA was enacted, as well as in later correspondence in 1984 and 1988, staff recommended that the Board comply with the spirit and intent of FMFIA. It is unclear, however, from this correspondence whether the Board officially adopted this recommendation or exactly what staff intended in establishing a FMFIA-compliant program. Given the priorities and budgetary constraints underlying the Board's new strategic framework, we believe that creating additional infrastructure to develop and implement policies and processes, to include developing a training program, must be carefully balanced with other competing resource priorities. We will evaluate whether, and in what form, an agency-wide framework makes sense and coordinate with the Executive Committee of the Board to implement any additional requirements.

BC:
Bill Mitchell
Kit Wheatley

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU

HOTLINE

1-800-827-3340

OIGHotline@frb.gov

Report Fraud, Waste, and Abuse

Those suspecting possible wrongdoing may contact the OIG Hotline by mail, e-mail, fax, or telephone.

Office of Inspector General, c/o Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW, Mail Stop K-300, Washington, DC 20551
Attention: OIG Hotline

Fax: 202-973-5044

Questions about what to report?

Visit the OIG website at www.federalreserve.gov/oig
or
www.consumerfinance.gov/oig

No FEAR Act Data

No FEAR Act Notice

PDF (24 KB)

The Notification and Federal Employee Anti-discrimination and Retaliation Act (No FEAR Act) of 2002 increases federal agency accountability for acts of discrimination or reprisal against employees.

The No FEAR Act requires agencies to post on their public websites statistical data relating to equal employment opportunity complaints filed against the respective agencies.

The Federal Reserve Board's public website contains statistical data in accordance with the No FEAR Act.

Information updated as of June 30, 2014

(b) (5)

Complaint activity	Comparative data Previous fiscal year data					Fiscal Year 2014 10/2013 - 6/2014
	2009	2010	2011	2012	2013	
Number of complaints filed	1	7	10	12	6	7
Number of complainants	3	9	17	23	18	21
Repeat filers	0	0	0	0	0	0

Return to top

Complaints by basis Note: Complaints can be filed alleging multiple bases. The sum of the bases may not equal total complaints filed	Comparative data Previous fiscal year data					Fiscal Year 2014 10/2013 - 6/2014
	2009	2010	2011	2012	2013	
Race	1	6	10	16	15	17
Color	0	1	2	3	4	5
Religion	0	0	0	2	2	3
Reprisal	1	2	5	11	8	7
Sex	1	5	8	11	11	11
National origin	1	2	3	3	1	2
Equal Pay Act	0	0	0	1	3	4
Age	3	6	8	15	9	9
Disability	0	3	2	5	2	3
Non EEO	0	0	0	0	0	0

Return to top

Complaints by issue Note: Complaints can be filed alleging multiple issues. The sum of the issues may not equal total complaints filed	Comparative data Previous fiscal year data					Fiscal Year 2014 10/2013 - 6/2014
	2009	2010	2011	2012	2013	
Appointment/hire	0	0	0	0	0	1
Assignment of duties	0	2	3	4	4	4

Awards	0	0	0	0	0	0
Conversion to full-time	0	0	0	0	0	0
Disciplinary action						
Demotion	0	0	0	0	0	0
Reprimand	0	0	0	1	2	3
Removal	0	2	2	2	1	3
Suspension	0	0	0	0	0	0
Other	0	0	0	1	1	0
Duty hours	0	1	0	0	0	1
Evaluation appraisal	1	1	2	4	3	4
Examination/test	0	0	0	0	0	0
Harassment						
Nonsexual	0	4	8	11	10	12
Sexual	0	1	2	1	1	0
Medical examination	0	0	0	0	0	0
Pay (including overtime)	0	1	1	1	3	4
Promotion/nonselection	2	5	6	10	10	11
Reassignment						
Denied	0	0	0	0	0	0
Directed	0	0	0	0	0	0
Reasonable accommodation	0	1	1	3	2	3
Reinstatement	0	0	0	0	0	0
Retirement	0	0	0	0	0	0
Termination	0	0	2	2	0	0
Terms/conditions of employment	0	2	2	9	5	6
Time and attendance	0	0	0	0	0	0
Training	0	0	0	0	1	1
Other	0	3	4	1	2	3

Return to top

Processing time	Comparative data Previous fiscal year data					Fiscal Year 2014 10/2013 - 6/2014
	2009	2010	2011	2012	2013	
Complaints pending during fiscal year						
Average number of days in investigation stage	209	68	151	133	228	136
Average number of days in final action stage	28	28	36	53	26	0
Complaints pending during fiscal year where hearing was requested						
Average number of days in investigation stage	209	93	183	148	151	100
Average number of days in final action stage	28	28	36	47	27	0
Complaints pending during fiscal year where hearing was not requested						
Average number of days in investigation stage	0	67	0	93	220	317
Average number of days in final action stage	0	62	0	92	24	0

Return to top

Complaints dismissed by agency	Comparative data Previous fiscal year data					Fiscal Year 2014 10/2013 - 6/2014
	2009	2010	2011	2012	2013	
Total complaints dismissed by agency	0	0	1	0	1	0
Average days pending prior to dismissal	0	0	531	0	27	0
Complaints withdrawn by complainants						
Total complaints withdrawn by complainants	1	0	0	1	1	1

Return to top

Total final actions finding discrimination	Comparative data Previous fiscal year data					Fiscal Year 2014 10/2013 - 6/2014
	2009	2010	2011	2012	2013	

	#	%	#	%	#	%	#	%	#	%	#	%
Total number findings	0		0		0		0		0		0	
Without hearing	0	0	0	0	0	0	0	0	0	0	0	0
With hearing	0	0	0	0	0	0	0	0	0	0	0	0

Return to top

Findings of discrimination rendered by basis	Comparative data Previous fiscal year data										Fiscal Year 2014 10/2013 - 6/2014	
Note: Complaints can be filed alleging multiple bases. The sum of the bases may not equal total complaints and findings	2009		2010		2011		2012		2013			
	#	%	#	%	#	%	#	%	#	%	#	%
Total number findings	0		0		0		0		0		0	
Race	0	0	0	0	0	0	0	0	0	0	0	0
Color	0	0	0	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0	0	0	0
Reprisal	0	0	0	0	0	0	0	0	0	0	0	0
Sex	0	0	0	0	0	0	0	0	0	0	0	0
National orgin	0	0	0	0	0	0	0	0	0	0	0	0
Equal Pay Act	0	0	0	0	0	0	0	0	0	0	0	0
Age	0	0	0	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0	0	0	0
Non EEO	0	0	0	0	0	0	0	0	0	0	0	0
Findings after hearing	0		0		0		0		0		0	
Race	0	0	0	0	0	0	0	0	0	0	0	0
Color	0	0	0	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0	0	0	0
Reprisal	0	0	0	0	0	0	0	0	0	0	0	0
Sex	0	0	0	0	0	0	0	0	0	0	0	0
National orgin	0	0	0	0	0	0	0	0	0	0	0	0
Equal Pay Act	0	0	0	0	0	0	0	0	0	0	0	0
Age	0	0	0	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0	0	0	0
Non EEO	0	0	0	0	0	0	0	0	0	0	0	0
Findings without hearings	0		0		0		0		0		0	
Race	0	0	0	0	0	0	0	0	0	0	0	0
Color	0	0	0	0	0	0	0	0	0	0	0	0
Religion	0	0	0	0	0	0	0	0	0	0	0	0
Reprisal	0	0	0	0	0	0	0	0	0	0	0	0
Sex	0	0	0	0	0	0	0	0	0	0	0	0
National orgin	0	0	0	0	0	0	0	0	0	0	0	0
Equal Pay Act	0	0	0	0	0	0	0	0	0	0	0	0
Age	0	0	0	0	0	0	0	0	0	0	0	0
Disability	0	0	0	0	0	0	0	0	0	0	0	0
Non EEO	0	0	0	0	0	0	0	0	0	0	0	0

Return to top

Findings of discrimination rendered, by issue	Comparative data Previous fiscal year data										Fiscal Year 2014 10/2013 - 6/2014	
	2009		2010		2011		2012		2013			
	#	%	#	%	#	%	#	%	#	%	#	%
Total number findings	0		0		0		0		0		0	
Appointment/hire	0	0	0	0	0	0	0	0	0	0	0	0
Assignment of duties	0	0	0	0	0	0	0	0	0	0	0	0
Awards	0	0	0	0	0	0	0	0	0	0	0	0
Conversion to full-time	0	0	0	0	0	0	0	0	0	0	0	0
Disciplinary action	0	0	0	0	0	0	0	0	0	0	0	0
Demotion	0	0	0	0	0	0	0	0	0	0	0	0
Reprimand	0	0	0	0	0	0	0	0	0	0	0	0

Suspension	0	0	0	0	0	0	0	0	0	0	0	0
Removal	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0
Duty hours	0	0	0	0	0	0	0	0	0	0	0	0
Evaluation appraisal	0	0	0	0	0	0	0	0	0	0	0	0
Examination/test	0	0	0	0	0	0	0	0	0	0	0	0
Harassment	0	0	0	0	0	0	0	0	0	0	0	0
Nonsexual	0	0	0	0	0	0	0	0	0	0	0	0
Sexual	0	0	0	0	0	0	0	0	0	0	0	0
Medical examination	0	0	0	0	0	0	0	0	0	0	0	0
Pay (including overtime)	0	0	0	0	0	0	0	0	0	0	0	0
Promotion/nonselection	0	0	0	0	0	0	0	0	0	0	0	0
Reassignment	0	0	0	0	0	0	0	0	0	0	0	0
Denied	0	0	0	0	0	0	0	0	0	0	0	0
Directed	0	0	0	0	0	0	0	0	0	0	0	0
Reasonable accommodation	0	0	0	0	0	0	0	0	0	0	0	0
Reinstatement	0	0	0	0	0	0	0	0	0	0	0	0
Retirement	0	0	0	0	0	0	0	0	0	0	0	0
Termination	0	0	0	0	0	0	0	0	0	0	0	0
Terms/conditions of employment	0	0	0	0	0	0	0	0	0	0	0	0
Time and attendance	0	0	0	0	0	0	0	0	0	0	0	0
Training	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0
Findings after hearings	**0**		**0**		**0**		**0**		**0**		**0**	
Appointment/hire	0	0	0	0	0	0	0	0	0	0	0	0
Assignment of duties	0	0	0	0	0	0	0	0	0	0	0	0
Awards	0	0	0	0	0	0	0	0	0	0	0	0
Conversion to full-time	0	0	0	0	0	0	0	0	0	0	0	0
Disciplinary action	0	0	0	0	0	0	0	0	0	0	0	0
Demotion	0	0	0	0	0	0	0	0	0	0	0	0
Reprimand	0	0	0	0	0	0	0	0	0	0	0	0
Suspension	0	0	0	0	0	0	0	0	0	0	0	0
Removal	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0
Duty hours	0	0	0	0	0	0	0	0	0	0	0	0
Evaluation appraisal	0	0	0	0	0	0	0	0	0	0	0	0
Examination/test	0	0	0	0	0	0	0	0	0	0	0	0
Harassment	0	0	0	0	0	0	0	0	0	0	0	0
Nonsexual	0	0	0	0	0	0	0	0	0	0	0	0
Sexual	0	0	0	0	0	0	0	0	0	0	0	0
Medical examination	0	0	0	0	0	0	0	0	0	0	0	0
Pay (including overtime)	0	0	0	0	0	0	0	0	0	0	0	0
Promotion/nonselection	0	0	0	0	0	0	0	0	0	0	0	0
Reassignment	0	0	0	0	0	0	0	0	0	0	0	0
Denied	0	0	0	0	0	0	0	0	0	0	0	0
Directed	0	0	0	0	0	0	0	0	0	0	0	0
Reasonable accommodation	0	0	0	0	0	0	0	0	0	0	0	0
Reinstatement	0	0	0	0	0	0	0	0	0	0	0	0
Retirement	0	0	0	0	0	0	0	0	0	0	0	0
Termination	0	0	0	0	0	0	0	0	0	0	0	0
Terms/conditions of employment	0	0	0	0	0	0	0	0	0	0	0	0
Time and attendance	0	0	0	0	0	0	0	0	0	0	0	0
Training	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0
Findings without hearing	**0**		**0**		**0**		**0**		**0**		**0**	
Appointment/hire	0	0	0	0	0	0	0	0	0	0	0	0
Assignment of duties	0	0	0	0	0	0	0	0	0	0	0	0
Awards	0	0	0	0	0	0	0	0	0	0	0	0
Conversion to full-time	0	0	0	0	0	0	0	0	0	0	0	0
Disciplinary action	0	0	0	0	0	0	0	0	0	0	0	0

Demotion	0	0	0	0	0	0	0	0	0	0	0	0
Reprimand	0	0	0	0	0	0	0	0	0	0	0	0
Suspension	0	0	0	0	0	0	0	0	0	0	0	0
Removal	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0
Duty hours	0	0	0	0	0	0	0	0	0	0	0	0
Evaluation appraisal	0	0	0	0	0	0	0	0	0	0	0	0
Examination/test	0	0	0	0	0	0	0	0	0	0	0	0
Harassment	0	0	0	0	0	0	0	0	0	0	0	0
Nonsexual	0	0	0	0	0	0	0	0	0	0	0	0
Sexual	0	0	0	0	0	0	0	0	0	0	0	0
Medical examination	0	0	0	0	0	0	0	0	0	0	0	0
Pay (including overtime)	0	0	0	0	0	0	0	0	0	0	0	0
Promotion/nonselection	0	0	0	0	0	0	0	0	0	0	0	0
Reassignment	0	0	0	0	0	0	0	0	0	0	0	0
Denied	0	0	0	0	0	0	0	0	0	0	0	0
Directed	0	0	0	0	0	0	0	0	0	0	0	0
Reasonable accommodation	0	0	0	0	0	0	0	0	0	0	0	0
Reinstatement	0	0	0	0	0	0	0	0	0	0	0	0
Retirement	0	0	0	0	0	0	0	0	0	0	0	0
Termination	0	0	0	0	0	0	0	0	0	0	0	0
Terms/conditions of employment	0	0	0	0	0	0	0	0	0	0	0	0
Time and attendance	0	0	0	0	0	0	0	0	0	0	0	0
Training	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	0	0	0

Return to top

(b) (5)

Pending complaints filed in previous fiscal years, by status	Comparative data Previous fiscal year data					Fiscal Year 2014 10/2013 - 6/2014
	2009	2010	2011	2012	2013	
Total complaints from previous fiscal years	2	2	10	13	14	14
Number of complaints pending						
Investigation	0	0	0	0	4	3
Hearing	1	1	6	4	7	9
Final action	0	0	0	1	0	0
Appeal with EEOC Office of Federal Operations	1	1	1	2	2	1
Class Certification with EEOC Office of Federal Operations	0	0	1	4	0	0
District Court	0	0	2	2	1	1

Return to top

Complaint investigations	Comparative data Previous fiscal year data					Fiscal Year 2014 10/2013 - 6/2014
	2009	2010	2011	2012	2013	
Pending complaints where investigations exceed required time frames	2	3	0	2	8	7

Return to top

For further information, please contact the Diversity & Inclusion Director.

Diversity & Inclusion Director, Stop 156
Board of Governors of the Federal Reserve System
20th and Constitution Avenue, N.W.
Washington, D.C. 20551

(b) (5)

Last update: August 26, 2014

Report to the Congress on the Office of Minority and Women Inclusion

March 2012

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

Report to the Congress on the Office of Minority and Women Inclusion

March 2012

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

To order additional copies of this or other Federal Reserve Board publications, contact:

Publications Fulfillment
Mail Stop N-127
Board of Governors of the Federal Reserve System
Washington, DC 20551
(ph) 202-452-3245
(fax) 202-728-5886
(e-mail) Publications-BOG@frb.gov

This and other Federal Reserve Board reports are also available online at
www.federalreserve.gov/boarddocs/rptcongress/default.htm.

Preface: Implementing the Dodd-Frank Act

The Board of Governors of the Federal Reserve System (the Board) is responsible for implementing numerous provisions of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank Act). The Dodd-Frank Act requires, among other things, that the Board produce reports to the Congress on a number of potential reform topics.

Pursuant to section 342(e) of the Dodd-Frank Act, Sheila Clark, director of the Board's Office of Diversity and Inclusion, submits this first annual report to the Congress outlining the activities, successes, and challenges of the office.

See the Board's website for an overview of the Dodd-Frank Act regulatory reform effort (www.federalreserve.gov/newsevents/reform_about.htm) and a list of the implementation initiatives recently completed by the Board as well as several of the most significant initiatives that the Board expects to address in the future (www.federalreserve.gov/newsevents/reform_milestones.htm).

Contents

Introduction

In January 2011, pursuant to section 342 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), the Board of Governors of the Federal Reserve System (the Board) established its Office of Diversity and Inclusion (ODI). The ODI builds on the Board's long-standing efforts to promote equal employment opportunity and diversity and to foster diversity in procurement. The Board has welcomed the new requirements under section 342 as a complement to its existing efforts as well as an opportunity to strengthen those efforts.

The ODI's mission and scope include the responsibilities identified in section 342 for the Office of Minority and Women Inclusion, as well as Equal Employment Opportunity (EEO) compliance and programs and initiatives addressing diversity and inclusion more generally (for example, inclusion of persons with disabilities).

Employment of Minorities and Women

The Board is committed to fostering an inclusive work environment where diversity is respected and leveraged to better serve the agency's mission. The Board has a long-standing equal employment policy and makes significant efforts to recruit and retain a staff that is diverse and inclusive. The best ideas, decisionmaking, and ultimately, service to the public are born from diverse perspectives.

Equal Employment Opportunity Policies

The Board's Equal Employment Program, which is housed within the ODI, strives to meet the "Essential Elements of a Model EEO Program" as prescribed in the Equal Employment Opportunity Commission's (EEOC) Management Directive 715 (MD-715). The Board has formal policies regarding equal employment opportunity, reasonable accommodation, and sexual harassment; and the EEO Program undertakes training and analysis to ensure that the Board complies with all applicable laws and regulations. The Board uses MD-715 (which includes an annual barrier analysis) as the primary metric to assess the effectiveness of its diversity policies. In addition, the Board conducts an impact analysis on employment transaction data (i.e., hires and promotions) and a complaint trend analysis. Each operational division has an EEO liaison who works with the ODI to address recruitment and retention issues specific to the liaison's division. The ODI, in conjunction with each EEO liaison, monitors progress on increasing workforce diversity.

The Board submits an EEO Program Status Report based on the requirements of MD-715 annually to the EEOC, as required by law. As part of that report, the Board provides the EEOC with an EEO-1 Report on workforce demographics. The EEO-1 Report is available on the Board's public website: www.federalreserve.gov/aboutthefed/diversityinclusion.htm. The Board's EEO-1 Report for calendar year 2011 is also appended to this report as appendix A. In general, the Board compares favorably to the federal government in workforce diversity, with an overall workforce that is approximately 46 percent female, 27 percent African American, 12 percent Asian, and 4 percent Hispanic. Within the ranks of Board officials and managers, approximately 44 percent are female, 15 percent are African American, 6 percent are Asian, and 2 percent are Hispanic. Recruitment and retention of Hispanics has been a strategic objective for the Board. We have made some progress in recent years; the Hispanic workforce has increased from 3.70 percent in 2010 to 4.02 percent in 2011.

The Board reviews the diversity profile of its workforce and applicant pool periodically, comparing against census availability data for major occupations. The following have been implemented based on the reviews and comparisons of our workforce against census availability data for major occupations:

- identification of effective recruitment resources to increase diversity in the applicant pool;
- development of recruitment outreach action plans;
- increased participation by divisions in summer internships and recruitment at minority and female professional career fairs; and
- mentoring and career development activities to increase the pipeline to senior professional, managerial, and official staff (i.e., its officers) positions.

To further strengthen its diversity, EEO, and inclusion policies and practices, the Board is a member of organizations that provide research, benchmarking, exchange of diversity best practices, and networking opportunities. The Board has participated in benchmarking surveys conducted by the Conference Board, the Society for Human Resource Management, the Organization Resource Network Council, the Equal Employment Advisory Council, and the Federal Inter-Agency Diversity Partnership. Board

staff have also served on committees and workgroups focusing on diversity and EEO topics.

Recruitment and Retention

The Board uses a variety of recruitment methods depending on the role, level, and grade of the position. Different divisions also may use different recruitment methods based on specialty skill sets needed. Methods of recruitment include, but are not limited to, posting positions on job boards, placing advertisements in targeted minority and female publications (such as *IMDiversity, Hispanic Business,* and *Careers & the Disabled*), and announcing job opportunities with industry, trade, and minority and female professional organizations. The Board also works with career placement offices at colleges and universities. Organizations such as the American Economic Association and the Urban Financial Services Association provide access to applicants for positions critical to meet the Board's mission. The Board has found that including hiring managers at recruitment events enhances recruiting effectiveness, and it has increased its use of this technique in recent years. Also, in order to increase diversity in candidate pools for executive positions, the Board at times uses external minority and female recruiting search firms. In addition, the Board has a summer intern program that provides an opportunity for students to work in a variety of Board positions, including financial analyst, information technology (IT), economic research, and business management. Summer intern applicants are sourced from colleges, universities, and diversity organizations, including INROADS and the Hispanic Association of Colleges and Universities.

To assess the effectiveness of the different recruitment channels and strategies in achieving a diverse applicant pool, the Board performs applicant tracking reviews to determine the diversity of applicant pools, interviewees, and hire results based on interviews. Information derived from program assessments is used to improve diversity outreach and recruitment efforts at colleges, universities, and professional career fairs. The ODI similarly monitors the retention of minorities and women by role, level, and grade. Where issues are identified in hiring or retention, meetings are held with management in the specific division. This enables the ODI to address issues and/or trends that adversely impact the Board's policies and practices pertaining to EEO.

Training and Mentoring

The Federal Reserve System and the Board sponsor the Federal Reserve System Leadership Exchange Program. This program, in conjunction with customized division mentoring programs, enables participants to develop depth and breadth of skills and experiences in their careers. Exchange assignments come in many forms, ranging from a short-term job shadow to a long-term critical project or a specialized experience tailored to support an individual's development goals. The exchange and mentoring programs provide hands-on learning; promote exposure to different functions, experiences, and cross-System opportunities; and expand cross-System and cross-function networks and visibility.

Further, the Board has implemented an apprenticeship program to provide employees in job families with limited potential for advancement the opportunity to receive classroom and on-the-job training in order to develop careers in skilled trades.

In addition, the Board has provided training in classroom and web-based formats. The following are examples of diversity training and education activities that have been offered to official staff and employees: Leading in an Environment of Diversity, Working in an Environment of Diversity, Workplace Harassment, Conflict Resolution, and Leadership Competencies. The ODI plans to increase its training activities in 2012 and going forward.

Successes

An ongoing focus of the Board is to increase diversity in the official staff. In 2011, the Board increased its official staff by 14 positions, of which 3, or more than 21 percent, were minorities. In addition, 17 Hispanics were hired in job categories with low Hispanic participation. Further, the Board's increased outreach efforts resulted in more diverse applicant pools for a number of positions.

Challenges

Despite some progress, the Board continues to have low minority representation in the economist job family. The Board hires a large number of Ph.D. economists, and the availability of minority candi-

dates for these positions is low. To address this challenge, the Board participates in educational forums and is a member of the American Economic Association's Committee on the Status of Minority Groups in the Economics Profession.

The Board also identified the need to enhance diversity in the pool of applicants for key functions such as financial analysis, IT, middle management, and senior professional positions. In response, the Board enhanced its recruitment outreach efforts for these positions by targeting recruitment venues with a more diversified applicant pool. The Board also included hiring managers at recruitment fairs with high participation by black and Hispanic MBAs, attorneys, and IT professionals. In addition, the Board has enhanced its advertisement of career opportunities in minority and female conference publications. These activities resulted in a more diverse applicant pool.

Inclusion of Minority-Owned and Women-Owned Businesses

The Procurement Section of the Board's Management Division, working with the ODI, is responsible for implementing section 342 of the Dodd-Frank Act in connection with developing standards and procedures to ensure, to the extent possible, the fair inclusion and utilization of minority- and women-owned businesses in the Board's procurement process. The ODI and the Procurement Section meet on a regular basis to assess the results of the supplier diversity objectives and activities and to determine whether additional efforts would be helpful in assisting minority- and women-owned businesses to compete successfully in the Board's acquisition process.

Currently, the Board continues to operate under its small disadvantaged business acquisition policy, which existed prior to the enactment of the Dodd-Frank Act. That policy helps to ensure that small and socially and economically disadvantaged businesses have an equitable opportunity to compete in the Board's procurement activities. To further enhance the Board's Small and Disadvantaged Business Development Program and to support the ODI's goals and objectives, the Procurement Section is in the process of implementing a supplier diversity program. Under the program, as required by section 342, the Board's general contract provisions will include standard language that requires contractors to confirm their commitment to ensuring the fair inclusion of women and minorities in employment and contracting. In addition, during the solicitation phase, the program will allow prospective vendors to submit a subcontracting plan with their proposal. With the adoption of the supplier diversity policy, the Board is confident that its vendor selection processes will encourage and support the participation of minority- and women-owned businesses.

Access Initiatives

In 2011, a supplier diversity specialist was hired to develop a comprehensive program strategy, including meetings with prospective suppliers to pre-qualify them and offer technical assistance as needed. By dedicating a full-time staff person to this effort, the Board expects to increase the participation and identification of diverse suppliers in the Board's acquisition process. Procurement staff and the supplier diversity specialist plan to host workshops and other technical assistance activities to assist vendors with the fundamentals of doing business with the Board.

The Board is also working to develop a website that will enable companies to register, identify their business type, and include information regarding their products and services.

Outreach Activities

The Board continues its outreach activities to attract a diverse pool of vendors by holding events to provide vendors an opportunity to meet with procurement staff and the technical end users. These vendor fairs have been well received by the vendors that attend as well as the internal-Board customers that meet one-on-one with potential suppliers. Giving the internal-Board customer an opportunity to meet with potential suppliers prior to starting the solicitation process provides the customer an opportunity to speak with the vendors about their qualifications. The Board plans to hold additional events, including workshops and forums for vendors on how to do business with the Board and how to access small business opportunities.

The Board's external strategies to increase contracting opportunities for minority- and women-owned firms focus on developing partnerships with advocacy groups representing minority- and women-owned businesses and organizational memberships. The Board is a member of the Maryland/District of Columbia Minority Supplier Development Council. As a member, the Board uses the Council's vendor database to find qualified suppliers to invite to out-

reach activities and to include in the bidding process for contracts with the Board. The Board is also applying for membership in the Women's Business Enterprise National Council, which hosts networking events focused on supplier diversity. In addition, the Board has met with advocacy groups, such as the Greenlining Institute, to discuss the inclusion of minority businesses in products and services contracts.

The Board also attends external vendor outreach events, such as the annual procurement conference sponsored by the Office of Small Disadvantaged Business Utilization in Washington, D.C., local and national conferences of the Minority Supplier Development Council, and the national conference of the Women's Business Enterprise National Council. In 2012, the Board plans to participate in a number of trade shows, such as the Minority Enterprise Development Week, D.C. Small Business Expo, the National Association of Women Business Owners, the U.S. Chamber of Commerce Business Summit, the U.S. Pan American Expo, the New York Small Business Expo, and the trade show held in conjunction with the Congressional Black Caucus annual conference.

Successes

As mentioned earlier in the report, the Procurement Section hired a supplier diversity specialist to enhance outreach activities and to focus the Board's efforts toward increasing the number of minority- and women-owned businesses involved in the Board's procurement process.

A separate budget was approved for the supplier diversity program to ensure that the program is adequately funded. As a result, the Board has tripled the number of outreach activities planned for 2012. During 2011, the Board participated in several local and national events designed to identify and educate minority- and women-owned businesses about contracting opportunities at the Board. In addition, the Board hosted its annual vendor fair, which provided the opportunity for minority- and women-owned businesses to meet with procurement staff and end users. These activities resulted in a more diverse pool of qualified minority- and women-owned businesses in the bid process.

Over the past five years, the Board has increased the amount of contracting dollars spent with minority- and women-owned businesses from $8,376,750 in 2007 to $15,414,147 in 2011, representing an increase of 84 percent.

In order to improve the accuracy of information on vendors in our procurement database, we contacted vendors to revalidate their classification and status. More than 90 percent of the vendors responded. This effort will enhance our ability to track and produce accurate reports.

Challenges

As an initial hurdle, the Board's total procurement expenditure is small relative to other federal agencies, and the specific mission of our agency dictates the type of products and services purchased. In particular, the Board spends a significant amount of its overall contracting dollars on purchases of economic data, which are generally not available from minority- or women-owned firms.

A further barrier to competition by minority- and women-owned businesses is the fact that many of these companies have never conducted business with the federal government and have expressed concern that the documentation requirements are an undue burden. The outreach and technical assistance programs described earlier are designed to assist minority- and women-owned businesses in addressing this concern.

In addition, to ensure further participation of minority- and women-owned businesses, it is important to identify ways to foster networking opportunities between prime contractors and minority- and women-owned firms interested in subcontracting opportunities.

Contracts with Minority-Owned and Women-Owned Businesses

The Board tracks the diversity of a company by its business size (small or large) and by its ownership classification (such as minority-owned or women-owned). The Board is more likely to receive a more diverse pool of vendor applications in some areas than others. For example, the Board has encountered a number of diverse vendors in the areas of temporary staffing, IT staffing, IT consulting, and office supplies and furnishings. Conversely, the Board does

not receive a diverse pool of vendor applications from firms that provide economic and statistical data.

During 2011, the Board's procurement contracts for goods and services totaled $125,070,569. Of this total, $15,414,147, or 12.3 percent, was awarded to minority-owned or women-owned businesses. Specific awards by contractor classification are as follows

- minority-owned businesses (excludes women-owned businesses) = $9,028,526 (7.2 percent of total);
- women-owned businesses (excludes minority women) = $4,237,038 (3.4 percent of total); and
- minority women-owned businesses = $2,148,583 (1.7 percent of total).

Financial Literacy Activities

The Board is dedicated to enhancing economic and financial literacy. The financial literacy program provides educational programs and resources for educators and students through workshops, classroom curricula, and other resources related to concepts of economics and personal finance.

In April 2011, Chairman Ben Bernanke provided a statement for the record, for a hearing held by the U.S. Senate Homeland Security and Governmental Affairs Subcommittee on Oversight of Government Management, in which he highlighted the importance of financial literacy to a stable and healthy economy. He also described some of the Federal Reserve System's efforts to help Americans make informed financial decisions. Specifically, the Chairman noted that exposing young people to financial concepts is particularly important and that the Federal Reserve is committed to helping teachers and schools work more effectively with students to develop financial literacy. For example, the Federal Reserve provides a financial and economic education website (federalreserveeducation.org) that features a variety of resources for teachers and students of various ages and knowledge levels.

The Board also participates in community outreach events and programs, examples of which are listed below.

- *Financial Literacy Day on the Hill:* The Board participated in the ninth annual "Financial Literacy Day on the Hill" on April 15, 2011, in the Cannon House Office Building in Washington, D.C. and provided financial publications and education program information to participants.
- *Congressional Black Caucus Annual Legislative Conference:* In September 2011, the Board sponsored a booth at the 41st Annual Legislative Conference. Financial education materials and information on how to access the System's public website for additional information regarding financial literacy were distributed to exhibit fair attendees.
- *FedEd Program:* During the summer of 2010, research assistants from divisions within the Board developed and implemented a program to work with local high-school students to improve understanding of personal financial subjects and the role of the Federal Reserve System in the economy. Subjects covered include budgeting, credit and the time value of money, and the importance of saving. Since the inception of the program, more than a dozen presentations have been made to middle- and high-school students in the Washington metropolitan area. The program is continuing in 2012 with an expanded focus on high schools with high minority and female student populations within the urban communities of Maryland, Virginia, and Washington, D.C.
- *Education and Training Materials Distribution:* During 2011, the Board provided financial literacy materials to the Ready to Achieve Mentoring Program (RAMP), a project of the Institute for Educational Leadership. RAMP is a high-tech, career-focused mentoring program being implemented by organizations across the country to promote employment and continued learning opportunities for underserved, at-risk youth. The Board provided training materials to PEN OR PENCIL: Writing a New History, a program developed by the National Alliance of Faith and Justice and the National CARES Mentoring Movement. The program's goal is to provide mentoring that will assist underserved youth in developing a keen and improved understanding of all aspects of financial literacy.
- *The Jump$tart Coalition for Personal Financial Literacy:* The Board continues to partner with and serve on the Jump$tart Coalition Board of Directors. In its 15-year history, Jump$tart has brought visibility and—through its biennial survey of high-school seniors—research-based data to the financial literacy movement. Jump$tart is a Washington, D.C.-based not-for-profit organization that seeks to improve the personal financial literacy of students in kindergarten through college. The Board

plans to continue its partnership with the Washington, D.C. Jump$tart chapter.

- In the spring of 2012, Chairman Bernanke delivered a four-part lecture series at the George Washington University about the history of the Federal Reserve and its response to the 2007–2009 financial crisis. The series was live-streamed to the public and was available on the Board's public website: www.federalreserve.gov/newsevents/lectures/about.htm.

Going forward, the Board is developing a strategic plan for continued implementation of the goals of section 342. The plan includes a proposal to convene a meeting of senior-level educators from the school systems in the Washington metropolitan area. The purpose of the meeting is to ascertain the goals of the respective school systems as related to expansion of financial education opportunities for the student population and to explore ways that the Board could add value and assist in achieving those goals. The Board will also pursue partnerships with financial education entities such as the Institute for Financial Literacy and the Council for Economic Education. Such partnerships will serve to enhance the Board's ability to develop and deliver the most meaningful financial education products to our partners and our community.

The Board will continue its outreach efforts and will continue to participate in conventions and seminars given by national groups such as the National School Boards Association.

Diversity Policies and Practices of Regulated Entities

Section 342 requires the Board and the other agencies with Offices of Minority and Women Inclusion to develop standards to assess the diversity policies and practices of the entities the agencies regulate. Board staff have met regularly with the staff of other financial regulatory agencies to establish a common framework for compliance with this provision of section 342. The regulatory community believes that a uniform approach is important to ensure that all entities are subject to similar standards regardless of regulator. This is particularly important because some entities are regulated by more than one agency, and conflicting or overlapping expectations could create significant confusion for the industry. The agencies are discussing a variety of approaches to implementing this provision of section 342 in a way that will have maximum impact while limiting regulatory burden and remaining within the constraints of the statutory authorization.

In order to develop a framework for standards that promote good faith efforts for diversity and EEO, the financial regulators hosted a roundtable of financial industry trade groups on February 20, 2012. Approximately 10 industry groups attended. The roundtable discussion focused on how to engage members on leading practices for diversity and EEO. Based on the feedback received, the financial regulators will establish a schedule of roundtable discussions with financial institutions and other regulated entities to further develop standards for the diversity policies and practices of regulated entities.

Appendix A: EEO-1 Report for the Board of Governors of the Federal Reserve System for Calendar Year 2011

Employer Information Report EEO-1

Federal Reserve Board, 2011 Employer Information Report

Occupational Categories	Total Employees			Race/Ethnicity													
						Non- Hispanic or Latino											
				Hispanic or Latino		White		Black or African American		Asian		Native Hawaiian or Other Pacific Islander		American Indian or Alaska Native		Two or More Races	
	All	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female
1.1 Exec. Sr. Lvl Mgrs, Governors, Officers, FR-29 & FR-28																	
By total	343	201	142	3	4	170	107	15	20	11	9	2	1	0	0	0	1
By percent	100.00%	58.60%	41.40%	0.87%	1.17%	49.56%	31.20%	4.37%	5.83%	3.21%	2.62%	0.58%	0.29%	0.00%	0.00%	0.00%	0.29%
1.2 1st/Mid Lvl																	
By total	81	38	43	1	0	19	25	15	16	3	2	0	0	0	0	0	0
By percent	100.00%	46.91%	53.09%	1.23%	0.00%	23.46%	30.86%	18.52%	19.75%	3.70%	2.47%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Officials and Managers Total																	
By total	424	239	185	4	4	189	132	30	36	14	11	2	1	0	0	0	1
By percent	100.00%	56.37%	43.63%	0.94%	0.94%	79.08%	31.13%	7.08%	8.49%	3.30%	2.59%	0.47%	0.24%	0.00%	0.00%	0.00%	0.24%
2. Professionals																	
By total	1,459	775	684	36	37	521	338	80	180	119	114	14	14	1	0	4	1
By percent	100.00%	53.12%	46.88%	2.47%	2.54%	67.23%	23.17%	5.48%	12.34%	8.16%	7.81%	0.96%	0.96%	0.07%	0.00%	0.27%	0.07%
3. Technicians																	
By total	6	2	4	0	0	0	2	2	2	0	0	0	0	0	0	0	0
By percent	0.00%	33.33%	66.67%	0.00%	0.00%	0.00%	33.33%	33.33%	33.33%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
4. Sales Workers																	
By total	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
By percent	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
5. Admin Support Workers																	
By total	154	27	127	1	5	7	12	19	104	0	4	0	0	0	2	0	0
By percent	100.00%	17.53%	82.47%	0.65%	3.25%	4.55%	7.79%	12.34%	67.53%	0.00%	2.60%	0.00%	0.00%	0.00%	1.30%	0.00%	0.00%
6. Craft Workers																	
By total	42	41	1	0	0	23	0	14	1	3	0	1	0	0	0	0	0
By percent	100.00%	97.62%	2.38%	0.00%	0.00%	54.76%	0.00%	33.33%	2.38%	7.14%	0.00%	2.38%	0.00%	0.00%	0.00%	0.00%	0.00%
7. Operatives																	
By total	12	12	0	0	0	1	0	11	0	0	0	0	0	0	0	0	0
By percent	100.00%	100.00%	0.00%	0.00%	0.00%	8.33%	0.00%	91.67%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
8. Laborers and Helpers																	
By total	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
By percent	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
9. Service Workers																	
By total	177	142	35	7	0	47	4	83	29	5	1	0	1	0	0	0	0
By percent	100.00%	80.23%	19.77%	3.95%	0.00%	26.55%	2.26%	46.89%	16.38%	2.82%	0.56%	0.00%	0.56%	0.00%	0.00%	0.00%	0.00%
Total Workforce																	
By total	2,274	1,238	1,036	48	46	788	488	239	352	141	130	17	16	1	2	4	2
By percent	100.00%	54.44%	45.56%	2.11%	2.02%	34.65%	21.46%	10.51%	15.48%	6.20%	5.72%	0.75%	0.70%	0.04%	0.09%	0.18%	0.09%

www.federalreserve.gov
0312

Report to the Congress on the Office of Minority and Women Inclusion

March 2013

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

Report to the Congress on the Office of Minority and Women Inclusion

March 2013

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

This and other Federal Reserve Board reports and publications are available online at
www.federalreserve.gov/publications/default.htm.

To order copies of Federal Reserve Board publications offered in print,
see the Board's Publication Order Form (www.federalreserve.gov/pubs/orderform.pdf)
or contact:

Publications Fulfillment
Mail Stop N-127
Board of Governors of the Federal Reserve System
Washington, DC 20551
(ph) 202-452-3245
(fax) 202-728-5886
(e-mail) Publications-BOG@frb.gov

Preface: Implementing the Dodd-Frank Act

Pursuant to section 342(e) of the Dodd-Frank Wall Street Reform and Consumer Protection Act (the Dodd-Frank Act), the Office of Diversity and Inclusion of the Board of Governors of the Federal Reserve System must submit an annual report to the Congress outlining the activities, successes, and challenges of the Office. This is the Office's report for 2012.

See the Board's website for an overview of the Dodd-Frank Act regulatory reform effort (www.federalreserve.gov/newsevents/reform_about.htm) and a list of the implementation initiatives recently completed by the Board as well as several of the most significant initiatives that the Board expects to address in the future (www.federalreserve.gov/newsevents/reform_milestones.htm).

Contents

Introduction

In January 2011, pursuant to section 342 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (the Dodd-Frank Act), the Board of Governors of the Federal Reserve System (the Board) established its Office of Diversity and Inclusion (ODI) to promote diversity and inclusion. ODI builds on the Board's long-standing efforts to promote equal employment opportunity and diversity and to foster diversity in procurement. The Board has welcomed the new requirements under section 342 as a complement to its existing efforts as well as an opportunity to strengthen those efforts.

ODI's mission and scope include the responsibilities identified in section 342 for the Office of Minority and Women Inclusion (OMWI), as well as Equal Employment Opportunity (EEO) compliance and programs, and initiatives addressing diversity and inclusion. Sheila Clark serves as the director of ODI.

Equal Employment of Minorities and Women

The Board is committed to equal employment opportunity in all aspects of employment, and to fostering diversity and inclusion in the workplace. The Board believes that it can assemble the workforce needed to complete its important mission only by attracting and hiring talented individuals without regard to race, gender, color, creed, nationality, or sexual preference, and by providing an inclusive and respectful work environment that allows its employees to fully use their individual talents to advance the mission of the Board most effectively.

In support of its commitment, the Board has in place strategic objectives to attract, hire, develop, promote, and retain a highly skilled and diverse workforce. The Board also allocates significant resources to ensure the success of its equal employment opportunity (EEO) and diversity and inclusion initiatives, which assist in enabling the Board to compete with other federal agencies and the private sector for talented individuals.

Equal Employment Opportunity

The Office of Diversity and Inclusion (ODI) has oversight for equal employment opportunity and diversity and inclusion initiatives for the Board.

The Board's Equal Employment Program, which is housed within ODI, strives to meet the "Essential Elements of a Model EEO Program" as prescribed in the Equal Employment Opportunity Commission's (EEOC) Management Directive 715 (MD-715) and the Government-Wide Diversity and Inclusion Strategic Plan 2011 issued by the Office of Personnel Management and mandated by the President's Executive Order 13583. The Board has formal policies regarding equal employment opportunity, reasonable accommodation, and sexual harassment, and the EEO Program undertakes training and analysis to ensure that the Board complies with all applicable laws and regulations. The Board uses MD-715 (which includes an annual barrier analysis) as the primary metric to assess the effectiveness of its diversity policies. In addition, the Board conducts an impact analysis on employment transaction data (i.e., hires and promotions) and a complaint trend analysis. Each of the Board's 15 operational divisions has an EEO liaison who works with ODI to address recruitment and retention issues specific to the liaison's division. ODI, in conjunction with each EEO liaison, monitors progress on increasing workforce diversity.

Table 1. Federal Reserve Board reported total workforce demographics, selected data, 2011 and 2012

	2012	2011	Change (number)
Male	1,315	1,238	+77
Female	1,072	1,036	+36
Non-minority	1,339	1,276	+63
Minority	1,048	998	+50
Total employees	2,387	2,274	+113

The Board annually submits to the EEOC an EEO Program Status Report as well as its EEO-1 Report, which is published at www.federalreserve.gov/aboutthefed/diversityinclusionrpt.htm. The Board's 2012 EEO-1 report is included in this document as appendix A.

Highlights of the Board's 2011 and 2012 EEO-1 reported total workforce demographics are shown in tables 1, 2, and 3. The Board's total workforce is 45 percent female and 44 percent minority. The Board reported an increase of 113 (5 percent) employees in the total workforce for 2012. The percentage of minorities in the Executive Senior Level category increased from 19 percent in 2011 to 21 percent in 2012. The percentage of minorities decreased from 46 percent in 2011 to 42 percent in 2012 in the 1st/Mid. Level Manager category compared to increases in previous years as noted in the MD-715 for 2007–10. The representation of women increased from 53 percent in 2011 to 65 percent in 2012 in the

1st/Mid. Level Manager category and decreased slightly in the Executive Senior Level category from 41 percent in 2011 to 40 percent in 2012. Hispanic representation in the Board's workforce continued to increase from a total of 94 employees in 2011 to 106 employees in 2012.

Table 2. Federal Reserve Board workforce profile, 2011

	EEO-1 categories									
	Exec. Sr. Level		1st/Mid. Level Manager		Professionals		Admin. Support Workers		Service Workers	
	Number	Percent	Number	Percent	Number	Percent	Number	Percent	Number	Percent
Male	201	59	38	47	775	53	27	18	142	80
Female	142	41	43	53	684	47	127	82	35	20
Non-minority	277	81	44	54	859	59	19	12	57	32
Minority	66	19	37	46	600	41	135	88	120	68
Total employees	**343**	**–**	**81**	**–**	**1,459**	**–**	**154**	**–**	**177**	**–**

Table 3. Federal Reserve Board workforce profile, 2012

	EEO-1 categories									
	Exec. Sr. Level		1st/Mid. Level Manager		Professionals		Admin. Support Workers		Service Workers	
	Number	Percent	Number	Percent	Number	Percent	Number	Percent	Number	Percent
Male	211	60	27	35	839	54	26	18	158	82
Female	140	40	51	65	723	46	119	82	34	18
Non-minority	277	79	45	58	914	59	21	14	57	30
Minority	74	21	33	42	648	41	124	86	135	70
Total employees	**351**	**–**	**78**	**–**	**1,562**	**–**	**145**	**–**	**192**	**–**

The Board recognizes that a strategic approach to diversity and inclusion requires multiple, integrated, ongoing efforts. The Board continuously reviews and assesses our employment policies, procedures, and practices to ensure EEO compliance and the full utilization of our diverse and talented workforce. As examples, the Board closely monitors: the pipeline in place to advance and promote young workers, efforts relating to skill development, succession planning, compensation equity, and analysis of applicant pool data. Results of the Board's assessment(s) are considered when deciding how to address issues and trends.

In addition to monitoring hiring and promotion, the Board also monitors the retention of women and minorities by job category, level, and grade. In the event there are concerns about retention, ODI works with management to address issues.

Further, the Board utilizes the complaint investigation process to address employees' concerns. This process is also utilized as a means of identifying trends in the workplace that may adversely affect the Board's employees.

ODI and the Office of Employee Relations collaborate to ensure that the Board properly administers its EEO policies, including those relating to reasonable accommodations for employees with disabilities, and its workplace-related policies, such as adverse actions and disciplinary actions.

Recruitment and Retention

The Board recognizes that a work environment that attracts and retains top talent is essential. ODI, Human Resources, Employee Relations, and Organizational Development and Learning collaborate continuously to promote an excellent quality of work life at the Board for all employees.

Short-term and long-term strategies are developed to help ensure women and minorities are represented in

Table 4. University career fairs and recruiting outreach initiatives utilized by the Board in 2012

Pennsylvania State University Career Fair – Interns
University of North Carolina at Chapel Hill – Diversity Job & Internship Fair
College of William & Mary – Diversity Job Fair
Virginia Tech – Business & Engineering Career Fairs
George Washington University School of Business
University of Maryland – College Park
AUCC: Spelman & Morehouse Colleges and Clark Atlanta University
University of Pittsburgh
Howard University
Florida A&M University
West Virginia University – Engineering
Florida International University
Hampton University
James Madison University
Syracuse University – IT and Business Career Fairs
University of Maryland – Baltimore County
Gallaudet University
University of Virginia – Diversity Fair
Columbia University Engineering Consortium

the Board's applicant and candidate pools and are considered for hires and/or promotions for key positions. In 2012, the Board filled 427 positions, including 116 summer interns. The positions were filled in the following major job families: financial analysis, information technology, economics, human resources, and legal.

The Board utilized a variety of sources to fill the positions. Thirty-five percent of the positions were filled through internal promotions. In filling the remaining 65 percent of positions, the Board used a variety of methods to reach out to a broad range of qualified candidates, including job boards, social media (e.g., LinkedIn Talent Advantage, Federal Reserve System's Diversity Twitter account), professional associations (e.g., National Black MBA Association, National Society of Hispanic MBAs, HBCU Connect), career fairs, and publications that aid in providing diverse pools of candidates with the skill sets—or the potential to develop such skill sets—necessary to fill positions.

Additionally, as part of its strategy to attract pools of talented applicants, the Board recruits from a number of colleges and universities for full-time positions, including those listed in table 4.

The Board also continues to partner with the Reserve Banks to participate in national diversity recruiting events by sharing the cost of career fairs, engagements hosted by professional organizations (National Black MBA Association, National Society of Hispanic MBAs, and the Association of Latino Professionals in Finance and Accounting), and networking opportunities with special interest organizations.

In addition, the Board identifies students for paid summer internships. The internship program helps enable the Board to identify candidates for future employment opportunities and provides students hands-on opportunities and insight into the mission and work of the Board and the Federal Reserve System. Many of the students are recruited through colleges and universities (including Historically Black Colleges and Universities), special interest publications, and diversity focused organizations (e.g., the Hispanic Association of Colleges and Universities, Washington Internship for Native American Students, Workforce Recruitment Programs - College Students with Disabilities, and INROADS).

Internally, to help ensure equal opportunity and diversity in their divisions, the Board appoints Division Liaisons to work directly with ODI. Divisions also develop their own equal employment opportunity and diversity strategies, such as management development, succession planning, and accountability, and include these strategies in management performance objectives.

To ensure Division Liaisons are aware of innovative developments and best practices, ODI consults with leading national professional organizations such as the Equal Employment Advisory Council, the Society of Human Resources Management, the Federal Interagency Diversity Partnership, Workforce Opportunity Network, and the Conference Board. These organizations conduct valuable research and benchmarking, and highlight relevant best practices, which ODI shares with Division Liaisons to meet the Board's needs.

Training and Mentoring

In 2012, the Board continued to provide Workplace Harassment Prevention training and counseling services to divisions to address EEO and/or diversity issues and trends. Other diversity-related training included "Leading in a Diverse Environment and Working in a Diverse Environment," "Conflict Resolution," and "Diversity Management Awareness." In compliance with the mandates of the No FEAR Act, the Board is enhancing the No FEAR web-based training to be implemented in the spring of 2013. This training is required for all employees.

The Federal Reserve System Leadership Exchange Program, in conjunction with division-specific mentoring programs, enables participants to develop skills relating to their careers. The exchange and mentoring programs provide hands-on learning, promote exposure to different experiences, and broaden cross-system opportunities and visibility.

The Board also has a Quick Start for Managers program, which provides several interactive learning sessions for managers to design a plan of action to help enable them to be successful managers. The sessions are: "Exploring Your Role as a Manager," "Motivating and Engaging Others," "Influencing and Managing Up," "Managing Results," "Providing High-Impact Feedback," "Navigating Conflict," "Building High Performance Teams," and "Realizing Your Impact."

Successes

At the officer level, the Board increased its staff by seven positions in 2012, of which six, or 86 percent, were minorities. Female representation in 1st/Mid. Level Manager category increased from 53 percent in 2011 to 65 percent in 2012. Further, the Board's outreach initiatives resulted in more diverse applicant pools for major job families, such as financial analyst and IT professional, as well as 26 minority hires (out of a total 66 hires). The minority hires included seven Hispanics in job categories with low Hispanic representation. Overall, there was an increase of Hispanic representation from a total of 94 employees in 2011 (4.1 percent of the workforce) to 106 employees in 2012 (4.4 percent of the workforce).

Challenges

Although there was some improvement, there continue to be challenges in hiring minorities in the economist job family and Hispanics in the overall employee workforce.

To help improve the current state of low Hispanic representation, the Board has strengthened its recruiting for major job occupations through its relationships with professional associations, such as the Association of Latino Professionals in Finance and Accounting, and by sourcing applicants for internships through organizations such as the Hispanic Association of Colleges and Universities.

The Board also continues to address these challenges through participation in educational forums, mentoring programs, and summer internships sponsored by the American Economic Association's Committee on Status of Minority Groups in Economics Profession (CSMGEP), of which the Board is a member.

In recent years, a senior staff member or an economist has represented the Board on CSMGEP. CSMGEP was established by the American Economic Association (AEA) to increase the representation of minorities in the economics profession, primarily by broadening opportunities for the training of underrepresented minorities. CSMGEP, which comprises economists from all areas of the profession, also works to ensure that issues related to the representation of minorities are considered in the work of the AEA, and engages in other efforts to promote the advancement of minorities in the economics profession. The Board representative helps to organize and oversee the three programs under the purview of CSMGEP: (1) the Summer Economics Fellows Program, which matches advanced graduate students or junior faculty with research-oriented sponsoring institutions (including the Board) for a short residency, during which fellows are expected to work in one of their own research projects while participating in the research community of the sponsoring institutions; (2) the Summer Training Program, which is designed to provide undergraduate students with a program of study and research opportunities that prepare them with a better understanding of what the study of economics entails at the doctoral level and career options for doctoral graduates; and (3) the Mentoring Program in which students are matched with a mentor who sees them through the critical junctures of their graduate program (including the transition from course work to research) or the early stages of their post-graduate career.

Board economics staff have been actively involved in all three CSMGEP programs serving as mentors in the Mentoring Program, instructors in the Summer Training Program, and sponsors for the Summer Fellows program.

Inclusion of Minority-Owned and Women-Owned Businesses

The Procurement Section in the Board's Division of Financial Management continues to demonstrate a strong and positive commitment to the inclusion of minority-owned and women-owned businesses in the Board's acquisition process. A comprehensive program strategy has been implemented by setting forth specific actions to assist the Board in fostering relationships with these types of businesses. This strategy contains objectives and activities with detailed steps that are aligned with the provisions of section 342 of the Dodd-Frank Act to help position the Board to cultivate minority-owned and women-owned businesses. Through networking with minority-owned and women-owned firms, the Procurement Section has made significant progress in fostering success for minority-owned and women-owned businesses looking to do business with the Board.

Outreach Activities

The Board is committed to executing a dynamic and effective outreach program to minority-owned and women-owned businesses. As a part of Procurement's Supplier Diversity Plan, the Procurement staff participated in numerous external outreach programs and activities. The Board designed and implemented an outreach plan primarily focused on three strategies: (1) forging partnerships with the local, regional, and national minority-owned and women-owned business communities; (2) creating or having access to a database of minority-owned and women-owned firms that can offer the Board quality goods and services; and (3) reviewing minority-owned and women-owned firms offering goods and services aligned with the Board's expected needs. As will be discussed, the Board has made significant progress in implementing each of the three strategies outlined above.

Providing Technical Assistance

In April 2012, ODI and the Federal Reserve Bank of Richmond's Office of Minority and Women Inclusion sponsored an Empower Forum. The goal of the forum was to provide capacity-building resources for minority-owned and women-owned businesses. Featured sessions included "How to do business with the Federal Reserve System and other Government agencies," "Sustaining minority-owned and women-owned businesses during challenging economic times," "Building successful and beneficial relationships to grow business," "Challenges of accessing capital," and "Top characteristics of emerging businesses."

Federal Reserve Board Chairman Ben Bernanke provided opening remarks, and presentations were given by the following partnering organizations: U.S. Department of the Treasury, Minority Business Development Agency, Small Business Investor Alliance, Interise, Women's Business Enterprise National Council, United States Hispanic Chamber of Commerce, and the U.S. Pan Asian American Chamber of Commerce. Representatives from the Board and the Federal Reserve Bank of Richmond participated in and led various panel discussions and workshops.

Fifty percent of the total participants at the forum were minority-owned businesses of which 50 percent were African American, 36 percent were Asian American, and eight percent were Hispanic American; 35 percent of the total participants were women-owned businesses. The largest number of participants represented companies that focus on business services and information technology. Other sectors represented were: law firms, management, consulting, and the service industry.

Further, the Supplier Diversity Specialist, hired by the Board in 2011, has continued to work with suppliers to provide technical assistance in order to increase the participation and identification of diverse suppliers in the Board's acquisition process. A major initiative in 2012 was the implementation of an external vendor management system. This web-based application allows vendors to register their

companies' information with the Board to become potential suppliers.

The Board is very proud that its Procurement Section was named 2012 Minority Business Advocate of the Year by the Minority Business Development Agency (MBDA) Business Center of Washington, D.C. Through the Board's Supplier Diversity Program, the Procurement Section worked closely with the MBDA to raise awareness among minority-owned firms of contracting opportunities at the Board, and to provide technical assistance regarding the Board's acquisition process.

Program Enhancements

The Board has made a number of internal program enhancements. The Procurement Section now requires that for all procurements greater than or equal to $50,000, staff members are to make concerted efforts to include minority-owned and women-owned companies in the solicitation process by reviewing the solicitations and adding to the list of potential vendors qualified companies identified through the Procurement vendor management system or through other means. The Board is also making efforts to review U.S. General Services Administration and Federal Supply Schedule purchases to ensure that, where possible, minority-owned and women-owned companies are included in contracting opportunities. In 2013, the Board also plans to solicit information from its telephone and utility company contractors regarding their second-tier sourcing with minority-owned and women-owned companies in an effort to better track such subcontracts.

Successes

In 2012, the Procurement Section made substantial progress in its supplier diversity initiatives, which are designed to foster the fair inclusion and utilization of minority-owned and women-owned businesses in the Board's acquisition process.

The Board incorporated supplier diversity language in contracts, including a statement requiring contractors to confirm their commitment to equal opportunity in employment and contracting, and to the fair inclusion of minorities and women in their workforce.

As mentioned earlier, the Board implemented a web-based application allowing vendors to register their companies' information with the Board to become potential suppliers. Approximately 900 companies have registered with the Board using the web-based application. This information is available to internal purchasers of goods and services (such as the Procurement Section) to use as a tool to identify registered minority-owned and women-owned companies for solicitations. The site also allows internal users to export stored data in a way that allows Procurement and other Board users to measure and track the progress made to include minority-owned and women-owned companies in the solicitation process. Ultimately, this system will also be used to communicate information to potential suppliers regarding goods and services projected in the Board's forecast of contract opportunities and networking/outreach opportunities.

The Board held its annual Vendor Outreach Fair in May 2012. Vendors were able to conduct one-on-one meetings to share their capabilities with representatives from several Board functional areas, including Human Resources, Benefits, Employee Relations, Staffing, Information Technology, Facilities, Communications, Staff Development, Organizational Development and Learning, Space Planning, and Automation Programs Applications. Representatives from the Small Business Administration and from the Federal Reserve Bank of Richmond were also in attendance to meet with vendors. Approximately 116 of the roughly 200 firms that attended the event were minority-owned and/or women-owned firms.

Further, the Board designed capacity-development workshops on "How to do Business with the Federal Reserve Board," and conducted these workshops at the 2012 Vendor Outreach Fair and at other outreach events. These capacity workshops are designed to assist minority-owned and women-owned firms with overcoming obstacles that inhibit them from successfully competing in the Board's acquisition process.

The Board also obtained memberships in national and local organizations which serve as a method to connect directly with qualified minority-owned and women-owned companies. Memberships in these types of organizations will provide direct access to diverse suppliers that demonstrate the ability to provide high-quality goods and services.

The Board significantly strengthened its relationships in the business community by forging key external relationships through collaboration. Relationships with the following key external organizations were either established or enhanced, through organization memberships and/or participation in conferences and outreach events: the Greater Washington Hispanic Chamber of Commerce, the U.S. Hispanic Chamber of Commerce, the Office of Small and Disadvantaged Business Utilization (OSDBU), the U.S. Black Chamber of Commerce, Women Impacting Public Policy, the U.S. Women's Chamber of Commerce, the U.S. Pan Asian American Chamber of Commerce, the Minority Business Development Agency, the National Minority Supplier Development Council, the MD/DC Minority Supplier Development Council, the Chicago Minority Supplier Development Council, the Women Business Enterprise National Council, the National Association of Small Disadvantaged Businesses, the Small Business Administration, the National 8(a) Association, and the National Center for American Indian Enterprise Development. The Board continues to work to identify additional opportunities for outreach and networking events with minority-owned and women-owned companies, locally and nationally.

Contracts with Minority-Owned and Women-Owned Businesses

In reviewing the 2012 contract awards, the Board identified a critical need to implement a systematic process to track, monitor, and forecast the progress of contracts from inception to completion, including the contract option years. To address this need, Procurement staff is working with technical support staff to discuss requirements for an automated system that will track contracts.

The Board continues to maintain indefinite-delivery/indefinite-quantity (IDIQ) contracts for information technology consulting services with several minority-owned and women-owned firms, through which the Board can order consulting services. Out of 15 total IDIQ contracts for IT consulting services, eight are with minority-owned or women-owned companies, and the Board will continue to place task orders with these firms on an ongoing basis. In an effort to further the Board's contracting activity with minority-owned and women-owned construction firms, the Board conducted a competitive solicitation, offer, and award process that resulted in the award of several Basic Ordering Agreement construction contracts to minority-owned firms. The Board plans to issue task orders for construction projects to these firms during 2013 and beyond.

During 2012, the Board's contracts for goods and services totaled $141,168,580. Of that amount, a total of $13,556,629, or 9.6 percent, was awarded to minority-owned or women-owned businesses. Contracting with minority-owned businesses decreased in 2012 compared to 2011, due in part to a number of construction contracts that concluded in 2011. At the same time, however, contracts issued to women-owned businesses increased significantly, from 3.4 percent of contract expenditures in 2011 to 8.4 percent in 2012, and contracts with minority women-owned businesses also expanded.

Table 5. Contract awards for minority-owned and women-owned businesses, 2011 and 2012

	2012[1]		2011[2]	
	Dollars	Percent	Dollars	Percent
Minority-owned businesses[3]	$3,726,415	2.6	$9,028,526	7.2
Women-owned businesses[3]	$8,145,183	8.4	$4,237,038	3.4
Minority women-owned businesses	$1,685,031	1.2	$2,148,583	1.7

1 Total contracts awarded in 2012 were $141,168,580.
2 Total contracts awarded in 2011 were $125,070,569.
3 Does not include contracts with minority women-owned businesses.

Challenges

Much of the Board's procurement activity involves acquisition of economic data, generally purchased from large companies. ODI and Procurement offices have met with minority-owned and women-owned businesses that have indicated that they can provide these services, and expect to host a meeting between the Board's research divisions and these prospective vendors. The meeting agenda will focus on the Board's requirements for economic data, and will provide an opportunity for vendors to discuss their capabilities.

The Procurement section continues to actively solicit and review minority-owned and women-owned vendors to participate in the Board's contracting activities. Procurement collaborates with advocacy groups representing minority-owned and women-owned firms to better understand the challenges of these

businesses and provide assistance to help them navigate the Board's acquisition process.

Looking Ahead

The Board will continue to improve its acquisition process to enhance the ability of minority-owned and women-owned firms to successfully compete. Among its strategies are comprehensive training programs for all Board employees, supplier diversity performance plans for procurement staff, targeted outreach programs, revised procurement policies, and the adoption of online tools and resources. The Board is currently finalizing a draft Supplier Diversity Policy which will assist the Board in implementing policies that will increase the number of contracts awarded to minority-owned and women-owned businesses.

To maximize the impact on minority-owned and women-owned firms, the Board will focus on increasing the participation of small business enterprises in its acquisition process. To that end, the Board will post on Procurement's external webpage a forecast of upcoming solicitations to inform firms of contracting opportunities. The Board will continue to collaborate with other Federal banking agencies, the OSDBU, and the Federal Reserve System Supplier Diversity Work Group to share successful "best practices" and to integrate those practices into the Board's business processes and systems to capture relevant data and monitor improvements in the inclusion of minority-owned and women-owned firms. The Board will provide resources to its end users who participate in the Board purchase card program to allow them to purchase from minority-owned and women-owned companies to the maximum extent practicable.

In addition, the Board plans to host networking meetings for vendors in specific markets such as economic research/data and legal services in order to expand opportunities for the Board to contract with minority-owned and women-owned firms in these industries. In preparation for a major construction project anticipated to take place in the next few years, the Board plans to host networking meetings where large general construction firms that might be included as prime contractors for the construction project could meet with minority-owned and women-owned construction firms that could serve as subcontractors on the project. The Board also plans to solicit information from its primary contractors regarding their second-tier sourcing with minority-owned and women-owned companies in an effort to better track such subcontracts.

Finally, the Board will continue to nurture and foster relationships with small minority-owned and women-owned firms to broaden its access to quality products and services.

Financial Literacy Activities

During 2012, the Board continued to participate in community outreach events and programs, examples of which are listed below.

- *Conversation with the Chairman: A Teacher Town Hall Meeting*: In August 2012, Chairman Bernanke held a town hall meeting with teachers and educators across the 12 Reserve Bank Districts to discuss the need for personal financial education in the wake of the recent financial crisis. Chairman Bernanke took questions in person and via videoconference from K–12 and post-secondary educators of economics, personal finance, and related disciplines, who were gathered at Federal Reserve Bank offices across the country.
- *Congressional Black Caucus Annual Legislative Conference*: In September 2012, the Board, in conjunction with the Federal Reserve Banks, sponsored a booth at the 42nd Annual Legislative Conference. Financial education materials and information on how to access the System's public website for additional information regarding financial literacy were distributed to exhibit fair attendees. The Board also provided support for the Financial Education Youth Summit convened by the Black Caucus held at the U.S. Capitol Visitor's Center and Trinity Washington University.
- *FedEd Program*: During 2012, research assistants from divisions within the Board continued to expand upon and implement a program developed to work with local high school students to improve their understanding of personal finances and the role of the Federal Reserve System in the economy. Subjects covered included the importance of saving, budgeting, use of credit, and the establishment of financial goals. In 2012, more than a dozen presentations were made to middle and high school students in the Washington metropolitan area. Presentations were made at six schools: Friendly High School and Sherwood High School in Maryland; Cardozo High School and The Duke Ellington School of the Arts in Washington, D.C.; and the Academy of Finance at T.C. Williams High School in Virginia.
- *Math x Economics*: In May 2012, the Board hosted a one-day program for high school juniors and seniors who are exceptionally talented in mathematics. The goal of the program was to introduce students to economics as a potential course of study in college, and as a future career option.
- *D.C. Public Schools Partner Fair*: In June 2012, Board research assistants participated in the "Connecting School Leaders and Community Partners" event held at Eastern High School in Washington, D.C. The research assistants distributed information on the Federal Reserve Board's FedEd program as well as other financial literacy materials from the Federal Reserve System. As a result of this activity, several school administrators requested presentations for their students. Presentations have been scheduled for the 2013 school year.
- *Education and Training Materials Distribution*: During 2012, the Board continued to provide financial literacy materials to consumer education and financial literacy groups including the University of Maryland Extension Family and Consumer Sciences Center, the YMCA of Metropolitan Washington, and Operation HOPE.
- *Financial Literacy Day on the Hill*: The Board participated in the 10th annual "Financial Literacy Day on the Hill" on April 17, 2012, in the Hart Senate Building in Washington, D.C., and provided financial publications and education program information to participants.

Diversity Policies and Practices of Regulated Entities

In 2012, an interagency working group comprising the financial agency OMWI Directors (the Board, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Consumer Financial Protection Bureau, and the Securities Exchange Commission) continued to coordinate closely in the development of standards for assessing the diversity policies and practices of entities regulated by each agency. The priority of the interagency working group is to meet the provisions of section 342(b)(3) of the Dodd-Frank Act pertaining to the development of standards to assess the diversity policies and practices of entities regulated by the agencies, and ensure that all entities are subject to similar standards regardless of regulator.

The interagency working group completed the following activities in 2012:

- held meetings with the EEOC, the Department of Labor, Office of Federal Contract Compliance Programs, and the Department of Justice to determine available resources;
- held industry, trade, and public roundtables throughout the United States, and telephone conferences with industry, trade, and state banking representatives;
- held meetings with community interest group representatives to broadly discuss implementation of section 342 of the Dodd-Frank Act; and
- held meetings with banking and industry trade representatives to gather information and discuss leading practices in recognition of the wide-ranging sizes, markets, and complexities of the regulated entities.

The roundtables referenced above, held with the OMWI Directors, regulated entities, industry trade organizations, and consumer organizations in Washington, D.C.; Chicago; Dallas; New York City; Charlotte; and Denver, were attended by more than 100 representatives. In addition, two roundtable conference calls were held to enable community bankers from across the country to provide input. The information and suggestions gathered from these meetings have assisted the interagency group's efforts in developing a direction for standards that would promote diversity best practices while not disrupting existing, successful programs or imposing undue burdens on the financial services and banking industry. Attendees responded to questions and shared suggestions and concerns regarding standards and implementation methods. Using this input, as well as diversity best practices research information, the OMWI Directors have drafted proposed interagency standards.

The interagency OMWI Directors plan to publish for comment a Proposed Policy Statement proposing joint standards to assess the diversity policies and practices of regulated entities during spring 2013. The standards describe leading diversity practices for the financial services industry in four key areas: organizational commitment, workforce profile and employment practices, supplier diversity in procurement and business practices, and transparency of organizational diversity and inclusion policies.

Appendix A: EEO-1 Report for the Board of Governors of the Federal Reserve System for Calendar Year 2012

Employer Information Report EEO-1

Federal Reserve Board, 2012 Employer Information Report

Occupational Categories	Total Employees			Race/Ethnicity													
						Non- Hispanic or Latino											
				Hispanic or Latino		White		Black or African American		Asian		Native Hawaiian or Other Pacific Islander		American Indian or Alaska Native		Two or More Races	
	All	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female
1.1 Exec. Sr. Level Managers, Governors, Officers, FR-29 & FR-28																	
By total	351	211	140	4	6	176	101	19	21	11	10	1	1	0	0	0	1
By percent	100.00%	60.11%	39.89%	1.14%	1.71%	50.14%	28.77%	5.41%	5.98%	3.13%	2.85%	0.28%	0.28%	0.00%	0.00%	0.00%	0.28%
1.2 1st/Mid. Level																	
By total	78	27	51	0	1	15	30	8	19	4	1	0	0	0	0	0	0
By percent	100.00%	34.62%	65.38%	0.00%	1.28%	19.23%	38.46%	10.26%	24.36%	5.13%	1.28%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Officials and Managers Total																	
By total	429	238	191	4	7	191	131	27	40	15	11	1	1	0	0	0	1
By percent	100.00%	55.48%	44.52%	0.93%	1.63%	80.25%	30.54%	6.29%	9.32%	3.50%	2.56%	0.23%	0.23%	0.00%	0.00%	0.00%	0.23%
2. Professionals																	
By total	1,562	839	723	39	41	559	355	86	186	133	126	17	15	1	0	4	0
By percent	100.00%	53.71%	46.29%	2.50%	2.62%	66.63%	22.73%	5.51%	11.91%	8.51%	8.07%	1.09%	0.96%	0.06%	0.00%	0.26%	0.00%
3. Technicians																	
By total	6	2	4	0	0	0	2	2	2	0	0	0	0	0	0	0	0
By percent	100.00%	33.33%	66.67%	0.00%	0.00%	0.00%	33.33%	33.33%	33.33%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
4. Sales Workers																	
By total	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
By percent	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
5. Admin. Support Workers																	
By total	145	26	119	1	5	6	15	18	93	1	4	0	0	0	2	0	0
By percent	100.00%	17.93%	82.07%	0.69%	3.45%	4.14%	10.34%	12.41%	64.14%	0.69%	2.76%	0.00%	0.00%	0.00%	1.38%	0.00%	0.00%
6. Craft Workers																	
By total	42	41	1	0	0	23	0	13	1	4	0	1	0	0	0	0	0
By percent	100.00%	97.62%	2.38%	0.00%	0.00%	54.76%	0.00%	30.95%	2.38%	9.52%	0.00%	2.38%	0.00%	0.00%	0.00%	0.00%	0.00%
7. Operatives																	
By total	11	11	0	0	0	0	0	11	0	0	0	0	0	0	0	0	0
By percent	100.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
8. Laborers and Helpers																	
By total	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
By percent	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
9. Service Workers																	
By total	192	158	34	9	0	53	4	93	28	3	1	0	1	0	0	0	0
By percent	100.00%	82.29%	17.71%	4.69%	0.00%	27.60%	2.08%	48.44%	14.58%	1.56%	0.52%	0.00%	0.52%	0.00%	0.00%	0.00%	0.00%
Total Workforce																	
By total	2,387	1,315	1,072	53	53	832	507	250	350	156	142	19	17	1	2	4	1
By percent	100.00%	55.09%	44.91%	2.22%	2.22%	34.86%	21.24%	10.47%	14.66%	6.54%	5.95%	0.80%	0.71%	0.04%	0.08%	0.17%	0.04%

www.federalreserve.gov
0313

Report to the Congress on the Office of Minority and Women Inclusion

April 2014

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

Report to the Congress on the Office of Minority and Women Inclusion

April 2014

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

This and other Federal Reserve Board reports and publications are available online at
www.federalreserve.gov/publications/default.htm.

To order copies of Federal Reserve Board publications offered in print,
see the Board's Publication Order Form (www.federalreserve.gov/pubs/orderform.pdf)
or contact:

Publications Fulfillment
Mail Stop N-127
Board of Governors of the Federal Reserve System
Washington, DC 20551
(ph) 202-452-3245
(fax) 202-728-5886
(e-mail) Publications-BOG@frb.gov

Preface: Implementing the Dodd-Frank Act

Pursuant to section 342(e) of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), the Office of Diversity and Inclusion (ODI) of the Board of Governors of the Federal Reserve System must submit an annual report to the Congress outlining the activities, successes, and challenges of the Office. This is the Office's report for calendar year 2013. Sheila Clark serves as the director of ODI.

See the Board's website for an overview of the Dodd-Frank Act regulatory reform effort (www.federalreserve.gov/newsevents/reform_about.htm) and a list of the implementation initiatives recently completed by the Board as well as several of the most significant initiatives that the Board expects to address in the future (www.federalreserve.gov/newsevents/reform_milestones.htm).

Contents

Introduction

In January 2011, pursuant to section 342 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), the Board of Governors of the Federal Reserve System (the Board) established its Office of Diversity and Inclusion (ODI) to promote diversity and inclusion. ODI builds on the Board's long-standing efforts to promote equal employment opportunity and diversity and to foster diversity in procurement.

ODI's mission and scope include the responsibilities identified in section 342 for the Office of Minority and Women Inclusion (OMWI), as well as Equal Employment Opportunity (EEO) compliance and programs, and initiatives addressing diversity and inclusion. ODI works to assess the Board's diversity policies, programs, and performance to determine progress and increase transparency. ODI's ongoing effort to foster an informed dialogue on diversity best practices includes participation in Equal Employment Opportunity Commission (EEOC) technical workshops, attendance at conferences and events held by professional organizations, and participation in financial industry groups.

Equal Employment of Minorities and Women

The Board is committed to equal employment opportunity in all aspects of employment, and to fostering diversity and inclusion in the workplace. In support of its commitment, the Board has in place strategic objectives to attract, hire, develop, promote, and retain a highly skilled and diverse workforce. The Board also allocates significant resources to ensure the success of its equal employment opportunity (EEO) and diversity and inclusion initiatives, which assist in enabling the Board to compete with other federal agencies and the private sector for talented individuals.

Table 1. Federal Reserve Board reported total workforce demographics, selected data, 2012 and 2013

	2012	2013	Change (number)
Male	1,315	1,364	+49
Female	1,072	1,092	+20
Non-minority	1,339	1,376	+37
Minority	1,048	1,080	+32
Total employees	2,387	2,456	+69

Equal Employment Opportunity

The Board's Equal Employment Program, which is housed within the Office of Diversity and Inclusion (ODI), strives to meet the "Essential Elements of a Model EEO Program" as prescribed in the Equal Employment Opportunity Commission's (EEOC) Management Directive 715 (MD-715) and the Government-Wide Diversity and Inclusion Strategic Plan 2011 issued by the Office of Personnel Management and mandated by the President's Executive Order 13583. The Board has formal policies regarding equal employment opportunity, reasonable accommodation, and discriminatory workplace harassment, and the EEO Program undertakes training and analysis to ensure that the Board complies with all applicable laws and regulations. The Board uses elements of MD-715 (which includes an annual barrier analysis) as the primary metric to assess the effectiveness of its diversity policies and initiatives. Further, the Board reviews quarterly employment transaction data (i.e., hires and promotions) to determine any adverse impact based on race or gender as well as a complaint trend analysis.

In addition, the Board utilizes EEO management systems to identify strengths and areas for improvement in the talent acquisition process. By identifying potential issues, the Board can develop action plans that incorporate short- and long-term objectives. ODI works in conjunction with EEO liaisons from each of the Board's 15 operational divisions and Board leadership to ensure that inclusion and diversity exist at all levels of employment throughout the Board and that divisions identify and approach diversity challenges with transparency. Divisions also develop their own additional EEO and diversity strategies, such as management development, succession planning, and accountability, and include these strategies in management performance objectives.

To ensure the Board is aware of innovative developments and best practices, ODI consults with leading national professional organizations such as the Equal Employment Advisory Council, the Society of Human Resources Management, the Federal Interagency Diversity Partnership, Workforce Opportunity Network, the Conference Board, and the Federal Dispute Resolution Conference. These organizations conduct valuable research and benchmarking, and highlight relevant best practices, which ODI shares with division EEO liaisons to meet the Board's needs.

The Board annually submits to the EEOC an EEO Program Status Report as well as its EEO-1 Report, which is published at www.federalreserve.gov/aboutthefed/diversityinclusionrpt.htm. The Board's 2013 EEO-1 Report is included in this document as appendix A.

Highlights of the Board's 2012 and 2013 EEO-1 reported total workforce demographics are shown in tables 1, 2, and 3. The Board's total workforce is 44 percent female and 44 percent minority. The Board reported an increase of 69 (3 percent) employ-

ees in the total workforce for 2013, of which 32 were minorities and 20 were women. The percentage of minorities in the Executive Senior Level category increased from 21 percent in 2012 to 23 percent in 2013. In the 1st/Mid. Level Manager category, the percentage of minorities increased from 42 percent in 2012 to 53 percent in 2013 and the representation of women decreased from 65 percent in 2012 to 55 percent in 2013. The representation of women remained at 40 percent in the Executive Senior Level category. Hispanic representation in the Board's workforce continued to increase from a total of 106 employees in 2012 to 109 employees in 2013.

Table 2. Federal Reserve Board workforce profile, 2012

	EEO-1 categories									
	Exec. Sr. Level		1st/Mid. Level Manager		Professionals		Admin. Support Workers		Service Workers	
	Number	Percent	Number	Percent	Number	Percent	Number	Percent	Number	Percent
Male	211	60	27	35	839	54	26	18	158	82
Female	140	40	51	65	723	46	119	82	34	18
Non-minority	277	79	45	58	914	59	21	14	57	30
Minority	74	21	33	42	648	41	124	86	135	70
Total employees	**351**	**–**	**78**	**–**	**1,562**	**–**	**145**	**–**	**192**	**–**

Table 3. Federal Reserve Board workforce profile, 2013

	EEO-1 categories									
	Exec. Sr. Level		1st/Mid. Level Manager		Professionals		Admin. Support Workers		Service Workers	
	Number	Percent	Number	Percent	Number	Percent	Number	Percent	Number	Percent
Male	231	60	38	45	894	54	24	18	124	82
Female	153	40	47	55	747	46	112	82	28	18
Non-minority	294	77	40	47	960	59	18	13	41	27
Minority	90	23	45	53	681	41	118	87	111	73
Total employees	**384**	**–**	**85**	**–**	**1,641**	**–**	**136**	**–**	**152**	**–**

The Board recognizes that a strategic approach to diversity and inclusion requires multiple, integrated, ongoing efforts. The Board continuously reviews and assesses its employment policies, procedures, and practices to ensure EEO compliance and the full utilization of our diverse and talented workforce. As examples, the Board closely monitors applicant pool data; the programs in place to advance and promote employees, as well as those related to skill development, succession planning, and compensation equity; and the pipeline of personnel available for promotions. Results of the Board's assessment(s) are considered when deciding how to address issues and trends.

In addition to monitoring hiring and promotion, the Board also monitors the retention of women and minorities by job category, level, and grade. In the event there are concerns about retention, ODI works with management to address any issues.

Further, the Board utilizes the complaint investigation process to address employees' concerns and to identify trends in the workplace that may adversely affect the Board's employees.

ODI and the Office of Employee Relations collaborate to ensure that the Board properly administers its EEO policies, including those relating to reasonable accommodations for employees with disabilities, and its workplace-related policies, such as adverse actions and disciplinary actions.

Recruitment and Retention

The Board recognizes that a work environment that attracts and retains top talent is essential. ODI, Human Resources, Employee Relations, and Organizational Development and Learning collaborate continuously to promote an excellent quality of work life at the Board for all employees.

Short-term and long-term strategies are developed to help ensure women and minorities are represented in the Board's applicant and candidate pools and are considered for hires and/or promotions for key positions. In 2013, the Board filled 409 positions, of which 113 were summer interns. Fifty-seven percent of the positions filled were in the following major job families: attorney, computer professional, financial analyst, economist, and research assistant.

The Board utilized a variety of sources to fill the positions. Thirty-nine percent of the positions were filled internally. In filling the remaining 61 percent of positions, the Board used a variety of methods to attract a broad range of candidates, including job boards, social media (e.g., LinkedIn Talent Advantage, Federal Reserve System's Diversity Twitter account), career fairs, and publications that aid in providing diverse pools of candidates with the skill sets necessary to fill positions.

Additionally, as part of its strategy to attract diverse pools of talented applicants, the Board recruits from a number of colleges and universities for full-time positions, including those listed in table 4.

The Board also continues to partner with the Reserve Banks to participate in national diversity recruiting events by sharing the cost of career fairs, engagements hosted by professional organizations (National Society of Hispanic MBAs, Asian MBA (AMBA), and the Thurgood Marshall College Fund), and networking opportunities with special interest organizations. The Board is collaborating with the National Capital Region chapter of Year Up and will have a formal internship program during the summer of 2014. Year Up empowers urban young adults with the skills, experience, and support to achieve their potential through professional career opportunities and higher education. It offers a one-year, intensive training program that equips students with a combination of hands-on skill development, college credits, and corporate internships.

Table 4. University career fairs and recruiting outreach initiatives utilized by the Board in 2013

Big East Career Fair
Carnegie Mellon University
Christopher Newport University
Clark Atlanta University
Columbia University – Engineering Consortium
Cornell University
Drexel University
Florida A&M University
Florida International University
George Washington University – School of Business
Hampton University
Howard University
James Madison University
Morehouse College
New Jersey Institute of Technology
Pennsylvania State University
New York University – Polytechnic School of Engineering
Rochester Institute of Technology
Scholarship for Service
Spelman College
Syracuse University
University of Maryland
University of Miami
University of North Carolina at Charlotte
University of Virginia

In addition, the Board identifies students for paid summer internships. The internship program helps enable the Board to identify candidates for future employment opportunities and provides students hands-on opportunities and insight into the mission and work of the Board and the Federal Reserve System. Many of the students are recruited through colleges and universities (including Historically Black Colleges and Universities), special interest publications, and diversity focused organizations (e.g., the Hispanic Association of Colleges and Universities, Washington Internship for Native American Students, Workforce Recruitment Programs – College Students with Disabilities, and INROADS).

Training and Mentoring

In 2013, the Board continued to provide Workplace Harassment Prevention training and counseling services to divisions to address EEO and/or diversity issues and trends. Other diversity-related training included "Conflict Resolution," "Diversity Management Awareness," "Fierce Conversations," and "Micro-Triggers."

In compliance with the training requirements of the Notification and Federal Employee Antidiscrimination and Retaliation Act (No FEAR Act), the Board has contracted with Navex Global to provide No FEAR web-based training in 2014. This training is required for all employees. The segments will cover EEO compliance, disability and accommodations, and discriminatory workplace harassment.

The Federal Reserve System Leadership Exchange Program, in conjunction with division-specific mentoring programs, enables participants to develop skills relating to their careers. The exchange and mentoring programs provide hands-on learning, promote exposure to different employment experiences, and broaden cross-system opportunities and visibility.

The Board's talent development processes also correlate to six performance competencies:

- decision quality
- learning agility
- drive for excellence
- perspective and strategic
- collaborative relationships
- effective communications

The competencies are grouped by employee role (e.g., manager or officer) and include desired behaviors in shaping, guiding, and leveraging diversity and inclusion.

Talent is developed through participation in the Executive Coaching Program, the System Senior Leadership Initiative, and the Quick Start for Managers Program. The Quick Start for Managers Program provides several interactive learning sessions for new managers to design a plan of action to help enable them to be successful. The sessions are: "Exploring Your Role as a Manager," "Motivating and Engaging Others," "Influencing and Managing Up," "Managing Results," "Providing High-Impact Feedback," "Navigating Conflict," "Building High Performance Teams," and "Realizing Your Impact." A Quick Start program for officers will be developed in 2014.

Employees are encouraged to take part in development opportunities through self-assessment, coaching, mentoring, service on task forces, participating in significant high priority projects, and taking on special assignments.

In 2013, a total of 149 officers and managers participated in leadership programs, of which 46 percent were female and 31 percent were minorities.

Successes

Minorities in the pipeline (grades FR-27 through 29) to official staff increased by 13 percent, from 256 in 2012 to 289 in 2013.[1] The Board's outreach initiatives resulted in more diverse applicant pools for major job families, such as financial analyst and information technology (IT) professional. Out of a total of 409 hires, 167 were minorities. The minority hires included 15 Hispanics in the major job families.

Challenges and Next Steps

Although there was some improvement, there continue to be challenges in the hiring of Hispanics in the overall workforce, and in the hiring of minorities in the job families of economist, program analyst, and regulatory and business analyst.

To help improve the current state of low Hispanic representation, the Board has strengthened its recruiting for major job occupations through its relationships with professional associations and academic institutions, such as the Association of Latino Professionals in Finance and Accounting, the National Society of Hispanic MBAs, and universities with significant Hispanic representation (e.g., Florida International University, the University of Maryland, and the New Jersey Institute of Technology), and by sourcing applicants for internships through organizations such as the Hispanic Association of Colleges and Universities.

Further, the Board also anticipates exploring new sources for recruitment of Hispanics such as partnering with community colleges that have joint programs with four-year universities and colleges to identify juniors for summer internship positions. This will enable students to gain experience in critical job occupations and encourage future applicants and candidates for job opportunities after degree completion.

The Board continues to address low representation of minorities in the official staff as well as in the pipeline to become official staff. During calendar year 2013, the official staff had 20 new appointments, of

[1] Official staff is equivalent to Senior Executive Service.

which 14 were internal promotions. While 8 women were appointed, no minorities were appointed. This can be attributed to insufficient availability of minorities in the senior professional levels from grades FR-28 through 29 from which official staff is drawn. Although minorities were not appointed to the official staff of the Board in 2013, there was an increase of 36 percent in minority managers (grades FR-25 through 27). The potential for these managers to reach senior professional levels in the long-term should increase the number of minorities in the pipeline from which official staff is selected. Under a broad management mandate, succession planning and workforce planning strategy objectives are being established to ensure leadership and accountability in addressing this issue. In addition, during the initial stages of appointing official staff, the director of ODI is now consulted and is a member of the reviewing team (which also includes representatives from the Human Resources Department and the Division of Financial Management) that evaluates proposed actions. This allows the ODI director to better support inclusion and diversity at the official staff level and to ensure that the Board's leadership nomination criteria and process are inclusive.

The Board has also completed an availability analysis utilizing the 2010 Census civilian labor force data to determine minority representation in the major occupations of the Board. The census data continue to show significant low availability of minorities, particularly in the economist job occupation for all minority groups and women. To address this, the Board continues to organize, oversee, and participate in the three programs under the purview of the American Economic Association's Committee on the Status of Minority Groups in the Economics Profession (CSMGEP): (1) the Summer Economics Fellow Program; (2) the Summer Training Program; and (3) the Mentoring Program. The Board also plans to expand its participation at a number of recruitment and outreach events that target minority and women students and experienced professionals in the occupations of financial analyst, IT, quality assurance, system analyst, and attorney.

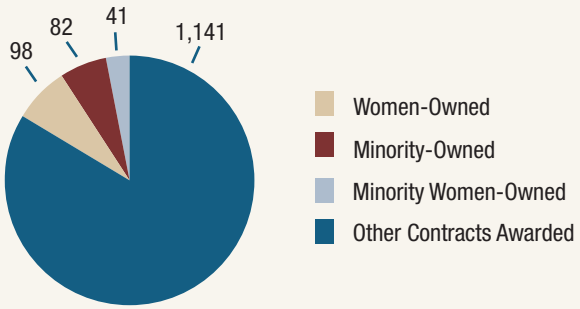
Inclusion of Minority-Owned and Women-Owned Businesses

The Procurement Function in the Board's Division of Financial Management continued to demonstrate a strong and positive commitment to the inclusion of minority-owned and women-owned businesses in the Board's acquisition process. As outlined below, a comprehensive program strategy was implemented by setting forth specific actions to assist the Board in fostering relationships with these types of businesses. This strategy contains objectives and activities that are aligned with the provisions of section 342 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) and will help position the Board to continue to cultivate positive relationships with minority-owned and women-owned businesses. Key elements of the program strategy include

- establishing a supplier diversity policy that reaffirms the Board's commitment to equal opportunity in the acquisition process;
- developing an internal and external communication plan, including the design and dissemination of informational brochures and the creation of an external website where vendors can register their companies with the Board and obtain information on upcoming procurement opportunities;
- creating a vendor management system that allows Procurement to track the status of minority-owned and women-owned businesses throughout the acquisition process;
- conducting capacity-building workshops;
- reviewing subcontractor plans from prime contractors; and
- preparing quarterly reports for senior management that describe the status and results of the Supplier Diversity Program.

Through implementation of the program strategy and through networking with minority-owned and women-owned firms, Procurement has made significant progress in fostering success for those firms seeking to do business with the Board.

Figure 1. Distribution of contracts awarded by the Board, 2013



Successes

The accomplishments of the Supplier Diversity Program complement the Board's long-standing commitment to support the inclusion of minority-owned and women-owned businesses in the procurement process. During 2013, the Board increased the number of contracts awarded to minority-owned and women-owned businesses. This was due in part to an increased focus on providing technical training, enhancing outreach activities, and holding meetings with senior leaders and division representatives to discuss their role and responsibility in implementing Dodd-Frank Act requirements related to supplier diversity. The Board awarded 1,362 contracts in 2013; figure 1 shows the distribution of those contracts among minority-owned businesses, women-owned businesses, minority women-owned businesses, and other businesses. The Board awarded contracts for goods and services in the amount of $158,196,516.[2] Of this total, $20,997,715, or 13.3 percent, was awarded to minority-owned or women-owned businesses. This represents a 54.9 percent increase in the dollar value of contracts awarded to minorities and

[2] This report describes the contracts awarded by the Board for the period January 1, 2013 through December 31, 2013. The dollar amount shown represents the estimated value of the contracts rather than the actual amount spent.

Table 5. Contract awards for minority-owned and women-owned businesses, 2011 through 2013

	2013[1]		2012[2]		2011[3]	
	Dollars	Percent	Dollars	Percent	Dollars	Percent
Minority-owned businesses[4]	$ 6,806,841	4.3	$ 3,726,415	2.6	$ 9,028,526	7.2
Women-owned businesses[4]	$11,520,842	7.3	$ 8,145,183	5.8	$ 4,237,038	3.4
Minority women-owned businesses	$ 2,670,032	1.7	$ 1,685,031	1.2	$ 2,148,583	1.7
Total	$20,997,715	13.3	$13,556,629	9.6	$15,414,147	12.3

[1] Total contracts awarded in 2013 were $158,196,516.
[2] Total contracts awarded in 2012 were $141,168,580.
[3] Total contracts awarded in 2011 were $125,070,569.
[4] Does not include contracts with minority women-owned businesses.

women in 2012. Table 5 summarizes the Board's contract awards for the period 2011–2013.

Outreach Activities

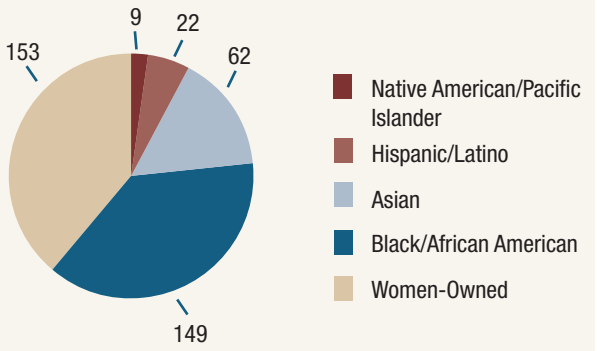
The Procurement Function implemented an effective outreach program to minority-owned and women-owned businesses. As part of these efforts, Procurement participated in events hosted by a wide array of organizations that promote the growth and development of minority-owned and women-owned businesses. A listing of these outreach events is shown in table 6.

The Board hosted its annual vendor outreach fair in May. The fair, which allows vendors to interact with the procurement staff and Board technical representatives, was an overwhelming success. More than 400 companies, along with the U.S. Small Business Administration, other federal financial regulatory agencies, the Federal Reserve Bank of Richmond, and 87 Board staff members participated in the event. Vendors were given the opportunity to learn about the Board's purchasing needs, to attend a seminar on "How to Do Business with the Board," and to discuss their business capabilities with Board representatives and staff from other agencies. Figure 2 shows a breakdown of companies participating in the fair.

Table 6. Supplier diversity outreach activities, 2013

National 8(a) Association Small Business Conference
Alliance Mid-Atlantic Small Business Procurement Fair
National Reservation Economic Summit for Native American Businesses
WBENC 2013 Summit & Salute to Women's Business Enterprises
U.S. Hispanic Chamber of Commerce Conference
Women-Owned Small Business National Council Contracting Summit
Federal Reserve Board's Annual Vendor Fair
Greater Washington Hispanic Chamber of Commerce (GWHCC) Business Exposition
Annual Government Procurement Conference
US Pan Asian CelebrASIAN
National Minority Supplier Development Council (NMSDC) Conference
U.S. Women's Chamber of Commerce Conference
American Small Business Chamber of Commerce
U.S. Black Chambers, Inc.
Congressional Black Caucus Foundation's Annual Legislative Conference

Figure 2. Participation of minority-owned and women-owned businesses at the Board's annual vendor fair, 2013



Providing Technical Assistance

A significant amount of time and effort was devoted to supplier development. Procurement provided guidance to interested vendors to help them be more competitive in the procurement process. Technical assistance included discussing how to do business with the Board, providing information on upcoming contracting opportunities, monitoring the period of performance during the life of the contract, and preparing post-contract award debriefs. Debriefs include the following information:

- an evaluation of significant weaknesses or deficiencies in the offeror's proposal;

- the overall cost or price and technical rating, if applicable, of the successful offeror and the debriefed offeror;
- past performance information on the debriefed offeror;
- the overall ranking of all offerors; and
- a summary of the rationale for the award to assist the offeror in preparing more comprehensive proposals for future acquisitions.

Internal Training and Automation Support

During 2013, Procurement enhanced the Contracting Officer Technical Representative (COTR) training to include discussions of Dodd-Frank Act requirements, the COTR's responsibility in supporting supplier diversity initiatives, and the competitive advantages of the inclusion of minority-owned and women-owned businesses.

Procurement also implemented a system to track the status of vendors throughout the acquisition process. This system allows the Board's staff to identify where barriers may exist within the acquisition process, and helps staff develop targeted technical training for vendors. Other automation initiatives included

- implementing a business intelligence reporting tool that provides trend analyses and dashboards to assist Procurement and Board divisions in evaluating their procurement activity;
- developing a web-based tutorial video, "How to Do Business with the Board," which will be located on the Board's public website when completed; and
- creating a link to expiring contracts on the Board's public website.

Challenges

Among the challenges faced by the Procurement Function in 2013 is the issue of vendors' self-designation of their status as a minority-owned or women-owned business. The Board currently accepts vendors' self-designation, which may result in inaccurate data classification. To address this issue, the Board plans to meet with the Women's Business Enterprise National Council (WBENC) and National Minority Supplier Development Council (NMSDC) to validate their certification procedures so that their certifications can be used during the Board's vetting process. This will help validate vendors' status more efficiently during the acquisition process.

In addition, Procurement continues to recognize the need to increase Board staff awareness and understanding of Dodd-Frank Act requirements as they relate to supplier diversity. Procurement and ODI have implemented a strategy to raise awareness within the agency that includes educating and training staff on the importance of supplier diversity, holding regular meetings with senior leadership to discuss the Supplier Diversity Program and garner their support, and engaging division leadership to work as champions by supporting the inclusion of minority-owned and women-owned businesses in their contracting opportunities.

Finally, Procurement is working to revise existing acquisition policies and procedures that have become outdated and do not reflect the objectives of the Supplier Diversity Policy approved in 2013. Acquisition policies and procedures are being revised to reflect the commitment and objectives of the Supplier Diversity Program.

Financial Literacy Activities

During 2013, the Board continued to participate in community and Federal Reserve System outreach events and programs, examples of which are listed below.

- *Congressional Black Caucus Annual Legislative Conference*: In September 2013, the Board, in conjunction with the Federal Reserve System, sponsored a booth at the 43rd Annual Legislative Conference. Financial education materials and information were distributed to conference attendees. The Board also provided support for the Financial Education Youth Summit convened by the Congressional Black Caucus held at the U.S. Capitol Visitor Center and Trinity Washington University.
- *FedEd Program*: During 2013, research assistants from divisions within the Board continued to implement a program developed to work with local high school students to improve their understanding of personal finances and the role of the Federal Reserve System in the economy. Subjects covered include the importance of saving, budgeting, using credit, establishing financial goals, and the impact of Federal Reserve policy on those subjects. More than 40 presentations were made to middle and high school students in the Washington metropolitan area. Presentations were made at ten schools in the District of Columbia: Roosevelt High School; Wilson High School; Coolidge High School; Dunbar High School; Anacostia High School; Ballou High School; Washington Latin Public Charter School; Edmund Burke School; KIPP DC Charter School; and St. Albans School. Presentations were made at two schools in Virginia—Annandale High School and Marshall High School—and one school in Maryland—Stone Ridge School of the Sacred Heart. Presentations were also made at the District of Columbia Public Schools Central Office to preview the FedEd Program for the New Heights Providers Meeting, the Sumner School for the DC Future Business Leaders of America, and the Heights School.
- *Federal Reserve Financial Literacy Day*: On October 23, 2013, the Board and the Federal Reserve System held training programs and seminars around the country on such topics as saving, budgeting, credit use, and the establishment of financial goals. Board research assistants presented the program to classes at two schools in the District of Columbia: Cardozo High School and the Columbia Heights Education Campus.
- *Math x Economics*: On May 23, 2013, the Board hosted the Math x Economics program for a second year in a row. The goal of the program was to introduce students to economics as a potential course of study in college and as a future career option. The Board's recruitment efforts targeted groups who are underrepresented in the field of economics, including minorities and females, especially from underserved schools. A total of 29 students from Washington metropolitan area schools attended. The students completed a survey at the end of the program; all 29 participants said they would recommend the program to other students. The descriptive statistics of the respondents are listed below.

Distribution of participants	Percent
Female	56
Male	44
Juniors	78
Seniors	22
African American	25.9
Hispanic	18.5
Asian	18.5
White	18.5
More than one ethnicity	14.8
Did not specify ethnicity	3.7

- *Education and Training Materials Distribution*: During 2013, the Board continued to provide financial literacy materials to consumer education and financial literacy groups, including the University of Maryland Extension Family and Consumer Sciences Center, the YMCA of Metropolitan Washington, Operation HOPE, and It Takes a Community to Raise a Child (located in New York City).
- *Professional Outreach*: On April 3, 2013, Chairman Bernanke delivered remarks to the 13th Annual Redefining Investment Strategy Education (RISE) Forum. His remarks highlighted the importance of promoting economic and financial knowledge among people of all ages and walks of life. He stated that the Board and the 12 Federal Reserve Banks are all deeply involved in economic education and in supporting the work of teachers, schools, and national organizations.

On November 13, 2013, Chairman Bernanke hosted the annual Teacher Town Hall Meeting at the Federal Reserve Board. Federal Reserve Banks also held gatherings around the country to provide educators the opportunity to listen to the Chairman and ask questions. His remarks covered the origins, history, and role of the Federal Reserve, and how it has helped shape the nation's economy and financial system.

Diversity Policies and Practices of Regulated Entities

In 2013, an interagency working group comprising the financial agency OMWI directors (the Board, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the National Credit Union Administration, the Consumer Financial Protection Bureau, and the Securities and Exchange Commission) published proposed standards for assessing the diversity policies and practices of entities regulated by each agency. The proposed standards were published in the *Federal Register* on October 25, 2013, for public comment; the comment period was later extended to February 7, 2014.[3]

The interagency working group is meeting to review all comments received and expects to adopt final standards in 2014.

---

[3] See the *Federal Register* notices at www.gpo.gov/fdsys/pkg/FR-2013-10-25/pdf/2013-25142.pdf and www.gpo.gov/fdsys/pkg/FR-2013-12-24/pdf/2013-30629.pdf.

Appendix A: EEO-1 Report for the Board of Governors of the Federal Reserve System for Calendar Year 2013

Employer Information Report EEO-1

Federal Reserve Board, 2013 Employer Information Report

Occupational Categories	Total Employees			Race/Ethnicity													
						Non- Hispanic or Latino											
				Hispanic or Latino		White		Black or African American		Asian		Native Hawaiian or Other Pacific Islander		American Indian or Alaska Native		Two or More Races	
	All	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female
1.1 Exec. Sr. Level Managers, Governors, Officers, FR-29 & FR-28																	
By total	384	231	153	4	6	187	107	23	29	16	9	1	2	0	0	0	0
By percent	100.00%	60.16%	39.84%	1.05%	1.56%	48.70%	27.86%	5.99%	7.55%	4.17%	2.34%	0.26%	0.52%	0.00%	0.00%	0.00%	0.00%
1.2 1st/Mid. Level																	
By total	85	38	47	1	2	17	23	17	19	3	3	0	0	0	0	0	0
By percent	100.00%	44.71%	55.29%	1.18%	2.35%	20.00%	27.06%	20.00%	22.35%	3.53%	3.53%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Officials and Managers Total																	
By total	469	269	200	5	8	204	130	40	48	19	12	1	2	0	0	0	0
By percent	100.00%	57.36%	42.64%	1.07%	1.71%	43.50%	27.72%	8.53%	10.23%	4.05%	2.56%	0.21%	0.43%	0.00%	0.00%	0.00%	0.00%
2. Professionals																	
By total	1,641	894	747	49	34	594	366	90	184	139	150	20	13	0	0	2	0
By percent	100.00%	54.48%	45.52%	2.99%	2.07%	36.20%	22.30%	5.48%	11.21%	8.47%	9.14%	1.22%	0.80%	0.00%	0.00%	0.12%	0.00%
3. Technicians																	
By total	6	2	4	0	0	0	2	2	2	0	0	0	0	0	0	0	0
By percent	100.00%	33.33%	66.67%	0.00%	0.00%	0.00%	33.33%	33.33%	33.33%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
4. Sales Workers																	
By total	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
By percent	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
5. Admin. Support Workers																	
By total	136	24	112	1	5	5	13	17	86	1	4	0	2	0	2	0	0
By percent	100.00%	17.65%	82.35%	0.74%	3.68%	3.68%	9.56%	12.50%	63.24%	0.74%	2.94%	0.00%	1.47%	0.00%	1.47%	0.00%	0.00%
6. Craft Workers																	
By total	41	40	1	0	0	21	0	14	1	4	0	1	0	0	0	0	0
By percent	100.00%	97.56%	2.44%	0.00%	0.00%	51.22%	0.00%	34.15%	2.44%	9.76%	0.00%	2.44%	0.00%	0.00%	0.00%	0.00%	0.00%
7. Operatives																	
By total	11	11	0	0	0	0	0	11	0	0	0	0	0	0	0	0	0
By percent	100.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
8. Laborers and Helpers																	
By total	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
By percent	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
9. Service Workers																	
By total	152	124	28	7	0	38	3	76	23	3	1	0	1	0	0	0	0
By percent	100.00%	81.58%	18.42%	4.61%	0.00%	25.00%	1.97%	50.00%	15.13%	1.97%	0.66%	0.00%	0.66%	0.00%	0.00%	0.00%	0.00%
Total Workforce																	
By total	2,456	1,364	1,092	62	47	862	514	250	344	166	167	22	18	0	2	2	0
By percent	100.00%	55.54%	44.46%	2.52%	1.91%	35.10%	20.93%	10.18%	14.01%	6.76%	6.80%	0.90%	0.73%	0.00%	0.08%	0.08%	0.00%

www.federalreserve.gov
0414

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

September 30, 2014

MEMORANDUM

TO: Board of Governors

FROM: Mark Bialek
Inspector General

SUBJECT: The OIG's List of Major Management Challenges for the Board

We are pleased to provide you with the Office of Inspector General's (OIG) first listing of major management challenges facing the Board of Governors of the Federal Reserve System (Board). These challenges represent what we believe to be the areas that, if not addressed, are most likely to hamper the Board's accomplishment of its strategic objectives.

We used audit and evaluation work performed by the OIG, audits performed by the U.S. Government Accountability Office, and the Board's strategic planning documentation to identify the Board's major management challenges, which are listed in the table below.

Management challenge no.	Description	Attachment 1 page no.
1	Continuing to implement a financial stability regulatory and supervisory framework	1
2	Human capital	3
3	Board governance	5
4	Capital improvement projects	8
5	Information security	11

Details on each challenge are in attachment 1 of this memorandum. Attachment 2 maps our ongoing and planned work related to the major management challenges we have identified for the Board.

We appreciate the cooperation that we received from the Board as we developed this listing of challenges. Feel free to contact me if you would like to discuss any of the challenges.

Attachments

cc: Scott Alvarez, General Counsel, Legal Division
Eric Belsky, Director, Division of Consumer and Community Affairs
Michell Clark, Director, Management Division
Robert deV. Frierson, Secretary of the Board, Office of the Secretary
William English, Director, Division of Monetary Affairs
Michael Gibson, Director, Division of Banking Supervision and Regulation
Donald Hammond, Chief Operating Officer, Office of the Chief Operating Officer
Steven Kamin, Director, Division of International Finance
J. Nellie Liang, Director, Office of Financial Stability Policy and Research
William Mitchell, Chief Financial Officer and Director, Division of Financial Management
Sharon Mowry, Chief Information Officer and Director, Division of Information Technology
Louise Roseman, Director, Division of Reserve Bank Operations and Payment Systems
Michelle Smith, Assistant to the Board, Chief of Staff, and Director, Office of Board Members
David Wilcox, Director, Division of Research and Statistics

Attachment 1

Major Management Challenges for the Board of Governors of the Federal Reserve System, September 2014

Management Challenge 1: Continuing to Implement a Financial Stability Regulatory and Supervisory Framework

As outlined in the Board of Governors of the Federal Reserve System's (Board) *Strategic Framework 2012–15*, continuing to build a robust infrastructure for regulating, supervising, and monitoring risks to financial stability remains a strategic priority for the agency. The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) provided the Board with the authority to oversee nonbank financial companies designated by the Financial Stability Oversight Council (FSOC) as systemically important. In Supervision and Regulation Letter 12-17, the Board outlined its updated framework for consolidated supervision of large financial institutions as a result of lessons learned during the financial crisis. While Supervision and Regulation Letter 12-17 provides a high-level description of the framework and priorities for consolidated supervision for large institutions, including nonbank systemically important financial companies, we understand that the supporting guidance necessary to fully implement the framework is forthcoming. Finalizing the supporting guidance and effectively implementing it through examiner training programs will be a challenge for management in the coming years. The following sections describe specific challenges associated with implementing the financial stability regulatory and supervisory framework.

Cultivating Effective Relationships With Other Regulators

Effective consolidated supervision is predicated on the Board, as the consolidated supervisor for bank, financial, and savings and loan holding companies, cultivating strong cooperative relationships with the primary supervisors of holding company subsidiaries. Our evaluation work has revealed instances in which this cooperation could be improved.

Agency Actions

Since 2013, senior Board officials have made significant efforts to coordinate with their counterparts at the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation to align strategic objectives and minimize duplication of efforts with respect to the supervisory planning process. We also understand that similar efforts routinely occur at the examination-team level.

Finalizing and Ensuring Compliance With New Regulations

While the Board has finalized many of the regulations mandated by the Dodd-Frank Act and other significant rulemakings supporting the financial stability framework, such as the Basel III capital rules, some rulemakings remain in the comment phase or have yet to be finalized. For example, the comment period for the Board's proposal to amend its emergency lending regulations to conform to the requirements of the Dodd-Frank Act has closed, but the rules have yet to be finalized.[1]

Further, the Board will face challenges as its focus shifts from rulemaking to interpreting the rules and ensuring compliance with recently issued regulations. As an example of challenges related to interpreting rules, we understand that following the issuance of the Basel III capital rules, responding to industry questions for interpretive guidance became a priority for the Board. With regard to ensuring compliance, the Volcker Rule took effect in April 2014, and the Board has indicated its intent to hold banks accountable for complying with the requirements of the final rule starting in July 2015. Under delegated authority from the Board, Federal Reserve Bank examiners will be expected to monitor and enforce compliance with prohibitions and restrictions related to proprietary trading and certain relationships with hedge funds or private equity funds. Supervisory guidance on this topic needs to be issued, and examiners will need to be trained on how to assess compliance with the rule's provisions. Similar training and implementation challenges also exist for other significant rulemakings.

Agency Actions

The Board has made considerable progress in fulfilling the regulatory mandates outlined in the Dodd-Frank Act and in finalizing other significant rulemakings supporting the financial stability framework. Our office will assess the Board's progress toward implementing its supervisory approach for these new, complex regulations.

Developing Technology Infrastructure and Addressing Human Capital Challenges Associated With Monitoring Risks to Financial Stability

The Board faces operational and human capital challenges associated with its efforts to supervise and monitor risks to financial stability. Within the large bank portfolio, our evaluation work has revealed that supervisory teams have encountered challenges searching through the significant amounts of supervisory information that result from the Board's continuous monitoring activities. Within the regional and community bank portfolios, we understand that the Board is in the process of transitioning to a technology platform that will standardize the processes for conducting examinations across the Federal Reserve Banks. This project requires a multiyear implementation effort. The Board also faces challenges in attracting and retaining employees

1. The status of Dodd-Frank Act rulemakings is available on the Federal Reserve Bank of St. Louis's website at http://www.stlouisfed.org/regreformrules/index.aspx.

with the specialized subject-matter expertise necessary to execute its supervisory activities, as further discussed in the human capital management challenge.

Agency Actions

The Board recently improved supervisory teams' search capabilities for informal supervisory information related to specific institutions. Information previously stored in specific Lotus Notes databases has been transitioned to internal websites to facilitate these enhanced search capabilities. We also understand that the INSite platform will be implemented for the regional and community bank portfolios using a phased approach over multiple years.

Management Challenge 2: Human Capital

The Board's success in achieving its mission depends on having the right number of people with the necessary technical, managerial, and leadership skills. Accordingly, human capital is one of the key themes in the Board's *Strategic Framework 2012–15*. As the Board's framework notes, maximizing the value of the Board's human capital will depend on enhancing processes for effective recruitment, development, and retention of qualified staff. A key first step in ensuring that the Board has a workforce that can effectively carry out the Board's mission both now and in the future is identifying the critical technical, managerial, and leadership skills through workforce and succession planning. The Board faces challenges in maintaining the necessary skill sets due to competition for highly qualified staff and the difficulties associated with replacing employees who have the specialized knowledge and skill needed to fulfill the Board's mission. In addition, the Board will face challenges as it implements a new performance management process and continues its efforts to recruit and retain a more diverse workforce.

Identifying Mission-Critical Technical, Managerial, and Leadership Skills Through Workforce and Succession Planning

The Board will need to determine the skill sets and number of staff members needed to enable each division to efficiently and effectively accomplish its goals. The U.S. Government Accountability Office (GAO) congressional testimony highlighted the need for federal agencies to identify and address current and emerging critical skills gaps to reduce the risk of staffing shortfalls that could jeopardize agencies' efforts to accomplish their missions. In its 2003 report *Human Capital: Key Principles for Effective Strategic Workforce Planning*, GAO highlights effective principles for workforce planning that include determining the critical skills and competencies needed to achieve an agency's mission, along with strategies to address skill and competency gaps.

An important consideration in workforce planning is the need to develop a succession plan to ensure continuity of knowledge and leadership in key positions. The Board has noted the operational risks associated with staff retirement and turnover and the difficulties associated with replacing employees with specialized knowledge and skill sets. Failure to plan for and anticipate

turnover and departures could have a negative effect on the Board's ability to achieve its goals and fulfill its mission. In addition, the Board has experienced turnover in the leadership of various divisions, highlighting the need for clear succession plans. In a 2005 report on succession planning, GAO encourages federal agencies to "go beyond a succession planning approach that focuses on replacing individuals and engage in broad, integrated succession planning and management efforts that focus on strengthening current and future organizational capacity." To ensure that the Board successfully achieves its mission, each division will need to identify its current and emerging skill needs, develop and implement a plan to address any identified skill gaps, and ensure that leadership development is a component of its succession planning.

Agency Actions

In its strategic framework, the Board acknowledged the need to establish a Boardwide succession planning process, which will require considerable support across all divisions. The *2012–2015 Human Resources Strategic Plan* also identifies leadership development as a key focus area. In support of these objectives, the Board formed a Leading and Managing People workgroup, composed of senior managers and officers across divisions. The purpose of this workgroup is to develop leadership capacity, including but not limited to introducing leadership coaching, creating case studies to define successful and unsuccessful leadership skills, and developing a list of core competencies expected of leaders. The Board has also successfully implemented a new manager development program, which it is expanding to include senior Board officials, and has begun using a succession planning tool.

Implementing a New Performance Management Process

In early 2013, the Board elected to change how employees approach and use individual performance feedback. The Board is currently developing and implementing a new performance management program intended to align staff members to the work of the Board, provide greater accountability, and support employee development. The new program seeks to be a more forward-looking, development-centric process in which staff members and managers work together for the greater effectiveness of the Board. The new performance management program is a significant change for the Board. The Board will need to ensure that the new process is effective, fair, and not overly burdensome, while simultaneously maintaining distinctions between high and low performers. Ensuring a successful paradigm shift from a rating-centric process to a development-centric process for assessing employee performance, as well as ensuring that a consistent approach is followed across the Board, will be a challenge for the Board.

Agency Actions

The Board introduced the new performance management process as a pilot in six divisions for performance year 2013–2014. Full implementation in all divisions is planned for performance year 2014–2015. The Board contracted for the necessary

expertise to assist with the program's implementation, which includes information sessions, tools and guides, training, and other support.

Recruiting and Retaining a Diverse Workforce

The Board's policy is to provide equal opportunity in employment for all persons. In support of this commitment, the Board has established strategic objectives to attract, hire, develop, promote, and retain a highly diverse workforce. A diverse workforce is one that not only includes employees with a wide variety of attributes but also is rich in diversity of thought and perspective. According to the Office of Personnel Management's *Government-Wide Diversity and Inclusion Strategic Plan*, harnessing the innovation that can come from a diverse workforce will help agencies to realize full performance potential and to cultivate a high-performing organization. Although the Board has undertaken a number of activities to increase diversity, it noted continuing challenges in hiring minorities in its April 2014 *Report to the Congress on the Office of Minority and Women Inclusion.* In April 2013, GAO reported that federal agency officials said the main challenge to improving diversity was identifying candidates, noting that minorities and women are often underrepresented in both internal and external candidate pools.

Agency Actions

To successfully achieve its diversity goals and objectives, the Office of Human Resources plans to partner with divisions to design, develop, and implement an integrated Boardwide talent management strategy. This strategy will facilitate the management of a diverse workforce throughout all phases of the employee life cycle, which includes recruiting, engaging, retaining, and developing employees. Building on each phase of the life cycle will enable the Board to create an integrated approach to managing talent. An enterprise-wide talent management strategy that identifies the basic competencies every employee should possess will allow the Board to assess performance and to develop and retain talent. In addition, the Board continues to address challenges to improving diversity by participating in educational forums and offering mentoring programs and summer internships.

Management Challenge 3: Board Governance

Historically, the Board's divisions have operated largely autonomously in performing their specified mission functions, developing organizational structures, formulating budgets, and establishing management processes. As the Board's mandate expanded in the wake of the financial crisis and the enactment of the Dodd-Frank Act, so has the Board's need for strategic planning, management processes, and coordination across divisions. In its *Strategic Framework 2012–15*, the Board lists three strategic themes that address various aspects of its governance challenges:

- strengthening management processes to enable effective implementation of strategic themes, increasing operating efficiencies, and reducing administrative burden

- establishing a cost-reduction approach and a budgetary growth target that maintains an effective and efficient use of financial resources
- redesigning data governance and management processes to enhance the Board's data environment

The Board's strategic framework states that achieving its strategic objectives will require more active collaboration across divisions. Collaboration will be required to fulfill the Board's supervisory expectations under the Dodd-Frank Act as well as its traditional monetary policy functions. Collaboration will also be required to carry out the Board's agenda of management process changes to keep major investments on track, identify additional opportunities for cost savings, and improve overall operations. Enhancements to the Board's management processes will allow for increased ownership of and accountability for leadership decisions, an enhanced ability to prioritize strategic needs, and a potentially reduced administrative burden. We believe that aspects of Board governance, including internal control, information technology (IT), and data, will continue to pose management challenges to the Board's efficient accomplishment of its mission.

Internal Control Governance

Internal control is an integral part of managing an organization and is critical to improving organizational effectiveness and accountability. Internal control comprises the plans, methods, and procedures used to meet the organization's mission, goals, and objectives. The Federal Managers' Financial Integrity Act of 1982 (FMFIA) requires that each executive agency establish internal accounting and administrative controls in compliance with standards established by GAO and prepare an annual statement on internal control based on an evaluation performed using Office of Management and Budget guidelines. The Board is not subject to FMFIA.

Although the Board has stated that it voluntarily complies with the spirit and intent of FMFIA, it does not currently have a Boardwide process for maintaining and monitoring its administrative internal controls. Office of Inspector General (OIG) work has identified internal control weaknesses at the Board. While these control weaknesses have not prevented the Board from carrying out its mission or achieving its strategic objectives, some of them have introduced operational and reputational risks. Establishing a process for maintaining and monitoring internal controls will help ensure that the Board's controls, as designed and implemented, are effective and continue to work over time. Establishing a Boardwide process to monitor internal controls will also provide a means for the Board to identify and timely mitigate any control weaknesses that exist.

Agency Actions

Board management identified actions that it plans to take in 2014 to implement a process for maintaining and monitoring administrative internal controls. Management plans to (1) develop a Board policy describing the requirements for appropriate administrative internal controls based on the guidance provided by the Committee of Sponsoring

Organizations of the Treadway Commission[2] and GAO, (2) implement the new policy using a phased approach, (3) require each Division Director to provide a reliance letter acknowledging that the division is responsible for implementing and maintaining internal controls, and (4) develop training on administrative internal controls and the Board's policy. Management noted that given the priorities and budget constraints underlying the Board's new strategic framework, creating additional infrastructure to develop and implement policies and processes must be carefully balanced with other competing resource priorities.

IT Governance

The Board also faces governance challenges in both the centralized and decentralized management of IT services. A primary mission of the Division of Information Technology (Division of IT) is to provide services to meet the automation and data analysis needs of its customers; however, divisions also provide IT services to their employees. Our recent audit work found that over half of Board divisions perform their own application development and help desk activities, often using differing processes, procedures, and tools. We also found that Board divisions do not track costs for IT services in a consistent manner.

Agency Actions

The Board recently approved new delegations of authority that grant the Director of the Division of IT the authority for automation, telecommunications, and other IT matters; information security; and the formulation, approval, and implementation of the management policies for IT and information security.

The Director of the Division of IT chairs the Board's Business Technology Strategic Committee, which comprises senior IT representatives from each division. The purpose of the committee is to promote an enterprise view of the implementation and administration of IT services in a consistent, cost-sensitive, and secure manner that is informed by business needs. The Director of the Division of IT recently updated and finalized the committee's charter to increase coordination among the divisions; she also continues to hold discussions on strategic collaboration.

In 2013, the Director of the Division of IT administered a survey of IT costs across the divisions to help the Board better understand the scope and diversity of the technology services provisioned across the enterprise. Also, the Business Technology Strategic Committee designed a survey to collect information from each Board division and office to identify opportunities to improve operational efficiency.

---

2. The Committee of Sponsoring Organizations of the Treadway Commission's internal control framework is widely used and recognized as a leading framework for designing, implementing, and evaluating the effectiveness of internal control. It integrates various internal control concepts into a framework in which a common definition is established and control components are identified. The commission's internal control framework was updated in May 2013 with a transition period ending December 15, 2014.

Data Governance

As a result of expanded responsibilities under the Dodd-Frank Act, the Board is engaging in new data collection and analysis. New data collection and data management processes are required to perform these new responsibilities. The need for data across the divisions to support the Board's analytical challenges has also increased in terms of the quantity, sharing, awareness, access, controls, and quality. Traditionally, data were used within divisions to accomplish specific mission functions; however, to fulfill the Board's expanded responsibilities, divisions now need to increase coordination with each other and with the Board's new Office of Financial Stability Policy and Research, and they need to support the Board's participation in FSOC. A Boardwide data management view is needed to enhance the ability of staff members to obtain, interpret, and analyze these data. The Board will be challenged to expand its technology infrastructure and processes to support the increased requests for and analysis of data, as well as to enable comprehensive, enterprise-level data governance and information management practices.

Agency Actions

In the *Strategic Framework 2012–15*, the Board outlined the role of a new Chief Data Officer (CDO) position. The first CDO was hired in April 2013. The CDO is working with the Board Data Council and Board divisions to establish data governance policies and to facilitate coordination across data communities at the Board and among the Board; the Federal Reserve Banks; and other regulatory agencies, such as FSOC and the U.S. Department of the Treasury's Office of Financial Research.

A new Boardwide data governance and management structure is planned to support the growing need to share large amounts of data across divisions. The CDO is reviewing the current data collections, engaging divisions, and developing a cohesive enterprise data governance framework.

Management Challenge 4: Capital Improvement Projects

The Board is currently managing two major capital improvement projects that are included as key themes in the Board's *Strategic Framework 2012–15*: the Martin Building renovation and construction and the relocation of the Board's data center. Both are multiyear projects that involve significant resources and pose challenges due to their size, complexity, and effect on the Board's staff members and mission. In addition, managing large-scale construction projects is not a core function of the Board.

The Martin Building facility has not been significantly renovated since its construction in 1974. In addition to ensuring a safe and adequate environment in which individuals and groups can work and meet, efforts associated with the renovation will focus on security, energy efficiency, meeting and conference space, and physical plant capacity. Relocating the data center is critical because the Board needs increased storage capacity for the data essential to its mission. As currently planned, the relocation of the Board's data center will overlap with the Martin Building project, creating an additional challenge as the Board attempts to oversee and manage both

projects. In addition to managing these projects, the Board will have to adapt its space-planning and leasing activities due to the Martin Building project. The Board will need to manage the swing space acquired to accommodate its significant workforce growth as well as staff members displaced from the Martin Building during the construction period.

Martin Building Renovation and Construction

The Martin Building renovation and construction project is one of the Board's largest contracting efforts, and it will require an estimated $280 million expenditure. The concept for the project began shortly after the events of September 11, 2001. Since the original concept was developed, the Martin Building project has gone through a lengthy design phase, primarily due to significant scope changes. In addition, project management has been complicated by changes in the Board's organizational structure and leadership.

The Martin Building renovation and construction project is a complex undertaking with significant implementation risks and challenges that the Board must manage. These risks include scope changes, cost management, and disruption to staff members during the renovation. Delays during construction could lead to contractor claims and increased costs for the Board due to the size of the construction contract and the nature of construction work. Many parties are involved in the construction life cycle process, and interdependencies exist. As a result, delays could cascade and affect the timing and sequencing of others' work.

In September 2012, the Martin Building project team presented an overall conceptual construction cost estimate of $179.9 million to the Committee on Board Affairs. The project was approved as a strategic plan project, and the capital portions of the project are currently included as a multiyear capital project in the Board's *2013 Budget as Approved by the Board of Governors.* Our audit of this conceptual construction cost estimate identified opportunities for the Board to improve its recordkeeping, cost estimation, and cost management processes for the Martin Building project.

Agency Actions

Since 2011, the Board has hired personnel with construction experience. In addition to the project team, an executive team and the Executive Oversight Group were established to be strategic advisors to the Martin Building renovation and construction project. The project team purchased software that provides collaboration, project management, and information management applications specifically for the architectural, engineering, design, and construction business sector. In addition, the project team is currently maintaining files initiated by the former project manager to fulfill contracting officer technical representative and project recordkeeping responsibilities. After receiving independent cost reviews, a stated cost limitation was established with the architectural and engineering firm, and the firm submitted cost-saving items to aid in cost management.

Relocation of the Board's Data Center

A key consideration of the Martin Building renovation and construction project is the future of the data center. The Board has undertaken a multiyear project to move its data center from the Martin Building to the Baltimore Branch of the Federal Reserve Bank of Richmond. The Board is relocating the data center because the growing number of file servers, network racks, and network switches has dramatically increased the footprint of data center operations. Critical subsystems for cooling and power have exceeded their capacity. The data center relocation is a major element of the third theme in the Board's *Strategic Framework 2012–15*, and the multiyear data center project is composed of four overlapping phases, with completion scheduled for December 2015.

Relocating the Board's data center within the approved budget and schedule will pose challenges to the Board. The start of the Martin Building renovation and construction project is contingent on completion of the data center relocation. The construction phase of the data center relocation project has an aggressive schedule with several identified risk areas. The initial planning schedules for the Martin Building project and the completion of the data center project have a six-month overlap; therefore, delays in the data center schedule could affect the Martin Building project. The Board's data center operates 24 hours a day, 365 days a year, to monitor the operation of the Board's mainframe and the status of the file servers and other critical components of the Board's distributed network. The data center provides the infrastructure that makes data and IT available to the Board and to the Federal Reserve System for monetary policy, financial supervision, consumer protection, and economic research purposes.

The Board has approved $201.5 million as the overall budget for the project. The budget was based on a 10-year total cost of ownership estimate based on a rough order of magnitude. As the actual build-out work begins, additional changes and cost increases are possible, which could potentially affect the budget.

Agency Actions

The Federal Reserve Bank of Richmond is responsible for the build-out of the data center, and it designated a project manager to oversee the project. The Board designated a program manager and a project manager, both within the Division of IT, to oversee the project in coordination with a team composed of members with experience in IT, procurement, and financial management, among other areas. There is also an Executive Oversight Group that oversees and provides guidance on the project and ensures that the Board's strategic objectives are being met.

Space Planning and Leasing

The Board currently occupies space in several buildings in Washington, DC. The Board's overall staffing level has grown significantly over the last several years, and continued growth is expected in some of its divisions. The Board is challenged with accommodating both the expected growth of its workforce and the placement of staff members in swing space due to the

Martin Building renovation and construction project, while also effectively managing its existing real property assets.

The Board acknowledges the need to focus on its long-term space requirements while also considering, in the context of its strategic framework, factors such as the current space environment, building location limitations, the projected growth of the organization, technological requirements, the implications of telework, and the operational effects and life cycle costs of all options. Considering these factors will help the Board to develop a meaningful approach for the most efficient and effective use of space.

Agency Actions

The Board signed a 10-year lease for swing space to relocate staff members displaced by the Martin Building renovation. To accommodate anticipated growth in some divisions, the Board plans to retain that space after the renovation is complete. Recognizing that it needs to take a more consistent approach to space planning, the Board is developing a standard process for allocating and managing its space. The Board is also developing a strategic master plan for space planning, and it contracted for real estate advisory services to assist with this effort. This plan is intended to inform the decisions of the Board's senior leadership regarding the Board's space needs.

Management Challenge 5: Information Security

GAO continues to include as a priority for federal agencies the protection of information systems and the nation's cybercritical infrastructures. The OIG has also identified information security as a major management challenge for the Board. Management should place a high priority on implementing new federal requirements for developing a Boardwide continuous monitoring program and a Boardwide risk management program. In addition, the Board is challenged to ensure that information systems and services provided by third-party providers, including the Federal Reserve Banks, meet the requirements of the Federal Information Security Management Act of 2002 (FISMA) and the Board's information security program.

Continuous Monitoring of Information Security

Implementing Boardwide continuous monitoring of information security that complies with National Institute for Standards and Technology (NIST) requirements will pose challenges for the Board. NIST requires that agencies establish a continuous monitoring strategy and implement a continuous monitoring program that includes a configuration management process for the information system and its constituent components, a determination of the security impact of changes to the information system and the environment of operation, ongoing security control assessments in accordance with the organizational continuous monitoring strategy, and a reporting of the security state of the information system to appropriate organizational officials.

NIST Special Publication 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* (SP 800-137), states that at the mission/business processes tier, the organization needs to establish the minimum frequency with which each security control or metric is to be assessed or monitored. Frequencies need to be established across all organizational systems and common controls. SP 800-137 states that the organization-wide information security continuous monitoring strategy and associated policy should be developed at the organizational tier, with general procedures for implementation at the mission or business tier. OIG reports have identified that the Board's Chief Information Officer has continued to make progress in implementing a continuous monitoring program; however, the Chief Information Officer should finalize policies and procedures, establish metrics, and define the frequency of monitoring.

Agency Actions

The Board's Information Security Officer (ISO) outlined a strategic plan for the Board and has made progress in implementing NIST guidance. The initial plan for continuous monitoring was developed in 2011 and was updated in August 2012 to include additional continuous monitoring automation tools and to provide more detailed implementation status information. In August 2013, the ISO evolved the continuous monitoring strategy into an *Information Security Continuous Monitoring Program* document, which discusses three primary activities: continuous monitoring automation, manual processes, and key metrics. Lastly, the ISO developed a draft version of the continuous monitoring standard.

Risk Management

Implementing Boardwide risk management will pose challenges to the Board. Although the majority of the Board's computing environment is managed by the Division of IT, NIST requires that the risk management program be expanded to address and cover all aspects of the Board's computing environments within all divisions' missions and business processes.

FISMA requires organizations to develop and implement an organization-wide information security program for the information and the information systems that support the operations and assets of the organization, including those provided or managed by another organization, a contractor, or another source. NIST Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, expands the concept of risk management and covers a strategic-to-tactical organizational approach to risk management. NIST Special Publication 800-39, *Managing Information Security Risk*, states that it is imperative that leaders and managers at all levels understand their responsibilities and are held accountable for managing information security risk—that is, the risk associated with the operation and use of information systems that support the mission and business functions of their organizations. OIG reports have identified that the Board's Chief Information Officer has continued to make progress in implementing a risk management program; however, the program still needs to be implemented Boardwide.

Agency Actions

The ISO developed the *Risk Management Program and Risk Assessment Guide* to enhance the original risk assessment framework initiative.

Reliance on the Federal Reserve Banks and Third-Party Providers

The Board will be challenged to ensure that information systems and services provided by third-party providers, including systems supported by the Federal Reserve Banks while they transition to a NIST-based information security program, meet FISMA requirements. FISMA requires agencies to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, a contractor, or another source. The Board's information security program requires third parties, including Federal Reserve Banks, other agencies, and commercial providers, to use appropriate security controls to protect Board-provided information and services. The level of controls provided by third parties must be comparable to the controls provided for in NIST requirements.

The Board is part of the Federal Reserve System and relies on some services provided through the Federal Reserve Banks; however, the Federal Reserve Banks are not bound by the requirements of FISMA. We have issued information security control review reports to the Board that identified services provided by third-party providers, including Federal Reserve Banks, that did not meet the Board's information security requirements.

Agency Actions

The Federal Reserve System is currently implementing NIST guidance as the strategic direction for the Federal Reserve Bank information security program. The information security program defines the rules, such as the security objectives and control requirements, and the risk management process that help the Federal Reserve System manage information security risk.

The ISO performs onsite security reviews of Federal Reserve Bank systems that store or process Board data to ensure that the systems are meeting the requirements of the Board's information security program. The ISO has developed a security policy that applies to all third parties that collect or maintain Board information or those that operate or use information systems on behalf of the Board. The ISO also published an inventory guide that outlines how the Board accounts for all information assets and tracks the security compliance of all systems, including systems used or operated by third parties on behalf of the Board.

Attachment 2

Board Management Challenges: Crosswalk to Ongoing and Planned OIG Work

Management Challenge 1: Continuing to Implement a Financial Stability Regulatory and Supervisory Framework

Ongoing work

- Evaluation of the Federal Reserve's Supervisory Activities Related to the Loss at JPMorgan Chase & Co.'s Chief Investment Office
- Evaluation of the Division of Banking Supervision and Regulation's Model Risk Management Practices for Models Used in Support of the Annual Comprehensive Capital Analysis and Review

Planned work for 2014

- Audit of the Board's Process for Supervisory Assessments of Large Bank Holding Companies and Savings and Loan Holding Companies
- Evaluation of the Board's Continuous Monitoring Supervisory Tool
- Evaluation of Systemically Important Financial Institutions Supervision Teams: Preserving and Transferring Institutional Knowledge Within and Between Supervisory Teams
- Audit of the Board's C-SCAPE Project

Management Challenge 2: Human Capital

Ongoing work

- Audit of the Board's Diversity and Inclusion Processes

Planned work for 2014

- Evaluation of Systemically Important Financial Institutions Supervision Teams: Preserving and Transferring Institutional Knowledge Within and Between Supervisory Teams

Management Challenge 3: Board Governance

Ongoing work

None

Planned work for 2014

- Audit of the Board's Data Governance
- Audit of the Board's Strategic Plan Implementation and Governance

Management Challenge 4: Capital Improvement Projects

Ongoing work

- Audit of the Board's Data Center Relocation—Phase 2

Planned work for 2014

- Follow-Up on Martin Building Audit

Management Challenge 5: Information Security

Ongoing work

- 2014 Audit of the Board's Information Security Program
- Audit of the Board's STAR Modernization Project
- Audit of the Board's Information Technology Contingency Planning and Continuity of Operations Program
- Security Control Review of the C-SCAPE System

  Audit of the Information System Security Life Cycle Process

Planned work for 2014

- Board Security Control Reviews
- Vulnerability Scanning

Source: Office of Inspector General, *Work Plan*, updated September 5, 2014. The OIG's current *Work Plan* is available at http://oig.federalreserve.gov/reports/work-plan.htm.

Federal Sector

Overview

Federal Employees & Applicants

Federal EEO Coordination

Federal Agency EEO Directors

Laws, Regulations & Guidance

Management Directives & Federal Sector Guidance

Federal Sector Alternative Dispute Resolution

Federal Sector Reports

Appellate Decisions

Digest of EEO Law

Federal Sector EEO Portal (FedSEP)

Form 462 Reporting

Federal Training & Outreach

Home > Federal Agencies > Form 462

462 Data Collection Resources

The Office of Federal Operations (OFO) produces an Annual Report on the Federal Workforce that includes, among other data, information on federal equal employment opportunity complaints and ADR activities. This data is collected from each agency in the Annual Federal Equal Employment Opportunity Statistical Report of Discrimination Complaints (EEOC Form 462). Federal agency administrators upload data into the EEOC Federal Sector EEO Portal (FedSEP) provided by EEOC and which is not accessible to the general public but only to authorized federal agency administrators. OFO also produces an Instruction Manual which provides detailed information pertaining to the form which aids in understanding the data that must be submitted (rather than entered). Questions concerning the EEOC Form 462 report or Instruction Manual may be sent to the email address form462.form462@eeoc.gov.

Purpose	(b) (5) .
Source	Obtained from http://www.census.gov/people/eeotabulation/data/eeotables20062010.html
Scope	2006-2010 E.3.54
Conclusion	(b) (5)

EEO-ALL01R-Geography-United StatesEstimate-Estimate EEO 1r. Detailed
EEO Tabulation 2006-2010 (5-year ACS data)

The EEO Tabulation is sponsored by four Federal agencies consisting of

Occupation Code	Subject	Total, race and ethnicity	Hispanic or Latino		Not Hispanic or Latino, one race					Not Hispanic or Latino, two or more races							Balance of not Hispanic or Latino
			White alone Hispanic or Latino	A l other Hispanic or Latino	White alone	Black or African American alone	American Indian and Alaska Native alone	Asian alone	Native Hawa ian and Other Pac fic Islander alone	White and Black	Wh te and AIAN	White and Asian	Black and AIAN	NHPI and White (Hawaii only)	NHPI and Asian (Hawaii only)	NHPI and Asian and Wh te (Hawa i only)	
Total all occupations	Total both sexes																
Total, all occupations	Number	#########	13,249,225	9,207,885	##########	17,469,155	894,065	7,426,010	234,435	330,745	633,080	416,890	116,805	(X)	(X)	(X)	780,775
Total all occupations	Percent	100.0%	8.6%	6.0%	67.00%	11.3%	0.6%	4.8%	0.2%	0.2%	0.4%	0.3%	0.1%	(X)	(X)	(X)	0.5%
Total all occupations	Male																
Total all occupations	Number	81 323 085	7 569 470	5 308 805	54 794 265	8 050 065	448 660	3 877 925	123 255	157 770	328 910	209 525	51 985	(X)	(X)	(X)	402 450
Total all occupations	Percent	52.8%	4.9%	3.4%	35.6%	5.2%	0.3%	2.5%	0.1%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Total all occupations	Female																
Total all occupations	Number	72 714 390	5 679 755	3 899 080	48 484 140	9 419 090	445 405	3 548 085	111 180	172 975	304 170	207 365	64 820	(X)	(X)	(X)	378 320
Total all occupations	Percent	47.2%	3.7%	2.5%	31.5%	6.1%	0.3%	2.3%	0.1%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Chief executives and legislators 0010 (SOC 11-10XX)	Total both sexes																
Chief executives and legislators 0010 (SOC 11-10XX)	Number	1,158,885	39,090	13,230	1,001,235	38,695	4,825	50,490	465	1,020	3,740	2,265	330	(X)	(X)	(X)	3,510
Chief executives and legislators 0010 (SOC 11-10XX)	Percent	100.0%	3.4%	1.1%	86.4%	3.3%	0.4%	4.4%	0.0%	0.1%	0.3%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Chief executives and legislators 0010 (SOC 11-10XX)	Male																
Chief executives and legislators 0010 (SOC 11-10XX)	Number	901,735	28,800	10,060	787,200	24,900	3,135	39,390	275	785	2,745	1,570	190	(X)	(X)	(X)	2,685
Chief executives and legislators 0010 (SOC 11-10XX)	Percent	77.8%	2.5%	0.9%	67.9%	2.1%	0.3%	3.4%	0.0%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Chief executives and legislators 0010 (SOC 11-10XX)	Female																
Chief executives and legislators 0010 (SOC 11-10XX)	Number	257 150	10 290	3 170	214 035	13 790	1 690	11 100	185	235	995	695	140	(X)	(X)	(X)	825
Chief executives and legislators 0010 (SOC 11-10XX)	Percent	22.2%	0.9%	0.3%	18.5%	1.2%	0.1%	1.0%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
General and operations managers 0020 (SOC 11-1021)	Total both sexes																
General and operations managers 0020 (SOC 11-1021)	Number	969 820	49 050	22 170	785 520	56 755	4 210	38 880	1 070	1 260	3 830	2 925	345	(X)	(X)	(X)	3 800
General and operations managers 0020 (SOC 11-1021)	Percent	100.0%	5.1%	2.3%	81.0%	5.9%	0.4%	4.0%	0.1%	0.1%	0.4%	0.3%	0.0%	(X)	(X)	(X)	0.4%
General and operations managers 0020 (SOC 11-1021)	Male																
General and operations managers 0020 (SOC 11-1021)	Number	686 620	34 435	15 125	564 305	34 040	2 710	27 715	665	665	2 635	1 785	175	(X)	(X)	(X)	2 360
General and operations managers 0020 (SOC 11-1021)	Percent	70.8%	3.6%	1.6%	58.2%	3.5%	0.3%	2.9%	0.1%	0.1%	0.3%	0.2%	0.0%	(X)	(X)	(X)	0.2%
General and operations managers 0020 (SOC 11-1021)	Female																
General and operations managers 0020 (SOC 11-1021)	Number	283 200	14 620	7 045	221 215	22 715	1 500	11 165	405	595	1 195	1 140	165	(X)	(X)	(X)	1 440
General and operations managers 0020 (SOC 11-1021)	Percent	29.2%	1.5%	0.7%	22.8%	2.3%	0.2%	1.2%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Advertising and promotions managers 0040 (SOC 11-	Total both sexes																
Advertising and promotions managers 0040 (SOC 11-	Number	61 375	2 615	1 345	50 840	2 610	90	2 830	90	55	210	380	20	(X)	(X)	(X)	295
Advertising and promotions managers 0040 (SOC 11-	Percent	100.0%	4.3%	2.2%	82.8%	4.3%	0.1%	4.6%	0.1%	0.1%	0.3%	0.6%	0.0%	(X)	(X)	(X)	0.5%
Advertising and promotions managers 0040 (SOC 11-	Male																
Advertising and promotions managers 0040 (SOC 11-	Number	27 745	1 245	695	22 710	1 205	10	1 275	70	40	155	165	10	(X)	(X)	(X)	165
Advertising and promotions managers 0040 (SOC 11-	Percent	45.2%	2.0%	1.1%	37.0%	2.0%	0.0%	2.1%	0.1%	0.1%	0.3%	0.3%	0.0%	(X)	(X)	(X)	0.3%
Advertising and promotions managers 0040 (SOC 11-	Female																
Advertising and promotions managers 0040 (SOC 11-	Number	33 630	1 365	645	28 130	1 405	80	1 550	20	15	55	215	10	(X)	(X)	(X)	130
Advertising and promotions managers 0040 (SOC 11-	Percent	54.8%	2.2%	1.1%	45.8%	2.3%	0.1%	2.5%	0.0%	0.0%	0.1%	0.4%	0.0%	(X)	(X)	(X)	0.2%
Marketing and sales managers 0050 (SOC 11-2020)	Total both sexes																
Marketing and sales managers 0050 (SOC 11-2020)	Number	871 120	40 565	18 105	715 055	40 635	2 425	41 985	615	1 775	2 395	3 155	515	(X)	(X)	(X)	3 895
Marketing and sales managers 0050 (SOC 11-2020)	Percent	100.0%	4.7%	2.1%	82.1%	4.7%	0.3%	4.8%	0.1%	0.2%	0.3%	0.4%	0.1%	(X)	(X)	(X)	0.4%
Marketing and sales managers 0050 (SOC 11-2020)	Male																
Marketing and sales managers 0050 (SOC 11-2020)	Number	488 260	22 490	9 015	407 360	19 160	1 190	23 025	215	995	1 325	1 355	235	(X)	(X)	(X)	1 885
Marketing and sales managers 0050 (SOC 11-2020)	Percent	56.0%	2.6%	1.0%	46.8%	2.2%	0.1%	2.6%	0.0%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Marketing and sales managers 0050 (SOC 11-2020)	Female																
Marketing and sales managers 0050 (SOC 11-2020)	Number	382 860	18 075	9 090	307 695	21 470	1 235	18 960	400	785	1 070	1 795	275	(X)	(X)	(X)	2 010
Marketing and sales managers 0050 (SOC 11-2020)	Percent	44.0%	2.1%	1.0%	35.3%	2.5%	0.1%	2.2%	0.0%	0.1%	0.1%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Public relations and fundraising managers 0060 (SOC 11-	Total both sexes																
Public relations and fundraising managers 0060 (SOC 11-	Number	57 405	2 025	1 115	47 590	3 905	300	1 625	4	110	200	210	30	(X)	(X)	(X)	290
Public relations and fundraising managers 0060 (SOC 11-	Percent	100.0%	3.5%	1.9%	82.9%	6.8%	0.5%	2.8%	0.0%	0.2%	0.3%	0.4%	0.1%	(X)	(X)	(X)	0.5%
Public relations and fundraising managers 0060 (SOC 11-	Male																
Public relations and fundraising managers 0060 (SOC 11-	Number	22 880	890	355	18 775	1 675	185	700	0	15	95	75	0	(X)	(X)	(X)	115
Public relations and fundraising managers 0060 (SOC 11-	Percent	39.9%	1.6%	0.6%	32.7%	2.9%	0.3%	1.2%	0.0%	0.0%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Public relations and fundraising managers 0060 (SOC 11-	Female																
Public relations and fundraising managers 0060 (SOC 11-	Number	34 525	1 135	760	28 815	2 230	110	925	4	95	110	135	30	(X)	(X)	(X)	175
Public relations and fundraising managers 0060 (SOC 11-	Percent	60.1%	2.0%	1.3%	50.2%	3.9%	0.2%	1.6%	0.0%	0.2%	0.2%	0.2%	0.1%	(X)	(X)	(X)	0.3%
Administrative services managers 0100 (SOC 11-3011)	Total both sexes																
Administrative services managers 0100 (SOC 11-3011)	Number	111 065	5 085	3 640	85 845	10 430	685	3 500	230	135	475	210	200	(X)	(X)	(X)	630
Administrative services managers 0100 (SOC 11-3011)	Percent	100.0%	4.6%	3.3%	77.3%	9.4%	0.6%	3.2%	0.2%	0.1%	0.4%	0.2%	0.2%	(X)	(X)	(X)	0.6%
Administrative services managers 0100 (SOC 11-3011)	Male																
Administrative services managers 0100 (SOC 11-3011)	Number	72 410	3 290	2 195	57 580	5 700	465	1 990	95	100	340	95	140	(X)	(X)	(X)	415
Administrative services managers 0100 (SOC 11-3011)	Percent	65.2%	3.0%	2.0%	51.8%	5.1%	0.4%	1.8%	0.1%	0.1%	0.3%	0.1%	0.1%	(X)	(X)	(X)	0.4%
Administrative services managers 0100 (SOC 11-3011)	Female																
Administrative services managers 0100 (SOC 11-3011)	Number	38 660	1 795	1 450	28 265	4 735	215	1 510	135	35	135	115	60	(X)	(X)	(X)	215
Administrative services managers 0100 (SOC 11-3011)	Percent	34.8%	1.6%	1.3%	25.4%	4.3%	0.2%	1.4%	0.1%	0.0%	0.1%	0.1%	0.1%	(X)	(X)	(X)	0.2%
Computer and information systems managers 0110 (SOC	Total, both sexes																
Computer and information systems managers 0110 (SOC	Number	482 515	17 275	7 010	369 540	28 760	1 205	52 270	395	490	1 165	1 910	225	(X)	(X)	(X)	2 265
Computer and information systems managers 0110 (SOC	Percent	100.0%	3.6%	1.5%	76.6%	6.0%	0.2%	10.8%	0.1%	0.1%	0.2%	0.4%	0.0%	(X)	(X)	(X)	0.5%
Computer and information systems managers 0110 (SOC	Male																
Computer and information systems managers 0110 (SOC	Number	338 130	12 650	4 960	259 360	16 440	830	39 415	225	265	725	1 420	105	(X)	(X)	(X)	1 730
Computer and information systems managers 0110 (SOC	Percent	70.1%	2.6%	1.0%	53.8%	3.4%	0.2%	8.2%	0.0%	0.1%	0.2%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Computer and information systems managers 0110 (SOC	Female																
Computer and information systems managers 0110 (SOC	Number	144 385	4 625	2 045	110 180	12 320	375	12 855	170	225	440	490	120	(X)	(X)	(X)	535
Computer and information systems managers 0110 (SOC	Percent	29.9%	1.0%	0.4%	22.8%	2.6%	0.1%	2.7%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Financial managers 0120 (SOC 11-3031)	Total both sexes																
Financial managers 0120 (SOC 11-3031)	Number	1 108 810	64 680	32 715	842 550	85 905	3 300	65 010	990	1 810	3 095	3 455	480	(X)	(X)	(X)	4 815
Financial managers 0120 (SOC 11-3031)	Percent	100.0%	5.8%	3.0%	76.0%	7.7%	0.3%	5.9%	0.1%	0.2%	0.3%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Financial managers 0120 (SOC 11-3031)	Male																
Financial managers 0120 (SOC 11-3031)	Number	512 305	28 085	11 690	403 070	30 700	1 110	31 325	350	665	1 205	1 975	135	(X)	(X)	(X)	2 005
Financial managers 0120 (SOC 11-3031)	Percent	46.2%	2.5%	1.1%	36.4%	2.8%	0.1%	2.8%	0.0%	0.1%	0.1%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Financial managers 0120 (SOC 11-3031)	Female																
Financial managers 0120 (SOC 11-3031)	Number	596 500	36 595	21 030	439 480	55 205	2 190	33 690	640	1 145	1 890	1 480	345	(X)	(X)	(X)	2 810
Financial managers 0120 (SOC 11-3031)	Percent	53.8%	3.3%	1.9%	39.6%	5.0%	0.2%	3.0%	0.1%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Compensation and benefits managers 0135 (SOC 11-	Total both sexes																
Compensation and benefits managers 0135 (SOC 11-	Number	28 010	1 130	545	22 665	2 305	125	835	0	20	115	55	0	(X)	(X)	(X)	215
Compensation and benefits managers 0135 (SOC 11-	Percent	100.0%	4.0%	1.9%	80.9%	8.2%	0.4%	3.0%	0.0%	0.1%	0.4%	0.2%	0.0%	(X)	(X)	(X)	0.8%
Compensation and benefits managers 0135 (SOC 11-	Male																
Compensation and benefits managers 0135 (SOC 11-	Number	6,115	265	155	5,135	265	40	210	0	10	0	0	0	(X)	(X)	(X)	35
Compensation and benefits managers 0135 (SOC 11-	Percent	21.8%	0.9%	0.6%	18.3%	0.9%	0.1%	0.7%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Compensation and benefits managers 0135 (SOC 11-	Female																
Compensation and benefits managers 0135 (SOC 11-	Number	21,895	865	390	17,530	2,040	85	625	0	10	115	55	0	(X)	(X)	(X)	180
Compensation and benefits managers 0135 (SOC 11-	Percent	78.2%	3.1%	1.4%	62.6%	7.3%	0.3%	2.2%	0.0%	0.0%	0.4%	0.2%	0.0%	(X)	(X)	(X)	0.6%
Human resources managers 0136 (SOC 11-3121)	Total both sexes																
Human resources managers 0136 (SOC 11-3121)	Number	331 125	24 500	12 450	239 120	33 525	1 485	15 610	435	495	875	995	325	(X)	(X)	(X)	1 305
Human resources managers 0136 (SOC 11-3121)	Percent	100.0%	7.4%	3.8%	72.2%	10.1%	0.4%	4.7%	0.1%	0.1%	0.3%	0.3%	0.1%	(X)	(X)	(X)	0.4%
Human resources managers 0136 (SOC 11-3121)	Male																
Human resources managers 0136 (SOC 11-3121)	Number	134 365	10 120	5 655	98 145	11 100	435	7 175	125	25	420	485	100	(X)	(X)	(X)	585
Human resources managers 0136 (SOC 11-3121)	Percent	40.6%	3.1%	1.7%	29.6%	3.4%	0.1%	2.2%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Human resources managers 0136 (SOC 11-3121)	Female																
Human resources managers 0136 (SOC 11-3121)	Number	196 760	14 385	6 795	140 980	22 425	1 050	8 440	310	470	455	510	225	(X)	(X)	(X)	720
Human resources managers 0136 (SOC 11-3121)	Percent	59.4%	4.3%	2.1%	42.6%	6.8%	0.3%	2.5%	0.1%	0.1%	0.1%	0.2%	0.1%	(X)	(X)	(X)	0.2%
Training and development managers 0137 (SOC 11-3131)	Total both sexes																
Training and development managers 0137 (SOC 11-3131)	Number	43 755	1 755	860	34 945	4 360	180	1 085	100	105	110	135	40	(X)	(X)	(X)	80
Training and development managers 0137 (SOC 11-3131)	Percent	100.0%	4.0%	2.0%	79.9%	10.0%	0.4%	2.5%	0.2%	0.2%	0.3%	0.3%	0.1%	(X)	(X)	(X)	0.2%
Training and development managers 0137 (SOC 11-3131)	Male																
Training and development managers 0137 (SOC 11-3131)	Number	20 940	860	470	16 965	1 840	70	490	30	0	70	70	0	(X)	(X)	(X)	75
Training and development managers 0137 (SOC 11-3131)	Percent	47.9%	2.0%	1.1%	38.8%	4.2%	0.2%	1.1%	0.1%	0.0%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Training and development managers 0137 (SOC 11-3131)	Female																
Training and development managers 0137 (SOC 11-3131)	Number	22 810	895	390	17 975	2 520	110	590	70	105	45	70	40	(X)	(X)	(X)	4
Training and development managers 0137 (SOC 11-3131)	Percent	52.1%	2.0%	0.9%	41.1%	5.8%	0.3%	1.3%	0.2%	0.2%	0.1%	0.2%	0.1%	(X)	(X)	(X)	0.0%
Industrial production managers 0140 (SOC 11-3051)	Total both sexes																
Industrial production managers 0140 (SOC 11-3051)	Number	242 520	12 410	7 760	198 630	9 510	785	10 890	180	270	870	555	55	(X)	(X)	(X)	605
Industrial production managers 0140 (SOC 11-3051)	Percent	100.0%	5.1%	3.2%	81.9%	3.9%	0.3%	4.5%	0.1%	0.1%	0.4%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Industrial production managers 0140 (SOC 11-3051)	Male																
Industrial production managers 0140 (SOC 11-3051)	Number	198 415	10 215	5 940	165 495	6 700	545	7 575	170	200	710	375	55	(X)	(X)	(X)	430
Industrial production managers 0140 (SOC 11-3051)	Percent	81.8%	4.2%	2.4%	68.2%	2.8%	0.2%	3.1%	0.1%	0.1%	0.3%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Industrial production managers 0140 (SOC 11-3051)	Female																
Industrial production managers 0140 (SOC 11-3051)	Number	44 105	2 195	1 820	33 135	2 810	240	3 315	10	70	160	180	0	(X)	(X)	(X)	175
Industrial production managers 0140 (SOC 11-3051)	Percent	18.2%	0.9%	0.8%	13.7%	1.2%	0.1%	1.4%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Purchasing managers 0150 (SOC 11-3061)	Total both sexes																
Purchasing managers 0150 (SOC 11-3061)	Number	191 400	9 040	3 390	151 395	16 150	920	8 215	150	320	575	435	110	(X)	(X)	(X)	705
Purchasing managers 0150 (SOC 11-3061)	Percent	100.0%	4.7%	1.8%	79.1%	8.4%	0.5%	4.3%	0.1%	0.2%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Purchasing managers 0150 (SOC 11-3061)	Male																
Purchasing managers 0150 (SOC 11-3061)	Number	106 150	4 890	1 625	86 815	6 670	405	4 535	135	80	295	270	70	(X)	(X)	(X)	355
Purchasing managers 0150 (SOC 11-3061)	Percent	55.5%	2.6%	0.8%	45.4%	3.5%	0.2%	2.4%	0.1%	0.0%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.2%

Purchasing managers 0150 (SOC 11-3061)	Female																
Purchasing managers 0150 (SOC 11-3061)	Number	85 250	4 150	1 765	64 575	9 475	515	3 680	15	240	280	165	40	(X)	(X)	(X)	350
Purchasing managers 0150 (SOC 11-3061)	Percent	44.5%	2.2%	0.9%	33.7%	5.0%	0.3%	1.9%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Transportation, storage, and distribution managers 0160	Total, both sexes																
Transportation storage and distribution managers 0160	Number	230 320	16 570	10 635	171 210	20 295	1 220	7 325	650	220	770	525	75	(X)	(X)	(X)	825
Transportation storage and distribution managers 0160	Percent	100.0%	7.2%	4.6%	74.3%	8.8%	0.5%	3.2%	0.3%	0.1%	0.3%	0.2%	0.0%	(X)	(X)	(X)	0.4%
Transportation storage and distribution managers 0160	Male																
Transportation storage and distribution managers 0160	Number	188 740	13 780	9 040	141 480	15 470	910	5 680	430	200	640	445	65	(X)	(X)	(X)	600
Transportation storage and distribution managers 0160	Percent	81.9%	6.0%	3.9%	61.4%	6.7%	0.4%	2.5%	0.2%	0.1%	0.3%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Transportation storage and distribution managers 0160	Female																
Transportation storage and distribution managers 0160	Number	41 580	2 795	1 595	29 730	4 825	310	1 650	220	20	130	75	10	(X)	(X)	(X)	225
Transportation storage and distribution managers 0160	Percent	18.1%	1.2%	0.7%	12.9%	2.1%	0.1%	0.7%	0.1%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Farmers ranchers and other agricultural managers 0205	Total both sexes																
Farmers ranchers and other agricultural managers 0205	Number	671 560	19 135	13 295	617 105	6 110	3 010	7 600	245	440	2 900	435	40	(X)	(X)	(X)	1 240
Farmers ranchers and other agricultural managers 0205	Percent	100.0%	2.8%	2.0%	91.9%	0.9%	0.4%	1.1%	0.0%	0.1%	0.4%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Farmers ranchers and other agricultural managers 0205	Male																
Farmers ranchers and other agricultural managers 0205	Number	571 345	16 690	11 465	526 065	5 330	2 445	5 555	115	280	2 270	280	30	(X)	(X)	(X)	815
Farmers ranchers and other agricultural managers 0205	Percent	85.1%	2.5%	1.7%	78.3%	0.8%	0.4%	0.8%	0.0%	0.0%	0.3%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Farmers ranchers and other agricultural managers 0205	Female																
Farmers ranchers and other agricultural managers 0205	Number	100 215	2 445	1 830	91 040	775	565	2 045	130	160	630	160	10	(X)	(X)	(X)	425
Farmers ranchers and other agricultural managers 0205	Percent	14.9%	0.4%	0.3%	13.6%	0.1%	0.1%	0.3%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Construction managers 0220 (SOC 11-9021)	Total both sexes																
Construction managers 0220 (SOC 11-9021)	Number	893 930	51 260	30 000	749 580	31 495	4 035	16 895	770	755	4 530	1 455	305	(X)	(X)	(X)	2 855
Construction managers 0220 (SOC 11-9021)	Percent	100.0%	5.7%	3.4%	83.9%	3.5%	0.5%	1.9%	0.1%	0.1%	0.5%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Construction managers 0220 (SOC 11-9021)	Male																
Construction managers 0220 (SOC 11-9021)	Number	830,040	47,455	27,910	698,010	28,275	3,695	14,995	655	700	4,185	1,275	280	(X)	(X)	(X)	2,605
Construction managers 0220 (SOC 11-9021)	Percent	92.9%	5.3%	3.1%	78.1%	3.2%	0.4%	1.7%	0.1%	0.1%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Construction managers 0220 (SOC 11-9021)	Female																
Construction managers 0220 (SOC 11-9021)	Number	63,895	3,805	2,095	51,565	3,220	335	1,900	115	55	345	180	25	(X)	(X)	(X)	255
Construction managers 0220 (SOC 11-9021)	Percent	7.1%	0.4%	0.2%	5.8%	0.4%	0.0%	0.2%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Education administrators 0230 (SOC 11-9030)	Total both sexes																
Education administrators 0230 (SOC 11-9030)	Number	848 645	40 635	21 925	635 685	113 070	4 570	21 575	690	1 640	2 850	1 945	915	(X)	(X)	(X)	3 135
Education administrators 0230 (SOC 11-9030)	Percent	100.0%	4.8%	2.6%	74.9%	13.3%	0.5%	2.5%	0.1%	0.2%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Education administrators 0230 (SOC 11-9030)	Male																
Education administrators 0230 (SOC 11-9030)	Number	307 480	13 175	6 810	240 565	34 235	1 335	7 580	200	605	920	800	225	(X)	(X)	(X)	1 020
Education administrators 0230 (SOC 11-9030)	Percent	36.2%	1.6%	0.8%	28.3%	4.0%	0.2%	0.9%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Education administrators 0230 (SOC 11-9030)	Female																
Education administrators 0230 (SOC 11-9030)	Number	541 165	27 460	15 115	395 120	78 835	3 230	13 995	490	1 035	1 930	1 145	690	(X)	(X)	(X)	2 115
Education administrators 0230 (SOC 11-9030)	Percent	63.8%	3.2%	1.8%	46.6%	9.3%	0.4%	1.6%	0.1%	0.1%	0.2%	0.1%	0.1%	(X)	(X)	(X)	0.2%
Architectural and engineering managers 0300 (SOC 11-	Total both sexes																
Architectural and engineering managers 0300 (SOC 11-	Number	146 595	4 040	1 940	120 975	4 125	350	13 495	20	205	450	440	20	(X)	(X)	(X)	535
Architectural and engineering managers 0300 (SOC 11-	Percent	100.0%	2.8%	1.3%	82.5%	2.8%	0.2%	9.2%	0.0%	0.1%	0.3%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Architectural and engineering managers 0300 (SOC 11-	Male																
Architectural and engineering managers 0300 (SOC 11-	Number	134 670	3 615	1 760	112 325	3 265	345	12 010	10	130	385	395	20	(X)	(X)	(X)	405
Architectural and engineering managers 0300 (SOC 11-	Percent	91.9%	2.5%	1.2%	76.6%	2.2%	0.2%	8.2%	0.0%	0.1%	0.3%	0.3%	0.0%	(X)	(X)	(X)	0.3%
Architectural and engineering managers 0300 (SOC 11-	Female																
Architectural and engineering managers 0300 (SOC 11-	Number	11 920	425	175	8 650	855	4	1 485	10	70	65	40	0	(X)	(X)	(X)	130
Architectural and engineering managers 0300 (SOC 11-	Percent	8.1%	0.3%	0.1%	5.9%	0.6%	0.0%	1.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Food service managers 0310 (SOC 11-9051)	Total both sexes																
Food service managers 0310 (SOC 11-9051)	Number	958 745	83 270	54 995	630 060	80 870	4 040	90 080	1 525	2 030	3 455	3 275	440	(X)	(X)	(X)	4 710
Food service managers 0310 (SOC 11-9051)	Percent	100.0%	8.7%	5.7%	65.7%	8.4%	0.4%	9.4%	0.2%	0.2%	0.4%	0.3%	0.0%	(X)	(X)	(X)	0.5%
Food service managers 0310 (SOC 11-9051)	Male																
Food service managers 0310 (SOC 11-9051)	Number	509 395	47 055	31 095	331 720	36 720	1 650	53 055	800	895	1 600	1 895	250	(X)	(X)	(X)	2 655
Food service managers 0310 (SOC 11-9051)	Percent	53.1%	4.9%	3.2%	34.6%	3.8%	0.2%	5.5%	0.1%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Food service managers 0310 (SOC 11-9051)	Female																
Food service managers 0310 (SOC 11-9051)	Number	449 355	36 215	23 900	298 340	44 150	2 390	37 025	725	1 135	1 855	1 380	190	(X)	(X)	(X)	2 055
Food service managers 0310 (SOC 11-9051)	Percent	46.9%	3.8%	2.5%	31.1%	4.6%	0.2%	3.9%	0.1%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Gaming managers 0330 (SOC 11-9071)	Total both sexes																
Gaming managers 0330 (SOC 11-9071)	Number	19 195	905	675	14 025	1 400	1 220	585	20	10	245	45	0	(X)	(X)	(X)	65
Gaming managers 0330 (SOC 11-9071)	Percent	100.0%	4.7%	3.5%	73.1%	7.3%	6.4%	3.0%	0.1%	0.1%	1.3%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Gaming managers 0330 (SOC 11-9071)	Male																
Gaming managers 0330 (SOC 11-9071)	Number	11 720	575	330	8 985	730	535	350	0	10	150	15	0	(X)	(X)	(X)	45
Gaming managers 0330 (SOC 11-9071)	Percent	61.1%	3.0%	1.7%	46.8%	3.8%	2.8%	1.8%	0.0%	0.1%	0.8%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Gaming managers 0330 (SOC 11-9071)	Female																
Gaming managers 0330 (SOC 11-9071)	Number	7 475	330	345	5 040	670	685	240	20	0	100	25	0	(X)	(X)	(X)	20
Gaming managers 0330 (SOC 11-9071)	Percent	38.9%	1.7%	1.8%	26.3%	3.5%	3.6%	1.3%	0.1%	0.0%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Lodging managers 0340 (SOC 11-9081)	Total both sexes																
Lodging managers 0340 (SOC 11-9081)	Number	143 375	8 015	5 030	98 850	10 945	960	16 480	435	295	525	230	25	(X)	(X)	(X)	1 595
Lodging managers 0340 (SOC 11-9081)	Percent	100.0%	5.6%	3.5%	68.9%	7.6%	0.7%	11.5%	0.3%	0.2%	0.4%	0.2%	0.0%	(X)	(X)	(X)	1.1%
Lodging managers 0340 (SOC 11-9081)	Male																
Lodging managers 0340 (SOC 11-9081)	Number	70 085	3 940	2 120	47 240	4 325	390	10 575	215	100	305	135	10	(X)	(X)	(X)	730
Lodging managers 0340 (SOC 11-9081)	Percent	48.9%	2.7%	1.5%	32.9%	3.0%	0.3%	7.4%	0.1%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.5%
Lodging managers 0340 (SOC 11-9081)	Female																
Lodging managers 0340 (SOC 11-9081)	Number	73 295	4 075	2 910	51 610	6 620	570	5 900	220	195	220	95	10	(X)	(X)	(X)	865
Lodging managers 0340 (SOC 11-9081)	Percent	51.1%	2.8%	2.0%	36.0%	4.6%	0.4%	4.1%	0.2%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.6%
Medical and health services managers 0350 (SOC 11-	Total, both sexes																
Medical and health services managers 0350 (SOC 11-	Number	533 925	26 495	12 850	400 545	60 385	2 555	24 545	520	585	1 805	945	355	(X)	(X)	(X)	2 350
Medical and health services managers 0350 (SOC 11-	Percent	100.0%	5.0%	2.4%	75.0%	11.3%	0.5%	4.6%	0.1%	0.1%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Medical and health services managers 0350 (SOC 11-	Male																
Medical and health services managers 0350 (SOC 11-	Number	161 075	8 830	3 565	120 660	16 545	705	8 925	75	165	560	300	30	(X)	(X)	(X)	715
Medical and health services managers 0350 (SOC 11-	Percent	30.2%	1.7%	0.7%	22.6%	3.1%	0.1%	1.7%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Medical and health services managers 0350 (SOC 11-	Female																
Medical and health services managers 0350 (SOC 11-	Number	372 850	17 665	9 285	279 880	43 840	1 845	15 620	440	420	1 245	650	325	(X)	(X)	(X)	1 635
Medical and health services managers 0350 (SOC 11-	Percent	69.8%	3.3%	1.7%	52.4%	8.2%	0.3%	2.9%	0.1%	0.1%	0.2%	0.1%	0.1%	(X)	(X)	(X)	0.3%
Natural sciences managers 0360 (SOC 11-9121)	Total both sexes																
Natural sciences managers 0360 (SOC 11-9121)	Number	19 480	730	165	15 425	410	15	2 235	45	120	65	135	0	(X)	(X)	(X)	130
Natural sciences managers 0360 (SOC 11-9121)	Percent	100.0%	3.7%	0.8%	79.2%	2.1%	0.1%	11.5%	0.2%	0.6%	0.3%	0.7%	0.0%	(X)	(X)	(X)	0.7%
Natural sciences managers 0360 (SOC 11-9121)	Male																
Natural sciences managers 0360 (SOC 11-9121)	Number	11 915	490	45	9 490	215	4	1 375	45	45	30	45	0	(X)	(X)	(X)	125
Natural sciences managers 0360 (SOC 11-9121)	Percent	61.2%	2.5%	0.2%	48.7%	1.1%	0.0%	7.1%	0.2%	0.2%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.6%
Natural sciences managers 0360 (SOC 11-9121)	Female																
Natural sciences managers 0360 (SOC 11-9121)	Number	7 565	240	120	5 935	195	10	860	0	70	35	90	0	(X)	(X)	(X)	4
Natural sciences managers 0360 (SOC 11-9121)	Percent	38.8%	1.2%	0.6%	30.5%	1.0%	0.1%	4.4%	0.0%	0.4%	0.2%	0.5%	0.0%	(X)	(X)	(X)	0.0%
Property real estate and commun ty association	Total both sexes																
Property real estate and commun ty association	Number	559 240	36 115	24 680	424 685	44 235	3 120	17 665	865	995	2 755	1 430	455	(X)	(X)	(X)	2 235
Property real estate and commun ty association	Percent	100.0%	6.5%	4.4%	75.9%	7.9%	0.6%	3.2%	0.2%	0.2%	0.5%	0.3%	0.1%	(X)	(X)	(X)	0.4%
Property real estate and commun ty association	Male																
Property real estate and commun ty association	Number	274 700	15 585	11 785	215 215	17 715	1 375	9 255	345	315	1 245	695	180	(X)	(X)	(X)	985
Property real estate and commun ty association	Percent	49.1%	2.8%	2.1%	38.5%	3.2%	0.2%	1.7%	0.1%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Property real estate and commun ty association	Female																
Property, real estate, and commun ty association	Number	284,540	20,530	12,890	209,470	26,520	1,745	8,410	520	680	1,510	735	270	(X)	(X)	(X)	1,250
Property real estate and commun ty association	Percent	50.9%	3.7%	2.3%	37.5%	4.7%	0.3%	1.5%	0.1%	0.1%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Social and community service managers 0420 (SOC 11-	Total both sexes																
Social and community service managers 0420 (SOC 11-	Number	325,710	14,245	8,905	241,630	43,440	2,670	9,355	300	885	1,455	860	345	(X)	(X)	(X)	1,625
Social and community service managers 0420 (SOC 11-	Percent	100.0%	4.4%	2.7%	74.2%	13.3%	0.8%	2.9%	0.1%	0.3%	0.4%	0.3%	0.1%	(X)	(X)	(X)	0.5%
Social and community service managers 0420 (SOC 11-	Male																
Social and community service managers 0420 (SOC 11-	Number	107 455	4 385	3 010	80 860	13 655	805	3 335	50	300	460	185	65	(X)	(X)	(X)	345
Social and community service managers 0420 (SOC 11-	Percent	33.0%	1.3%	0.9%	24.8%	4.2%	0.2%	1.0%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Social and community service managers 0420 (SOC 11-	Female																
Social and community service managers 0420 (SOC 11-	Number	218 255	9 860	5 900	160 770	29 785	1 865	6 020	250	585	995	675	280	(X)	(X)	(X)	1 275
Social and community service managers 0420 (SOC 11-	Percent	67.0%	3.0%	1.8%	49.4%	9.1%	0.6%	1.8%	0.1%	0.2%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Emergency management directors 0425 (SOC 11-9161)	Total both sexes																
Emergency management directors 0425 (SOC 11-9161)	Number	3 295	130	50	2 645	340	15	35	0	15	0	4	15	(X)	(X)	(X)	50
Emergency management directors 0425 (SOC 11-9161)	Percent	100.0%	3.9%	1.5%	80.3%	10.3%	0.5%	1.1%	0.0%	0.5%	0.0%	0.1%	0.5%	(X)	(X)	(X)	1.5%
Emergency management directors 0425 (SOC 11-9161)	Male																
Emergency management directors 0425 (SOC 11-9161)	Number	2 140	70	50	1 745	205	15	35	0	0	0	4	0	(X)	(X)	(X)	15
Emergency management directors 0425 (SOC 11-9161)	Percent	64.9%	2.1%	1.5%	53.0%	6.2%	0.5%	1.1%	0.0%	0.0%	0.0%	0.1%	0.0%	(X)	(X)	(X)	0.5%
Emergency management directors 0425 (SOC 11-9161)	Female																
Emergency management directors 0425 (SOC 11-9161)	Number	1 155	60	0	900	135	0	0	0	15	0	0	15	(X)	(X)	(X)	35
Emergency management directors 0425 (SOC 11-9161)	Percent	35.1%	1.8%	0.0%	27.3%	4.1%	0.0%	0.0%	0.0%	0.5%	0.0%	0.0%	0.5%	(X)	(X)	(X)	1.1%
Miscellaneous managers including funeral service	Total both sexes																
Miscellaneous managers including funeral service	Number	3 183 835	161 540	81 980	2 494 480	225 570	13 515	162 745	3 285	4 530	11 695	9 150	2 315	(X)	(X)	(X)	13 030
Miscellaneous managers including funeral service	Percent	100.0%	5.1%	2.6%	78.3%	7.1%	0.4%	5.1%	0.1%	0.1%	0.4%	0.3%	0.1%	(X)	(X)	(X)	0.4%
Miscellaneous managers including funeral service	Male																
Miscellaneous managers including funeral service	Number	2 074 525	104 970	51 875	1 662 640	116 705	7 810	104 920	2 070	2 530	7 115	5 115	1 135	(X)	(X)	(X)	7 645
Miscellaneous managers including funeral service	Percent	65.2%	3.3%	1.6%	52.2%	3.7%	0.2%	3.3%	0.1%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Miscellaneous managers including funeral service	Female																
Miscellaneous managers including funeral service	Number	1 109 305	56 570	30 105	831 840	108 865	5 710	57 825	1 210	2 000	4 580	4 035	1 180	(X)	(X)	(X)	5 390
Miscellaneous managers, including funeral service	Percent	34.8%	1.8%	0.9%	26.1%	3.4%	0.2%	1.8%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Agents and business managers of artists performers and	Total both sexes																
Agents and business managers of artists performers and	Number	47 010	3 105	1 935	33 905	5 115	220	1 680	100	175	180	250	10	(X)	(X)	(X)	325
Agents and business managers of artists performers and	Percent	100.0%	6.6%	4.1%	72.1%	10.9%	0.5%	3.6%	0.2%	0.4%	0.4%	0.5%	0.0%	(X)	(X)	(X)	0.7%
Agents and business managers of artists performers and	Male																
Agents and business managers of artists performers and	Number	25 965	1 700	1 435	17 705	3 635	105	765	100	110	70	145	0	(X)	(X)	(X)	195
Agents and business managers of artists performers and	Percent	55.2%	3.6%	3.1%	37.7%	7.7%	0.2%	1.6%	0.2%	0.2%	0.1%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Agents and business managers of artists performers and	Female																
Agents and business managers of artists performers and	Number	21 040	1 405	500	16 200	1 480	115	920	0	70	110	105	10	(X)	(X)	(X)	130
Agents and business managers of artists performers and	Percent	44.8%	3.0%	1.1%	34.5%	3.1%	0.2%	2.0%	0.0%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.3%

Buyers and purchasing agents, farm products 0510 (SOC	Total, both sexes																
Buyers and purchasing agents, farm products 0510 (SOC	Number	11 860	1 015	500	9 285	360	45	450	110	20	10	15	15	(X)	(X)	(X)	45
Buyers and purchasing agents, farm products 0510 (SOC	Percent	100.0%	8.6%	4.2%	78.3%	3.0%	0.4%	3.8%	0.9%	0.2%	0.1%	0.1%	0.1%	(X)	(X)	(X)	0.4%
Buyers and purchasing agents, farm products 0510 (SOC	Male																
Buyers and purchasing agents, farm products 0510 (SOC	Number	8 785	660	370	7 140	205	20	255	45	20	10	0	15	(X)	(X)	(X)	45
Buyers and purchasing agents, farm products 0510 (SOC	Percent	74.1%	5.6%	3.1%	60.2%	1.7%	0.2%	2.2%	0.4%	0.2%	0.1%	0.0%	0.1%	(X)	(X)	(X)	0.4%
Buyers and purchasing agents, farm products 0510 (SOC	Female																
Buyers and purchasing agents, farm products 0510 (SOC	Number	3 075	350	130	2 140	155	25	190	65	0	4	15	0	(X)	(X)	(X)	0
Buyers and purchasing agents, farm products 0510 (SOC	Percent	25.9%	3.0%	1.1%	18.0%	1.3%	0.2%	1.6%	0.5%	0.0%	0.0%	0.1%	0.0%	(X)	(X)	(X)	0.0%
Wholesale and retail buyers, except farm products 0520	Total, both sexes																
Wholesale and retail buyers, except farm products 0520	Number	232 065	14 025	8 515	180 220	13 215	650	11 600	405	480	815	825	25	(X)	(X)	(X)	1 295
Wholesale and retail buyers, except farm products 0520	Percent	100.0%	6.0%	3.7%	77.7%	5.7%	0.3%	5.0%	0.2%	0.2%	0.4%	0.4%	0.0%	(X)	(X)	(X)	0.6%
Wholesale and retail buyers, except farm products 0520	Male																
Wholesale and retail buyers, except farm products 0520	Number	108 980	7 630	4 365	83 535	6 070	405	5 150	75	155	405	375	25	(X)	(X)	(X)	785
Wholesale and retail buyers, except farm products 0520	Percent	47.0%	3.3%	1.9%	36.0%	2.6%	0.2%	2.2%	0.0%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Wholesale and retail buyers, except farm products 0520	Female																
Wholesale and retail buyers, except farm products 0520	Number	123 085	6 395	4 150	96 685	7 140	240	6 450	330	325	410	450	0	(X)	(X)	(X)	510
Wholesale and retail buyers, except farm products 0520	Percent	53.0%	2.8%	1.8%	41.7%	3.1%	0.1%	2.8%	0.1%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Purchasing agents, except wholesale, retail, and farm	Total, both sexes																
Purchasing agents, except wholesale, retail, and farm	Number	271 240	13 790	7 640	212 635	22 455	1 210	10 175	360	345	940	625	160	(X)	(X)	(X)	900
Purchasing agents, except wholesale, retail, and farm	Percent	100.0%	5.1%	2.8%	78.4%	8.3%	0.4%	3.8%	0.1%	0.1%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.3%
Purchasing agents, except wholesale, retail, and farm	Male																
Purchasing agents, except wholesale, retail, and farm	Number	125 735	6 575	3 710	101 120	8 125	475	4 570	50	80	420	255	30	(X)	(X)	(X)	325
Purchasing agents, except wholesale, retail, and farm	Percent	46.4%	2.4%	1.4%	37.3%	3.0%	0.2%	1.7%	0.0%	0.0%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Purchasing agents, except wholesale, retail, and farm	Female																
Purchasing agents, except wholesale, retail, and farm	Number	145,500	7,215	3,930	111,515	14,325	735	5,605	310	260	520	370	130	(X)	(X)	(X)	575
Purchasing agents, except wholesale, retail, and farm	Percent	53.6%	2.7%	1.4%	41.1%	5.3%	0.3%	2.1%	0.1%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Claims adjusters, appraisers, examiners, and investigators	Total, both sexes																
Claims adjusters, appraisers, examiners, and investigators	Number	296,325	16,065	9,580	210,700	43,900	765	11,085	305	770	1,005	885	180	(X)	(X)	(X)	1,085
Claims adjusters, appraisers, examiners, and investigators	Percent	100.0%	5.4%	3.2%	71.1%	14.8%	0.3%	3.7%	0.1%	0.3%	0.3%	0.3%	0.1%	(X)	(X)	(X)	0.4%
Claims adjusters, appraisers, examiners, and investigators	Male																
Claims adjusters, appraisers, examiners, and investigators	Number	113 190	6 020	2 805	88 660	9 875	220	4 315	75	165	315	370	35	(X)	(X)	(X)	335
Claims adjusters, appraisers, examiners, and investigators	Percent	38.2%	2.0%	0.9%	29.9%	3.3%	0.1%	1.5%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Claims adjusters, appraisers, examiners, and investigators	Female																
Claims adjusters, appraisers, examiners, and investigators	Number	183 135	10 045	6 775	122 040	34 025	540	6 775	235	605	690	515	145	(X)	(X)	(X)	750
Claims adjusters, appraisers, examiners, and investigators	Percent	61.8%	3.4%	2.3%	41.2%	11.5%	0.2%	2.3%	0.1%	0.2%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Compliance officers 0565 (SOC 13-1041)	Total, both sexes																
Compliance officers 0565 (SOC 13-1041)	Number	179 290	11 110	5 320	129 325	19 905	1 390	9 395	310	210	630	550	190	(X)	(X)	(X)	950
Compliance officers 0565 (SOC 13-1041)	Percent	100.0%	6.2%	3.0%	72.1%	11.1%	0.8%	5.2%	0.2%	0.1%	0.4%	0.3%	0.1%	(X)	(X)	(X)	0.5%
Compliance officers 0565 (SOC 13-1041)	Male																
Compliance officers 0565 (SOC 13-1041)	Number	95 745	5 885	2 310	72 425	7 635	710	5 290	105	115	395	310	95	(X)	(X)	(X)	465
Compliance officers 0565 (SOC 13-1041)	Percent	53.4%	3.3%	1.3%	40.4%	4.3%	0.4%	3.0%	0.1%	0.1%	0.2%	0.2%	0.1%	(X)	(X)	(X)	0.3%
Compliance officers 0565 (SOC 13-1041)	Female																
Compliance officers 0565 (SOC 13-1041)	Number	83 545	5 225	3 010	56 895	12 270	680	4 105	210	90	235	240	95	(X)	(X)	(X)	485
Compliance officers 0565 (SOC 13-1041)	Percent	46.6%	2.9%	1.7%	31.7%	6.8%	0.4%	2.3%	0.1%	0.1%	0.1%	0.1%	0.1%	(X)	(X)	(X)	0.3%
Cost estimators 0600 (SOC 13-1051)	Total, both sexes																
Cost estimators 0600 (SOC 13-1051)	Number	130 470	5 505	3 185	114 620	1 910	405	3 440	50	80	485	255	35	(X)	(X)	(X)	495
Cost estimators 0600 (SOC 13-1051)	Percent	100.0%	4.2%	2.4%	87.9%	1.5%	0.3%	2.6%	0.0%	0.1%	0.4%	0.2%	0.0%	(X)	(X)	(X)	0.4%
Cost estimators 0600 (SOC 13-1051)	Male																
Cost estimators 0600 (SOC 13-1051)	Number	113 860	4 470	2 655	101 230	1 435	345	2 595	50	80	385	220	0	(X)	(X)	(X)	390
Cost estimators 0600 (SOC 13-1051)	Percent	87.3%	3.4%	2.0%	77.6%	1.1%	0.3%	2.0%	0.0%	0.1%	0.3%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Cost estimators 0600 (SOC 13-1051)	Female																
Cost estimators 0600 (SOC 13-1051)	Number	16 610	1 035	530	13 390	480	60	840	0	0	100	30	35	(X)	(X)	(X)	105
Cost estimators 0600 (SOC 13-1051)	Percent	12.7%	0.8%	0.4%	10.3%	0.4%	0.0%	0.6%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Human resources workers 0630 (SOC 13-1070)	Total, both sexes																
Human resources workers 0630 (SOC 13-1070)	Number	651 090	40 860	26 620	450 200	91 105	3 930	26 730	1 030	1 880	2 415	2 145	720	(X)	(X)	(X)	3 450
Human resources workers 0630 (SOC 13-1070)	Percent	100.0%	6.3%	4.1%	69.1%	14.0%	0.6%	4.1%	0.2%	0.3%	0.4%	0.3%	0.1%	(X)	(X)	(X)	0.5%
Human resources workers 0630 (SOC 13-1070)	Male																
Human resources workers 0630 (SOC 13-1070)	Number	191 270	12 020	7 285	134 975	25 230	1 050	7 735	220	575	565	660	75	(X)	(X)	(X)	880
Human resources workers 0630 (SOC 13-1070)	Percent	29.4%	1.8%	1.1%	20.7%	3.9%	0.2%	1.2%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Human resources workers 0630 (SOC 13-1070)	Female																
Human resources workers 0630 (SOC 13-1070)	Number	459 815	28 840	19 335	315 225	65 875	2 880	18 995	810	1 305	1 850	1 485	640	(X)	(X)	(X)	2 570
Human resources workers 0630 (SOC 13-1070)	Percent	70.6%	4.4%	3.0%	48.4%	10.1%	0.4%	2.9%	0.1%	0.2%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Compensation, benefits, and job analysis specialists 0640	Total, both sexes																
Compensation, benefits, and job analysis specialists 0640	Number	100 935	5 535	3 290	73 355	13 330	495	3 640	160	185	310	275	80	(X)	(X)	(X)	275
Compensation, benefits, and job analysis specialists 0640	Percent	100.0%	5.5%	3.3%	72.7%	13.2%	0.5%	3.6%	0.2%	0.2%	0.3%	0.3%	0.1%	(X)	(X)	(X)	0.3%
Compensation, benefits, and job analysis specialists 0640	Male																
Compensation, benefits, and job analysis specialists 0640	Number	17 360	1 020	555	12 340	2 420	105	665	45	30	70	55	0	(X)	(X)	(X)	50
Compensation, benefits, and job analysis specialists 0640	Percent	17.2%	1.0%	0.5%	12.2%	2.4%	0.1%	0.7%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.0%
Compensation, benefits, and job analysis specialists 0640	Female																
Compensation, benefits, and job analysis specialists 0640	Number	83 575	4 515	2 735	61 015	10 905	390	2 975	115	155	240	220	80	(X)	(X)	(X)	225
Compensation, benefits, and job analysis specialists 0640	Percent	82.8%	4.5%	2.7%	60.4%	10.8%	0.4%	2.9%	0.1%	0.2%	0.2%	0.2%	0.1%	(X)	(X)	(X)	0.2%
Training and development specialists 0650 (SOC 13-1151)	Total, both sexes																
Training and development specialists 0650 (SOC 13-1151)	Number	130 910	6 960	4 340	94 210	18 395	735	3 795	100	355	685	480	140	(X)	(X)	(X)	720
Training and development specialists 0650 (SOC 13-1151)	Percent	100.0%	5.3%	3.3%	72.0%	14.1%	0.6%	2.9%	0.1%	0.3%	0.5%	0.4%	0.1%	(X)	(X)	(X)	0.5%
Training and development specialists 0650 (SOC 13-1151)	Male																
Training and development specialists 0650 (SOC 13-1151)	Number	56 120	3 300	1 865	41 535	6 830	310	1 485	55	85	280	115	80	(X)	(X)	(X)	170
Training and development specialists 0650 (SOC 13-1151)	Percent	42.9%	2.5%	1.4%	31.7%	5.2%	0.2%	1.1%	0.0%	0.1%	0.2%	0.1%	0.1%	(X)	(X)	(X)	0.1%
Training and development specialists 0650 (SOC 13-1151)	Female																
Training and development specialists 0650 (SOC 13-1151)	Number	74 790	3 660	2 475	52 680	11 560	425	2 305	45	270	405	360	60	(X)	(X)	(X)	550
Training and development specialists 0650 (SOC 13-1151)	Percent	57.1%	2.8%	1.9%	40.2%	8.8%	0.3%	1.8%	0.0%	0.2%	0.3%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Logisticians 0700 (SOC 13-1081)	Total, both sexes																
Logisticians 0700 (SOC 13-1081)	Number	73 640	4 080	2 740	50 185	11 220	485	3 290	295	175	390	340	75	(X)	(X)	(X)	350
Logisticians 0700 (SOC 13-1081)	Percent	100.0%	5.5%	3.7%	68.1%	15.2%	0.7%	4.5%	0.4%	0.2%	0.5%	0.5%	0.1%	(X)	(X)	(X)	0.5%
Logisticians 0700 (SOC 13-1081)	Male																
Logisticians 0700 (SOC 13-1081)	Number	47 805	2 590	1 685	32 895	7 405	255	1 980	220	125	240	230	40	(X)	(X)	(X)	140
Logisticians 0700 (SOC 13-1081)	Percent	64.9%	3.5%	2.3%	44.7%	10.1%	0.3%	2.7%	0.3%	0.2%	0.3%	0.3%	0.1%	(X)	(X)	(X)	0.2%
Logisticians 0700 (SOC 13-1081)	Female																
Logisticians 0700 (SOC 13-1081)	Number	25 835	1 495	1 060	17 290	3 820	230	1 310	80	50	150	110	40	(X)	(X)	(X)	210
Logisticians 0700 (SOC 13-1081)	Percent	35.1%	2.0%	1.4%	23.5%	5.2%	0.3%	1.8%	0.1%	0.1%	0.2%	0.1%	0.1%	(X)	(X)	(X)	0.3%
Management analysts 0710 (SOC 13-1111)	Total, both sexes																
Management analysts 0710 (SOC 13-1111)	Number	690 680	24 445	10 145	542 035	45 075	2 135	57 040	410	840	1 980	2 455	595	(X)	(X)	(X)	3 525
Management analysts 0710 (SOC 13-1111)	Percent	100.0%	3.5%	1.5%	78.5%	6.5%	0.3%	8.3%	0.1%	0.1%	0.3%	0.4%	0.1%	(X)	(X)	(X)	0.5%
Management analysts 0710 (SOC 13-1111)	Male																
Management analysts 0710 (SOC 13-1111)	Number	407 820	14 065	5 105	327 155	20 320	1 015	35 025	150	460	1 000	1 255	190	(X)	(X)	(X)	2 075
Management analysts 0710 (SOC 13-1111)	Percent	59.0%	2.0%	0.7%	47.4%	2.9%	0.1%	5.1%	0.0%	0.1%	0.1%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Management analysts 0710 (SOC 13-1111)	Female																
Management analysts 0710 (SOC 13-1111)	Number	282 860	10 385	5 040	214 875	24 760	1 120	22 015	255	380	980	1 200	405	(X)	(X)	(X)	1 450
Management analysts 0710 (SOC 13-1111)	Percent	41.0%	1.5%	0.7%	31.1%	3.6%	0.2%	3.2%	0.0%	0.1%	0.1%	0.2%	0.1%	(X)	(X)	(X)	0.2%
Meeting, convention, and event planners 0725 (SOC 13-	Total, both sexes																
Meeting, convention, and event planners 0725 (SOC 13-	Number	60,660	2,990	2,320	45,860	5,640	160	2,440	10	215	240	305	60	(X)	(X)	(X)	415
Meeting, convention, and event planners 0725 (SOC 13-	Percent	100.0%	4.9%	3.8%	75.6%	9.3%	0.3%	4.0%	0.0%	0.4%	0.4%	0.5%	0.1%	(X)	(X)	(X)	0.7%
Meeting, convention, and event planners 0725 (SOC 13-	Male																
Meeting, convention, and event planners 0725 (SOC 13-	Number	13,810	820	890	9,255	1,785	4	765	4	40	15	65	50	(X)	(X)	(X)	110
Meeting, convention, and event planners 0725 (SOC 13-	Percent	22.8%	1.4%	1.5%	15.3%	2.9%	0.0%	1.3%	0.0%	0.1%	0.0%	0.1%	0.1%	(X)	(X)	(X)	0.2%
Meeting, convention, and event planners 0725 (SOC 13-	Female																
Meeting, convention, and event planners 0725 (SOC 13-	Number	46 850	2 170	1 430	36 605	3 855	160	1 675	4	175	225	235	10	(X)	(X)	(X)	305
Meeting, convention, and event planners 0725 (SOC 13-	Percent	77.2%	3.6%	2.4%	60.3%	6.4%	0.3%	2.8%	0.0%	0.3%	0.4%	0.4%	0.0%	(X)	(X)	(X)	0.5%
Fundraisers 0726 (SOC 13-1131)	Total, both sexes																
Fundraisers 0726 (SOC 13-1131)	Number	85 835	2 370	1 235	73 495	4 950	130	2 285	65	285	270	395	30	(X)	(X)	(X)	325
Fundraisers 0726 (SOC 13-1131)	Percent	100.0%	2.8%	1.4%	85.6%	5.8%	0.2%	2.7%	0.1%	0.3%	0.3%	0.5%	0.0%	(X)	(X)	(X)	0.4%
Fundraisers 0726 (SOC 13-1131)	Male																
Fundraisers 0726 (SOC 13-1131)	Number	24 080	535	295	20 480	1 680	75	550	10	150	150	45	0	(X)	(X)	(X)	105
Fundraisers 0726 (SOC 13-1131)	Percent	28.1%	0.6%	0.3%	23.9%	2.0%	0.1%	0.6%	0.0%	0.2%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Fundraisers 0726 (SOC 13-1131)	Female																
Fundraisers 0726 (SOC 13-1131)	Number	61 760	1 835	940	53 015	3 270	55	1 735	55	135	120	350	30	(X)	(X)	(X)	220
Fundraisers 0726 (SOC 13-1131)	Percent	72.0%	2.1%	1.1%	61.8%	3.8%	0.1%	2.0%	0.1%	0.2%	0.1%	0.4%	0.0%	(X)	(X)	(X)	0.3%
Market research analysts and marketing specialists 0735	Total, both sexes																
Market research analysts and marketing specialists 0735	Number	184 360	8 495	3 435	143 525	9 825	375	15 640	70	210	480	1 205	70	(X)	(X)	(X)	1 030
Market research analysts and marketing specialists 0735	Percent	100.0%	4.6%	1.9%	77.9%	5.3%	0.2%	8.5%	0.0%	0.1%	0.3%	0.7%	0.0%	(X)	(X)	(X)	0.6%
Market research analysts and marketing specialists 0735	Male																
Market research analysts and marketing specialists 0735	Number	82 815	3 730	1 295	64 870	4 110	140	7 490	0	65	245	490	0	(X)	(X)	(X)	385
Market research analysts and marketing specialists 0735	Percent	44.9%	2.0%	0.7%	35.2%	2.2%	0.1%	4.1%	0.0%	0.0%	0.1%	0.3%	0.0%	(X)	(X)	(X)	0.2%
Market research analysts and marketing specialists 0735	Female																
Market research analysts and marketing specialists 0735	Number	101 545	4 765	2 140	78 655	5 715	235	8 150	70	145	235	720	70	(X)	(X)	(X)	645
Market research analysts and marketing specialists 0735	Percent	55.1%	2.6%	1.2%	42.7%	3.1%	0.1%	4.4%	0.0%	0.1%	0.1%	0.4%	0.0%	(X)	(X)	(X)	0.3%
Business operations specialists, all other 0740 (SOC 13-	Total, both sexes																
Business operations specialists, all other 0740 (SOC 13-	Number	231 255	14 175	8 655	158 375	27 990	1 230	16 555	165	400	870	1 325	160	(X)	(X)	(X)	1 350
Business operations specialists, all other 0740 (SOC 13-	Percent	100.0%	6.1%	3.7%	68.5%	12.1%	0.5%	7.2%	0.1%	0.2%	0.4%	0.6%	0.1%	(X)	(X)	(X)	0.6%
Business operations specialists, all other 0740 (SOC 13-	Male																
Business operations specialists, all other 0740 (SOC 13-	Number	86 840	5 380	3 125	60 890	8 150	390	7 345	55	145	345	430	70	(X)	(X)	(X)	520
Business operations specialists, all other 0740 (SOC 13-	Percent	37.6%	2.3%	1.4%	26.3%	3.5%	0.2%	3.2%	0.0%	0.1%	0.1%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Business operations specialists, all other 0740 (SOC 13-	Female																
Business operations specialists, all other 0740 (SOC 13-	Number	144 415	8 795	5 530	97 485	19 835	845	9 210	110	260	525	895	90	(X)	(X)	(X)	835
Business operations specialists, all other 0740 (SOC 13-	Percent	62.4%	3.8%	2.4%	42.2%	8.6%	0.4%	4.0%	0.0%	0.1%	0.2%	0.4%	0.0%	(X)	(X)	(X)	0.4%
Accountants and auditors 0800 (SOC 13-2011)	Total, both sexes																
Accountants and auditors 0800 (SOC 13-2011)	Number	2 100 705	92 405	47 135	1 537 555	170 610	7 450	218 470	2 050	2 915	4 875	6 905	1 145	(X)	(X)	(X)	9 200
Accountants and auditors 0800 (SOC 13-2011)	Percent	100.0%	4.4%	2.2%	73.2%	8.1%	0.4%	10.4%	0.1%	0.1%	0.2%	0.3%	0.1%	(X)	(X)	(X)	0.4%

Accountants and auditors 0800 (SOC 13-2011)	Male																
Accountants and auditors 0800 (SOC 13-2011)	Number	840 595	35 025	16 060	643 790	54 340	2 010	78 990	680	1 005	1 715	3 005	290	(X)	(X)	(X)	3 685
Accountants and auditors 0800 (SOC 13-2011)	Percent	40.0%	1.7%	0.8%	30.6%	2.6%	0.1%	3.8%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Accountants and auditors 0800 (SOC 13-2011)	Female																
Accountants and auditors 0800 (SOC 13-2011)	Number	1 260 110	57 380	31 075	893 765	116 270	5 435	139 480	1 365	1 910	3 160	3 900	855	(X)	(X)	(X)	5 515
Accountants and auditors 0800 (SOC 13-2011)	Percent	60.0%	2.7%	1.5%	42.5%	5.5%	0.3%	6.6%	0.1%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Appraisers and assessors of real estate 0810 (SOC 13-	Total, both sexes																
Appraisers and assessors of real estate 0810 (SOC 13-	Number	112 895	4 140	1 560	98 590	4 110	415	2 870	75	110	425	230	55	(X)	(X)	(X)	315
Appraisers and assessors of real estate 0810 (SOC 13-	Percent	100.0%	3.7%	1.4%	87.3%	3.6%	0.4%	2.5%	0.1%	0.1%	0.4%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Appraisers and assessors of real estate 0810 (SOC 13-	Male																
Appraisers and assessors of real estate 0810 (SOC 13-	Number	74 545	2 500	940	66 435	2 085	135	1 825	50	30	155	105	45	(X)	(X)	(X)	240
Appraisers and assessors of real estate 0810 (SOC 13-	Percent	66.0%	2.2%	0.8%	58.8%	1.8%	0.1%	1.6%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Appraisers and assessors of real estate 0810 (SOC 13-	Female																
Appraisers and assessors of real estate 0810 (SOC 13-	Number	38 345	1 640	620	32 155	2 025	285	1 045	25	80	270	125	10	(X)	(X)	(X)	75
Appraisers and assessors of real estate 0810 (SOC 13-	Percent	34.0%	1.5%	0.5%	28.5%	1.8%	0.3%	0.9%	0.0%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Budget analysts 0820 (SOC 13-2031)	Total, both sexes																
Budget analysts 0820 (SOC 13-2031)	Number	52 945	2 320	1 400	35 560	8 340	230	3 780	130	150	335	250	85	(X)	(X)	(X)	365
Budget analysts 0820 (SOC 13-2031)	Percent	100.0%	4.4%	2.6%	67.2%	15.8%	0.4%	7.1%	0.2%	0.3%	0.6%	0.5%	0.2%	(X)	(X)	(X)	0.7%
Budget analysts 0820 (SOC 13-2031)	Male																
Budget analysts 0820 (SOC 13-2031)	Number	19 425	700	405	14 090	2 380	80	1 330	25	65	145	95	20	(X)	(X)	(X)	90
Budget analysts 0820 (SOC 13-2031)	Percent	36.7%	1.3%	0.8%	26.6%	4.5%	0.2%	2.5%	0.0%	0.1%	0.3%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Budget analysts 0820 (SOC 13-2031)	Female																
Budget analysts 0820 (SOC 13-2031)	Number	33 525	1 615	995	21 470	5 960	145	2 450	100	85	190	155	65	(X)	(X)	(X)	275
Budget analysts 0820 (SOC 13-2031)	Percent	63.3%	3.1%	1.9%	40.6%	11.3%	0.3%	4.6%	0.2%	0.2%	0.4%	0.3%	0.1%	(X)	(X)	(X)	0.5%
Credit analysts 0830 (SOC 13-2041)	Total, both sexes																
Credit analysts 0830 (SOC 13-2041)	Number	30,200	1,650	1,285	21,040	3,545	130	2,280	35	0	95	85	15	(X)	(X)	(X)	40
Credit analysts 0830 (SOC 13-2041)	Percent	100.0%	5.5%	4.3%	69.7%	11.7%	0.4%	7.5%	0.1%	0.0%	0.3%	0.3%	0.0%	(X)	(X)	(X)	0.1%
Credit analysts 0830 (SOC 13-2041)	Male																
Credit analysts 0830 (SOC 13-2041)	Number	12,750	530	480	9,335	1,320	20	965	20	0	45	30	0	(X)	(X)	(X)	4
Credit analysts 0830 (SOC 13-2041)	Percent	42.2%	1.8%	1.6%	30.9%	4.4%	0.1%	3.2%	0.1%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.0%
Credit analysts 0830 (SOC 13-2041)	Female																
Credit analysts 0830 (SOC 13-2041)	Number	17 450	1 120	805	11 710	2 225	110	1 315	15	0	55	50	15	(X)	(X)	(X)	35
Credit analysts 0830 (SOC 13-2041)	Percent	57.8%	3.7%	2.7%	38.8%	7.4%	0.4%	4.4%	0.0%	0.0%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.1%
Financial analysts 0840 (SOC 13-2051)	Total, both sexes																
Financial analysts 0840 (SOC 13-2051)	Number	84 900	3 275	1 450	61 550	6 050	120	10 910	55	170	140	650	40	(X)	(X)	(X)	490
Financial analysts 0840 (SOC 13-2051)	Percent	100.0%	3.9%	1.7%	72.5%	7.1%	0.1%	12.9%	0.1%	0.2%	0.2%	0.8%	0.0%	(X)	(X)	(X)	0.6%
Financial analysts 0840 (SOC 13-2051)	Male																
Financial analysts 0840 (SOC 13-2051)	Number	56 645	2 110	875	43 445	2 960	50	6 320	45	45	70	485	0	(X)	(X)	(X)	250
Financial analysts 0840 (SOC 13-2051)	Percent	66.7%	2.5%	1.0%	51.2%	3.5%	0.1%	7.4%	0.1%	0.1%	0.1%	0.6%	0.0%	(X)	(X)	(X)	0.3%
Financial analysts 0840 (SOC 13-2051)	Female																
Financial analysts 0840 (SOC 13-2051)	Number	28 255	1 170	575	18 100	3 090	70	4 590	4	130	75	165	40	(X)	(X)	(X)	240
Financial analysts 0840 (SOC 13-2051)	Percent	33.3%	1.4%	0.7%	21.3%	3.6%	0.1%	5.4%	0.0%	0.2%	0.1%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Personal financial advisors 0850 (SOC 13-2052)	Total, both sexes																
Personal financial advisors 0850 (SOC 13-2052)	Number	353 120	14 305	6 720	283 590	22 015	675	21 505	300	625	560	1 125	95	(X)	(X)	(X)	1 605
Personal financial advisors 0850 (SOC 13-2052)	Percent	100.0%	4.1%	1.9%	80.3%	6.2%	0.2%	6.1%	0.1%	0.2%	0.2%	0.3%	0.0%	(X)	(X)	(X)	0.5%
Personal financial advisors 0850 (SOC 13-2052)	Male																
Personal financial advisors 0850 (SOC 13-2052)	Number	245 655	8 795	3 090	205 690	11 755	320	13 245	140	425	360	720	40	(X)	(X)	(X)	1 075
Personal financial advisors 0850 (SOC 13-2052)	Percent	69.6%	2.5%	0.9%	58.2%	3.3%	0.1%	3.8%	0.0%	0.1%	0.1%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Personal financial advisors 0850 (SOC 13-2052)	Female																
Personal financial advisors 0850 (SOC 13-2052)	Number	107 465	5 510	3 630	77 900	10 260	355	8 260	160	200	200	405	55	(X)	(X)	(X)	525
Personal financial advisors 0850 (SOC 13-2052)	Percent	30.4%	1.6%	1.0%	22.1%	2.9%	0.1%	2.3%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Insurance underwriters 0860 (SOC 13-2053)	Total, both sexes																
Insurance underwriters 0860 (SOC 13-2053)	Number	102 170	3 805	2 615	79 090	10 380	200	4 810	95	150	155	395	105	(X)	(X)	(X)	365
Insurance underwriters 0860 (SOC 13-2053)	Percent	100.0%	3.7%	2.6%	77.4%	10.2%	0.2%	4.7%	0.1%	0.1%	0.2%	0.4%	0.1%	(X)	(X)	(X)	0.4%
Insurance underwriters 0860 (SOC 13-2053)	Male																
Insurance underwriters 0860 (SOC 13-2053)	Number	32 825	1 120	640	26 530	2 540	35	1 690	4	40	25	135	15	(X)	(X)	(X)	50
Insurance underwriters 0860 (SOC 13-2053)	Percent	32.1%	1.1%	0.6%	26.0%	2.5%	0.0%	1.7%	0.0%	0.0%	0.0%	0.1%	0.0%	(X)	(X)	(X)	0.0%
Insurance underwriters 0860 (SOC 13-2053)	Female																
Insurance underwriters 0860 (SOC 13-2053)	Number	69 345	2 685	1 975	52 560	7 840	165	3 120	90	115	130	260	95	(X)	(X)	(X)	315
Insurance underwriters 0860 (SOC 13-2053)	Percent	67.9%	2.6%	1.9%	51.4%	7.7%	0.2%	3.1%	0.1%	0.1%	0.1%	0.3%	0.1%	(X)	(X)	(X)	0.3%
Financial examiners 0900 (SOC 13-2061)	Total, both sexes																
Financial examiners 0900 (SOC 13-2061)	Number	12 920	625	270	9 260	1 515	35	1 020	0	60	15	55	0	(X)	(X)	(X)	65
Financial examiners 0900 (SOC 13-2061)	Percent	100.0%	4.8%	2.1%	71.7%	11.7%	0.3%	7.9%	0.0%	0.5%	0.1%	0.4%	0.0%	(X)	(X)	(X)	0.5%
Financial examiners 0900 (SOC 13-2061)	Male																
Financial examiners 0900 (SOC 13-2061)	Number	7 075	285	125	5 645	445	10	495	0	20	0	20	0	(X)	(X)	(X)	30
Financial examiners 0900 (SOC 13-2061)	Percent	54.8%	2.2%	1.0%	43.7%	3.4%	0.1%	3.8%	0.0%	0.2%	0.0%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Financial examiners 0900 (SOC 13-2061)	Female																
Financial examiners 0900 (SOC 13-2061)	Number	5 845	340	145	3 615	1 070	25	525	0	40	15	35	0	(X)	(X)	(X)	35
Financial examiners 0900 (SOC 13-2061)	Percent	45.2%	2.6%	1.1%	28.0%	8.3%	0.2%	4.1%	0.0%	0.3%	0.1%	0.3%	0.0%	(X)	(X)	(X)	0.3%
Credit counselors and loan officers 0910 (SOC 13-2070)	Total, both sexes																
Credit counselors and loan officers 0910 (SOC 13-2070)	Number	386 045	28 875	14 590	278 410	37 715	835	19 480	805	655	1 225	1 225	240	(X)	(X)	(X)	1 995
Credit counselors and loan officers 0910 (SOC 13-2070)	Percent	100.0%	7.5%	3.8%	72.1%	9.8%	0.2%	5.0%	0.2%	0.2%	0.3%	0.3%	0.1%	(X)	(X)	(X)	0.5%
Credit counselors and loan officers 0910 (SOC 13-2070)	Male																
Credit counselors and loan officers 0910 (SOC 13-2070)	Number	180 140	12 350	6 090	136 200	13 975	390	8 565	305	440	420	455	95	(X)	(X)	(X)	865
Credit counselors and loan officers 0910 (SOC 13-2070)	Percent	46.7%	3.2%	1.6%	35.3%	3.6%	0.1%	2.2%	0.1%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Credit counselors and loan officers 0910 (SOC 13-2070)	Female																
Credit counselors and loan officers 0910 (SOC 13-2070)	Number	205 905	16 525	8 500	142 210	23 745	445	10 915	500	210	805	770	145	(X)	(X)	(X)	1 135
Credit counselors and loan officers 0910 (SOC 13-2070)	Percent	53.3%	4.3%	2.2%	36.8%	6.2%	0.1%	2.8%	0.1%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Tax examiners and collectors, and revenue agents 0930	Total, both sexes																
Tax examiners and collectors, and revenue agents 0930	Number	65 105	4 835	2 365	40 760	12 645	275	3 085	105	275	190	205	140	(X)	(X)	(X)	225
Tax examiners and collectors, and revenue agents 0930	Percent	100.0%	7.4%	3.6%	62.6%	19.4%	0.4%	4.7%	0.2%	0.4%	0.3%	0.3%	0.2%	(X)	(X)	(X)	0.3%
Tax examiners and collectors, and revenue agents 0930	Male																
Tax examiners and collectors, and revenue agents 0930	Number	23 350	2 375	720	15 050	3 190	65	1 525	35	110	80	115	0	(X)	(X)	(X)	85
Tax examiners and collectors, and revenue agents 0930	Percent	35.9%	3.6%	1.1%	23.1%	4.9%	0.1%	2.3%	0.1%	0.2%	0.1%	0.2%	0.0%	(X)	(X)	(X)	0.1%
Tax examiners and collectors, and revenue agents 0930	Female																
Tax examiners and collectors, and revenue agents 0930	Number	41 755	2 460	1 645	25 710	9 455	210	1 555	70	160	115	90	140	(X)	(X)	(X)	140
Tax examiners and collectors, and revenue agents 0930	Percent	64.1%	3.8%	2.5%	39.5%	14.5%	0.3%	2.4%	0.1%	0.2%	0.2%	0.1%	0.2%	(X)	(X)	(X)	0.2%
Tax preparers 0940 (SOC 13-2082)	Total, both sexes																
Tax preparers 0940 (SOC 13-2082)	Number	107 865	7 995	4 300	73 150	15 585	370	5 250	120	55	415	100	95	(X)	(X)	(X)	435
Tax preparers 0940 (SOC 13-2082)	Percent	100.0%	7.4%	4.0%	67.8%	14.4%	0.3%	4.9%	0.1%	0.1%	0.4%	0.1%	0.1%	(X)	(X)	(X)	0.4%
Tax preparers 0940 (SOC 13-2082)	Male																
Tax preparers 0940 (SOC 13-2082)	Number	37 200	2 620	1 215	27 010	3 990	50	1 935	40	30	60	45	20	(X)	(X)	(X)	185
Tax preparers 0940 (SOC 13-2082)	Percent	34.5%	2.4%	1.1%	25.0%	3.7%	0.0%	1.8%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.2%
Tax preparers 0940 (SOC 13-2082)	Female																
Tax preparers 0940 (SOC 13-2082)	Number	70 665	5 375	3 090	46 140	11 595	320	3 315	80	25	355	55	75	(X)	(X)	(X)	250
Tax preparers 0940 (SOC 13-2082)	Percent	65.5%	5.0%	2.9%	42.8%	10.7%	0.3%	3.1%	0.1%	0.0%	0.3%	0.1%	0.1%	(X)	(X)	(X)	0.2%
Financial specia ists all other 0950 (SOC 13-2099)	Total, both sexes																
Financial specia ists all other 0950 (SOC 13-2099)	Number	65 370	4 265	2 640	45 025	8 060	370	3 930	40	85	385	210	95	(X)	(X)	(X)	270
Financial specia ists all other 0950 (SOC 13-2099)	Percent	100.0%	6.5%	4.0%	68.9%	12.3%	0.6%	6.0%	0.1%	0.1%	0.6%	0.3%	0.1%	(X)	(X)	(X)	0.4%
Financial specia ists all other 0950 (SOC 13-2099)	Male																
Financial specia ists, all other 0950 (SOC 13-2099)	Number	28,725	1,925	900	20,675	3,100	155	1,565	0	20	85	70	95	(X)	(X)	(X)	140
Financial specia ists all other 0950 (SOC 13-2099)	Percent	43.9%	2.9%	1.4%	31.6%	4.7%	0.2%	2.4%	0.0%	0.0%	0.1%	0.1%	0.1%	(X)	(X)	(X)	0.2%
Financial specia ists all other 0950 (SOC 13-2099)	Female																
Financial specia ists, all other 0950 (SOC 13-2099)	Number	36,645	2,340	1,740	24,355	4,960	215	2,360	40	65	300	140	0	(X)	(X)	(X)	130
Financial specia ists all other 0950 (SOC 13-2099)	Percent	56.1%	3.6%	2.7%	37.3%	7.6%	0.3%	3.6%	0.1%	0.1%	0.5%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Computer and information research scientists 1005 (SOC	Total, both sexes																
Computer and information research scientists 1005 (SOC	Number	16 090	585	290	10 540	1 055	25	3 405	40	30	30	75	0	(X)	(X)	(X)	20
Computer and information research scientists 1005 (SOC	Percent	100.0%	3.6%	1.8%	65.5%	6.6%	0.2%	21.2%	0.2%	0.2%	0.2%	0.5%	0.0%	(X)	(X)	(X)	0.1%
Computer and information research scientists 1005 (SOC	Male																
Computer and information research scientists 1005 (SOC	Number	11 260	345	195	7 415	560	4	2 580	40	30	30	45	0	(X)	(X)	(X)	15
Computer and information research scientists 1005 (SOC	Percent	70.0%	2.1%	1.2%	46.1%	3.5%	0.0%	16.0%	0.2%	0.2%	0.2%	0.3%	0.0%	(X)	(X)	(X)	0.1%
Computer and information research scientists 1005 (SOC	Female																
Computer and information research scientists 1005 (SOC	Number	4 830	235	100	3 125	495	20	820	0	0	0	30	0	(X)	(X)	(X)	10
Computer and information research scientists 1005 (SOC	Percent	30.0%	1.5%	0.6%	19.4%	3.1%	0.1%	5.1%	0.0%	0.0%	0.0%	0.2%	0.0%	(X)	(X)	(X)	0.1%
Computer systems analysts 1006 (SOC 15-1121)	Total, both sexes																
Computer systems analysts 1006 (SOC 15-1121)	Number	486 535	17 205	7 615	330 725	41 405	1 225	80 165	390	635	1 250	1 815	310	(X)	(X)	(X)	3 800
Computer systems analysts 1006 (SOC 15-1121)	Percent	100.0%	3.5%	1.6%	68.0%	8.5%	0.3%	16.5%	0.1%	0.1%	0.3%	0.4%	0.1%	(X)	(X)	(X)	0.8%
Computer systems analysts 1006 (SOC 15-1121)	Male																
Computer systems analysts 1006 (SOC 15-1121)	Number	314 990	11 560	4 645	215 070	21 910	750	55 655	195	395	795	1 030	185	(X)	(X)	(X)	2 785
Computer systems analysts 1006 (SOC 15-1121)	Percent	64.7%	2.4%	1.0%	44.2%	4.5%	0.2%	11.4%	0.0%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.6%
Computer systems analysts 1006 (SOC 15-1121)	Female																
Computer systems analysts 1006 (SOC 15-1121)	Number	171 545	5 645	2 965	115 655	19 490	475	24 510	195	240	450	780	125	(X)	(X)	(X)	1 015
Computer systems analysts 1006 (SOC 15-1121)	Percent	35.3%	1.2%	0.6%	23.8%	4.0%	0.1%	5.0%	0.0%	0.0%	0.1%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Information security analysts 1007 (SOC 15-1122)	Total, both sexes																
Information security analysts 1007 (SOC 15-1122)	Number	42 010	1 685	1 015	31 215	4 410	75	2 770	75	65	165	200	35	(X)	(X)	(X)	305
Information security analysts 1007 (SOC 15-1122)	Percent	100.0%	4.0%	2.4%	74.3%	10.5%	0.2%	6.6%	0.2%	0.2%	0.4%	0.5%	0.1%	(X)	(X)	(X)	0.7%
Information security analysts 1007 (SOC 15-1122)	Male																
Information security analysts 1007 (SOC 15-1122)	Number	31 330	1 455	660	23 830	2 780	65	1 935	55	35	125	170	35	(X)	(X)	(X)	200
Information security analysts 1007 (SOC 15-1122)	Percent	74.6%	3.5%	1.6%	56.7%	6.6%	0.2%	4.6%	0.1%	0.1%	0.3%	0.4%	0.1%	(X)	(X)	(X)	0.5%
Information security analysts 1007 (SOC 15-1122)	Female																
Information security analysts 1007 (SOC 15-1122)	Number	10 685	235	355	7 385	1 630	10	835	20	30	40	30	0	(X)	(X)	(X)	105
Information security analysts 1007 (SOC 15-1122)	Percent	25.4%	0.6%	0.8%	17.6%	3.9%	0.0%	2.0%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Computer programmers 1010 (SOC 15-1131)	Total, both sexes																
Computer programmers 1010 (SOC 15-1131)	Number	522 290	16 345	8 220	374 965	25 105	1 060	88 335	360	765	1 560	2 135	280	(X)	(X)	(X)	3 155
Computer programmers 1010 (SOC 15-1131)	Percent	100.0%	3.1%	1.6%	71.8%	4.8%	0.2%	16.9%	0.1%	0.1%	0.3%	0.4%	0.1%	(X)	(X)	(X)	0.6%
Computer programmers 1010 (SOC 15-1131)	Male																
Computer programmers 1010 (SOC 15-1131)	Number	394 745	12 990	6 425	290 660	16 700	755	60 900	285	670	1 185	1 590	140	(X)	(X)	(X)	2 450
Computer programmers 1010 (SOC 15-1131)	Percent	75.6%	2.5%	1.2%	55.7%	3.2%	0.1%	11.7%	0.1%	0.1%	0.2%	0.3%	0.0%	(X)	(X)	(X)	0.5%

Computer programmers 1010 (SOC 15-1131)	Female																
Computer programmers 1010 (SOC 15-1131)	Number	127 545	3 355	1 795	84 305	8 410	300	27 435	80	95	370	540	145	(X)	(X)	(X)	705
Computer programmers 1010 (SOC 15-1131)	Percent	24.4%	0.6%	0.3%	16.1%	1.6%	0.1%	5.3%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Software developers, applications and systems software	Total, both sexes																
Software developers applications and systems software	Number	860 790	22 575	10 655	525 150	37 710	1 505	247 000	670	1 200	2 010	4 175	290	(X)	(X)	(X)	7 850
Software developers applications and systems software	Percent	100.0%	2.6%	1.2%	61.0%	4.4%	0.2%	28.7%	0.1%	0.1%	0.2%	0.5%	0.0%	(X)	(X)	(X)	0.9%
Software developers applications and systems software	Male																
Software developers applications and systems software	Number	673 485	18 220	8 115	425 990	23 670	1 015	184 015	465	960	1 520	3 275	155	(X)	(X)	(X)	6 085
Software developers applications and systems software	Percent	78.2%	2.1%	0.9%	49.5%	2.7%	0.1%	21.4%	0.1%	0.1%	0.2%	0.4%	0.0%	(X)	(X)	(X)	0.7%
Software developers applications and systems software	Female																
Software developers applications and systems software	Number	187 305	4 360	2 540	99 160	14 040	490	62 980	210	240	485	900	135	(X)	(X)	(X)	1 765
Software developers applications and systems software	Percent	21.8%	0.5%	0.3%	11.5%	1.6%	0.1%	7.3%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Web developers 1030 (SOC 15-1134)	Total, both sexes																
Web developers 1030 (SOC 15-1134)	Number	162 325	6 420	3 055	125 235	7 530	550	15 225	205	525	945	1 260	85	(X)	(X)	(X)	1 290
Web developers 1030 (SOC 15-1134)	Percent	100.0%	4.0%	1.9%	77.2%	4.6%	0.3%	9.4%	0.1%	0.3%	0.6%	0.8%	0.1%	(X)	(X)	(X)	0.8%
Web developers 1030 (SOC 15-1134)	Male																
Web developers 1030 (SOC 15-1134)	Number	104 545	4 390	1 850	81 065	4 970	385	9 180	125	360	565	820	70	(X)	(X)	(X)	765
Web developers 1030 (SOC 15-1134)	Percent	64.4%	2.7%	1.1%	49.9%	3.1%	0.2%	5.7%	0.1%	0.2%	0.3%	0.5%	0.0%	(X)	(X)	(X)	0.5%
Web developers 1030 (SOC 15-1134)	Female																
Web developers 1030 (SOC 15-1134)	Number	57 780	2 030	1 205	44 170	2 560	165	6 045	80	165	380	445	15	(X)	(X)	(X)	525
Web developers 1030 (SOC 15-1134)	Percent	35.6%	1.3%	0.7%	27.2%	1.6%	0.1%	3.7%	0.0%	0.1%	0.2%	0.3%	0.0%	(X)	(X)	(X)	0.3%
Computer support specialists 1050 (SOC 15-1150)	Total both sexes																
Computer support specialists 1050 (SOC 15-1150)	Number	519 840	26 975	15 060	367 800	56 390	1 975	41 550	855	1 280	2 150	2 690	370	(X)	(X)	(X)	2 740
Computer support specialists 1050 (SOC 15-1150)	Percent	100.0%	5.2%	2.9%	70.8%	10.8%	0.4%	8.0%	0.2%	0.2%	0.4%	0.5%	0.1%	(X)	(X)	(X)	0.5%
Computer support specialists 1050 (SOC 15-1150)	Male																
Computer support specialists 1050 (SOC 15-1150)	Number	367,120	19,250	10,810	262,925	33,825	1,175	31,865	610	940	1,485	2,040	160	(X)	(X)	(X)	2,035
Computer support specialists 1050 (SOC 15-1150)	Percent	70.6%	3.7%	2.1%	50.6%	6.5%	0.2%	6.1%	0.1%	0.2%	0.3%	0.4%	0.0%	(X)	(X)	(X)	0.4%
Computer support specialists 1050 (SOC 15-1150)	Female																
Computer support specialists 1050 (SOC 15-1150)	Number	152,720	7,725	4,250	104,875	22,570	800	9,685	245	340	665	650	210	(X)	(X)	(X)	705
Computer support specialists 1050 (SOC 15-1150)	Percent	29.4%	1.5%	0.8%	20.2%	4.3%	0.2%	1.9%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Database administrators 1060 (SOC 15-1141)	Total both sexes																
Database administrators 1060 (SOC 15-1141)	Number	107 585	3 320	1 935	75 880	7 905	190	16 645	85	165	295	400	50	(X)	(X)	(X)	725
Database administrators 1060 (SOC 15-1141)	Percent	100.0%	3.1%	1.8%	70.5%	7.3%	0.2%	15.5%	0.1%	0.2%	0.3%	0.4%	0.0%	(X)	(X)	(X)	0.7%
Database administrators 1060 (SOC 15-1141)	Male																
Database administrators 1060 (SOC 15-1141)	Number	67 085	2 110	1 410	47 070	4 305	105	11 030	80	75	170	280	25	(X)	(X)	(X)	430
Database administrators 1060 (SOC 15-1141)	Percent	62.4%	2.0%	1.3%	43.8%	4.0%	0.1%	10.3%	0.1%	0.1%	0.2%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Database administrators 1060 (SOC 15-1141)	Female																
Database administrators 1060 (SOC 15-1141)	Number	40 500	1 210	525	28 810	3 600	85	5 615	4	90	125	120	25	(X)	(X)	(X)	300
Database administrators 1060 (SOC 15-1141)	Percent	37.6%	1.1%	0.5%	26.8%	3.3%	0.1%	5.2%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Network and computer systems administrators 1105 (SOC	Total both sexes																
Network and computer systems administrators 1105 (SOC	Number	269 780	12 490	6 045	197 265	22 500	940	25 670	285	400	1 155	1 150	405	(X)	(X)	(X)	1 485
Network and computer systems administrators 1105 (SOC	Percent	100.0%	4.6%	2.2%	73.1%	8.3%	0.3%	9.5%	0.1%	0.1%	0.4%	0.4%	0.2%	(X)	(X)	(X)	0.6%
Network and computer systems administrators 1105 (SOC	Male																
Network and computer systems administrators 1105 (SOC	Number	214 530	10 250	5 000	158 205	15 280	645	21 290	275	305	860	960	290	(X)	(X)	(X)	1 175
Network and computer systems administrators 1105 (SOC	Percent	79.5%	3.8%	1.9%	58.6%	5.7%	0.2%	7.9%	0.1%	0.1%	0.3%	0.4%	0.1%	(X)	(X)	(X)	0.4%
Network and computer systems administrators 1105 (SOC	Female																
Network and computer systems administrators 1105 (SOC	Number	55 250	2 240	1 045	39 065	7 220	290	4 380	10	95	295	190	115	(X)	(X)	(X)	310
Network and computer systems administrators 1105 (SOC	Percent	20.5%	0.8%	0.4%	14.5%	2.7%	0.1%	1.6%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Computer network architects 1106 (SOC 15-1143)	Total both sexes																
Computer network architects 1106 (SOC 15-1143)	Number	109 325	3 995	2 505	77 340	9 345	295	13 500	200	380	370	385	35	(X)	(X)	(X)	980
Computer network architects 1106 (SOC 15-1143)	Percent	100.0%	3.7%	2.3%	70.7%	8.5%	0.3%	12.3%	0.2%	0.3%	0.3%	0.4%	0.0%	(X)	(X)	(X)	0.9%
Computer network architects 1106 (SOC 15-1143)	Male																
Computer network architects 1106 (SOC 15-1143)	Number	97 220	3 655	2 235	69 530	7 795	260	11 780	200	310	335	305	35	(X)	(X)	(X)	785
Computer network architects 1106 (SOC 15-1143)	Percent	88.9%	3.3%	2.0%	63.6%	7.1%	0.2%	10.8%	0.2%	0.3%	0.3%	0.3%	0.0%	(X)	(X)	(X)	0.7%
Computer network architects 1106 (SOC 15-1143)	Female																
Computer network architects 1106 (SOC 15-1143)	Number	12 105	340	270	7 815	1 550	35	1 720	0	70	35	80	0	(X)	(X)	(X)	190
Computer network architects 1106 (SOC 15-1143)	Percent	11.1%	0.3%	0.2%	7.1%	1.4%	0.0%	1.6%	0.0%	0.1%	0.0%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Computer occupations a l other 1107 (SOC 15-1199)	Total both sexes																
Computer occupations a l other 1107 (SOC 15-1199)	Number	287 425	13 485	8 775	194 675	29 020	1 430	34 315	480	480	1 075	1 335	250	(X)	(X)	(X)	2 110
Computer occupations a l other 1107 (SOC 15-1199)	Percent	100.0%	4.7%	3.1%	67.7%	10.1%	0.5%	11.9%	0.2%	0.2%	0.4%	0.5%	0.1%	(X)	(X)	(X)	0.7%
Computer occupations a l other 1107 (SOC 15-1199)	Male																
Computer occupations a l other 1107 (SOC 15-1199)	Number	217 285	10 590	7 030	149 100	19 530	1 025	25 600	350	335	905	980	230	(X)	(X)	(X)	1 610
Computer occupations a l other 1107 (SOC 15-1199)	Percent	75.6%	3.7%	2.4%	51.9%	6.8%	0.4%	8.9%	0.1%	0.1%	0.3%	0.3%	0.1%	(X)	(X)	(X)	0.6%
Computer occupations a l other 1107 (SOC 15-1199)	Female																
Computer occupations a l other 1107 (SOC 15-1199)	Number	70 135	2 895	1 745	45 575	9 490	405	8 715	130	145	175	355	20	(X)	(X)	(X)	500
Computer occupations a l other 1107 (SOC 15-1199)	Percent	24.4%	1.0%	0.6%	15.9%	3.3%	0.1%	3.0%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Actuaries 1200 (SOC 15-2011)	Total both sexes																
Actuaries 1200 (SOC 15-2011)	Number	24 310	440	100	20 105	645	10	2 675	20	20	35	185	0	(X)	(X)	(X)	70
Actuaries 1200 (SOC 15-2011)	Percent	100.0%	1.8%	0.4%	82.7%	2.7%	0.0%	11.0%	0.1%	0.1%	0.1%	0.8%	0.0%	(X)	(X)	(X)	0.3%
Actuaries 1200 (SOC 15-2011)	Male																
Actuaries 1200 (SOC 15-2011)	Number	16 110	295	100	13 890	320	0	1 330	20	20	0	80	0	(X)	(X)	(X)	55
Actuaries 1200 (SOC 15-2011)	Percent	66.3%	1.2%	0.4%	57.1%	1.3%	0.0%	5.5%	0.1%	0.1%	0.0%	0.3%	0.0%	(X)	(X)	(X)	0.2%
Actuaries 1200 (SOC 15-2011)	Female																
Actuaries 1200 (SOC 15-2011)	Number	8 200	145	0	6 215	325	10	1 350	0	0	35	105	0	(X)	(X)	(X)	15
Actuaries 1200 (SOC 15-2011)	Percent	33.7%	0.6%	0.0%	25.6%	1.3%	0.0%	5.6%	0.0%	0.0%	0.1%	0.4%	0.0%	(X)	(X)	(X)	0.1%
Operations research analysts 1220 (SOC 15-2031)	Total, both sexes																
Operations research analysts 1220 (SOC 15-2031)	Number	120 780	5 500	2 740	87 305	13 510	285	9 390	190	335	310	535	120	(X)	(X)	(X)	555
Operations research analysts 1220 (SOC 15-2031)	Percent	100.0%	4.6%	2.3%	72.3%	11.2%	0.2%	7.8%	0.2%	0.3%	0.3%	0.4%	0.1%	(X)	(X)	(X)	0.5%
Operations research analysts 1220 (SOC 15-2031)	Male																
Operations research analysts 1220 (SOC 15-2031)	Number	62 465	2 705	1 400	47 445	4 870	140	4 870	95	210	175	245	30	(X)	(X)	(X)	285
Operations research analysts 1220 (SOC 15-2031)	Percent	51.7%	2.2%	1.2%	39.3%	4.0%	0.1%	4.0%	0.1%	0.2%	0.1%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Operations research analysts 1220 (SOC 15-2031)	Female																
Operations research analysts 1220 (SOC 15-2031)	Number	58 315	2 795	1 345	39 860	8 640	150	4 520	95	125	140	285	90	(X)	(X)	(X)	270
Operations research analysts 1220 (SOC 15-2031)	Percent	48.3%	2.3%	1.1%	33.0%	7.2%	0.1%	3.7%	0.1%	0.1%	0.1%	0.2%	0.1%	(X)	(X)	(X)	0.2%
Miscellaneous mathematical science occupations	Total both sexes																
Miscellaneous mathematical science occupations	Number	40 775	1 560	545	27 925	2 820	165	6 990	110	75	135	195	20	(X)	(X)	(X)	235
Miscellaneous mathematical science occupations	Percent	100.0%	3.8%	1.3%	68.5%	6.9%	0.4%	17.1%	0.3%	0.2%	0.3%	0.5%	0.0%	(X)	(X)	(X)	0.6%
Miscellaneous mathematical science occupations	Male																
Miscellaneous mathematical science occupations	Number	21 325	775	150	15 965	930	50	3 040	0	45	110	140	20	(X)	(X)	(X)	105
Miscellaneous mathematical science occupations	Percent	52.3%	1.9%	0.4%	39.2%	2.3%	0.1%	7.5%	0.0%	0.1%	0.3%	0.3%	0.0%	(X)	(X)	(X)	0.3%
Miscellaneous mathematical science occupations	Female																
Miscellaneous mathematical science occupations	Number	19 450	785	395	11 960	1 890	110	3 950	110	30	25	60	0	(X)	(X)	(X)	130
Miscellaneous mathematical science occupations	Percent	47.7%	1.9%	1.0%	29.3%	4.6%	0.3%	9.7%	0.3%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Architects except naval 1300 (SOC 17-1010)	Total both sexes																
Architects except naval 1300 (SOC 17-1010)	Number	198 105	10 160	4 380	157 820	5 165	345	17 550	195	190	565	910	65	(X)	(X)	(X)	755
Architects except naval 1300 (SOC 17-1010)	Percent	100.0%	5.1%	2.2%	79.7%	2.6%	0.2%	8.9%	0.1%	0.1%	0.3%	0.5%	0.0%	(X)	(X)	(X)	0.4%
Architects except naval 1300 (SOC 17-1010)	Male																
Architects except naval 1300 (SOC 17-1010)	Number	148 095	7 370	3 185	120 010	3 730	285	11 885	130	105	355	490	20	(X)	(X)	(X)	530
Architects except naval 1300 (SOC 17-1010)	Percent	74.8%	3.7%	1.6%	60.6%	1.9%	0.1%	6.0%	0.1%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Architects except naval 1300 (SOC 17-1010)	Female																
Architects, except naval 1300 (SOC 17-1010)	Number	50,010	2,790	1,195	37,810	1,435	60	5,670	60	85	210	425	45	(X)	(X)	(X)	225
Architects except naval 1300 (SOC 17-1010)	Percent	25.2%	1.4%	0.6%	19.1%	0.7%	0.0%	2.9%	0.0%	0.0%	0.1%	0.2%	0.0%	(X)	(X)	(X)	0.1%
Surveyors cartographers and photogrammetrists 1310	Total both sexes																
Surveyors, cartographers, and photogrammetrists 1310	Number	40,140	1,510	600	34,730	1,490	245	1,030	0	70	175	180	15	(X)	(X)	(X)	95
Surveyors cartographers and photogrammetrists 1310	Percent	100.0%	3.8%	1.5%	86.5%	3.7%	0.6%	2.6%	0.0%	0.2%	0.4%	0.4%	0.0%	(X)	(X)	(X)	0.2%
Surveyors cartographers and photogrammetrists 1310	Male																
Surveyors cartographers and photogrammetrists 1310	Number	32 695	1 210	420	28 695	1 105	195	695	0	70	125	115	15	(X)	(X)	(X)	45
Surveyors cartographers and photogrammetrists 1310	Percent	81.5%	3.0%	1.0%	71.5%	2.8%	0.5%	1.7%	0.0%	0.2%	0.3%	0.3%	0.0%	(X)	(X)	(X)	0.1%
Surveyors cartographers and photogrammetrists 1310	Female																
Surveyors cartographers and photogrammetrists 1310	Number	7 445	300	175	6 035	385	50	335	0	0	45	70	0	(X)	(X)	(X)	50
Surveyors cartographers and photogrammetrists 1310	Percent	18.5%	0.7%	0.4%	15.0%	1.0%	0.1%	0.8%	0.0%	0.0%	0.1%	0.2%	0.0%	(X)	(X)	(X)	0.1%
Aerospace engineers 1320 (SOC 17-2011)	Total both sexes																
Aerospace engineers 1320 (SOC 17-2011)	Number	139 665	5 585	2 450	105 405	5 545	395	17 990	140	190	445	755	230	(X)	(X)	(X)	530
Aerospace engineers 1320 (SOC 17-2011)	Percent	100.0%	4.0%	1.8%	75.5%	4.0%	0.3%	12.9%	0.1%	0.1%	0.3%	0.5%	0.2%	(X)	(X)	(X)	0.4%
Aerospace engineers 1320 (SOC 17-2011)	Male																
Aerospace engineers 1320 (SOC 17-2011)	Number	123 200	4 860	2 140	94 270	4 705	320	14 980	140	165	410	645	145	(X)	(X)	(X)	420
Aerospace engineers 1320 (SOC 17-2011)	Percent	88.2%	3.5%	1.5%	67.5%	3.4%	0.2%	10.7%	0.1%	0.1%	0.3%	0.5%	0.1%	(X)	(X)	(X)	0.3%
Aerospace engineers 1320 (SOC 17-2011)	Female																
Aerospace engineers 1320 (SOC 17-2011)	Number	16 460	725	315	11 140	840	75	3 010	0	25	35	110	85	(X)	(X)	(X)	110
Aerospace engineers 1320 (SOC 17-2011)	Percent	11.8%	0.5%	0.2%	8.0%	0.6%	0.1%	2.2%	0.0%	0.0%	0.0%	0.1%	0.1%	(X)	(X)	(X)	0.1%
Biomedical and agricu tural engineers 1340 (SOC 17-	Total both sexes																
Biomedical and agricu tural engineers 1340 (SOC 17-	Number	13 860	415	310	10 660	720	35	1 550	0	10	30	60	0	(X)	(X)	(X)	75
Biomedical and agricu tural engineers 1340 (SOC 17-	Percent	100.0%	3.0%	2.2%	76.9%	5.2%	0.3%	11.2%	0.0%	0.1%	0.2%	0.4%	0.0%	(X)	(X)	(X)	0.5%
Biomedical and agricu tural engineers 1340 (SOC 17-	Male																
Biomedical and agricu tural engineers 1340 (SOC 17-	Number	11 575	385	205	8 975	680	35	1 185	0	10	30	35	0	(X)	(X)	(X)	40
Biomedical and agricu tural engineers 1340 (SOC 17-	Percent	83.5%	2.8%	1.5%	64.8%	4.9%	0.3%	8.5%	0.0%	0.1%	0.2%	0.3%	0.0%	(X)	(X)	(X)	0.3%
Biomedical and agricu tural engineers 1340 (SOC 17-	Female																
Biomedical and agricu tural engineers 1340 (SOC 17-	Number	2 285	30	105	1 680	40	0	365	0	0	0	25	0	(X)	(X)	(X)	35
Biomedical and agricu tural engineers 1340 (SOC 17-	Percent	16.5%	0.2%	0.8%	12.1%	0.3%	0.0%	2.6%	0.0%	0.0%	0.0%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Chemical engineers 1350 (SOC 17-2041)	Total both sexes																
Chemical engineers 1350 (SOC 17-2041)	Number	60 555	2 085	1 010	46 320	3 270	75	7 145	4	65	100	175	25	(X)	(X)	(X)	275
Chemical engineers 1350 (SOC 17-2041)	Percent	100.0%	3.4%	1.7%	76.5%	5.4%	0.1%	11.8%	0.0%	0.1%	0.2%	0.3%	0.0%	(X)	(X)	(X)	0.5%
Chemical engineers 1350 (SOC 17-2041)	Male																
Chemical engineers 1350 (SOC 17-2041)	Number	51 375	1 765	695	40 010	2 535	75	5 740	4	40	85	155	25	(X)	(X)	(X)	245
Chemical engineers 1350 (SOC 17-2041)	Percent	84.8%	2.9%	1.1%	66.1%	4.2%	0.1%	9.5%	0.0%	0.1%	0.1%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Chemical engineers 1350 (SOC 17-2041)	Female																
Chemical engineers 1350 (SOC 17-2041)	Number	9 185	325	315	6 315	735	4	1 405	0	25	15	25	0	(X)	(X)	(X)	30
Chemical engineers 1350 (SOC 17-2041)	Percent	15.2%	0.5%	0.5%	10.4%	1.2%	0.0%	2.3%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%

Civil engineers 1360 (SOC 17-2051)	Total, both sexes																
Civil engineers 1360 (SOC 17-2051)	Number	322 820	11 875	5 775	251 915	14 410	855	33 230	375	180	905	1 385	55	(X)	(X)	(X)	1 855
Civil engineers 1360 (SOC 17-2051)	Percent	100.0%	3.7%	1.8%	78.0%	4.5%	0.3%	10.3%	0.1%	0.1%	0.3%	0.4%	0.0%	(X)	(X)	(X)	0.6%
Civil engineers 1360 (SOC 17-2051)	Male																
Civil engineers 1360 (SOC 17-2051)	Number	281 770	9 730	4 695	223 350	12 080	720	27 495	255	155	645	1 035	50	(X)	(X)	(X)	1 560
Civil engineers 1360 (SOC 17-2051)	Percent	87.3%	3.0%	1.5%	69.2%	3.7%	0.2%	8.5%	0.1%	0.0%	0.2%	0.3%	0.0%	(X)	(X)	(X)	0.5%
Civil engineers 1360 (SOC 17-2051)	Female																
Civil engineers 1360 (SOC 17-2051)	Number	41 050	2 140	1 080	28 570	2 330	135	5 735	120	25	260	355	4	(X)	(X)	(X)	295
Civil engineers 1360 (SOC 17-2051)	Percent	12.7%	0.7%	0.3%	8.9%	0.7%	0.0%	1.8%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Computer hardware engineers 1400 (SOC 17-2061)	Total, both sexes																
Computer hardware engineers 1400 (SOC 17-2061)	Number	65 755	2 515	1 330	41 305	4 310	310	14 860	20	145	125	290	20	(X)	(X)	(X)	520
Computer hardware engineers 1400 (SOC 17-2061)	Percent	100.0%	3.8%	2.0%	62.8%	6.6%	0.5%	22.6%	0.0%	0.2%	0.2%	0.4%	0.0%	(X)	(X)	(X)	0.8%
Computer hardware engineers 1400 (SOC 17-2061)	Male																
Computer hardware engineers 1400 (SOC 17-2061)	Number	55 415	2 090	1 105	35 395	3 465	265	12 135	4	120	120	245	0	(X)	(X)	(X)	475
Computer hardware engineers 1400 (SOC 17-2061)	Percent	84.3%	3.2%	1.7%	53.8%	5.3%	0.4%	18.5%	0.0%	0.2%	0.2%	0.4%	0.0%	(X)	(X)	(X)	0.7%
Computer hardware engineers 1400 (SOC 17-2061)	Female																
Computer hardware engineers 1400 (SOC 17-2061)	Number	10 345	425	225	5 910	845	45	2 725	20	30	10	45	20	(X)	(X)	(X)	45
Computer hardware engineers 1400 (SOC 17-2061)	Percent	15.7%	0.6%	0.3%	9.0%	1.3%	0.1%	4.1%	0.0%	0.0%	0.0%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Electrical and electronics engineers 1410 (SOC 17-2070)	Total, both sexes																
Electrical and electronics engineers 1410 (SOC 17-2070)	Number	242 135	9 340	4 645	172 435	12 365	605	39 635	145	205	660	845	105	(X)	(X)	(X)	1 145
Electrical and electronics engineers 1410 (SOC 17-2070)	Percent	100.0%	3.9%	1.9%	71.2%	5.1%	0.2%	16.4%	0.1%	0.1%	0.3%	0.3%	0.0%	(X)	(X)	(X)	0.5%
Electrical and electronics engineers 1410 (SOC 17-2070)	Male																
Electrical and electronics engineers 1410 (SOC 17-2070)	Number	220 100	8 270	4 060	160 100	10 395	515	34 065	130	205	620	655	45	(X)	(X)	(X)	1 035
Electrical and electronics engineers 1410 (SOC 17-2070)	Percent	90.9%	3.4%	1.7%	66.1%	4.3%	0.2%	14.1%	0.1%	0.1%	0.3%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Electrical and electronics engineers 1410 (SOC 17-2070)	Female																
Electrical and electronics engineers 1410 (SOC 17-2070)	Number	22,040	1,070	585	12,335	1,970	85	5,570	20	0	40	190	65	(X)	(X)	(X)	110
Electrical and electronics engineers 1410 (SOC 17-2070)	Percent	9.1%	0.4%	0.2%	5.1%	0.8%	0.0%	2.3%	0.0%	0.0%	0.0%	0.1%	0.0%	(X)	(X)	(X)	0.0%
Environmental engineers 1420 (SOC 17-2081)	Total, both sexes																
Environmental engineers 1420 (SOC 17-2081)	Number	34,200	840	615	26,690	2,220	155	3,245	45	80	75	95	0	(X)	(X)	(X)	140
Environmental engineers 1420 (SOC 17-2081)	Percent	100.0%	2.5%	1.8%	78.0%	6.5%	0.5%	9.5%	0.1%	0.2%	0.2%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Environmental engineers 1420 (SOC 17-2081)	Male																
Environmental engineers 1420 (SOC 17-2081)	Number	25 790	670	450	20 455	1 660	110	2 170	4	15	65	95	0	(X)	(X)	(X)	100
Environmental engineers 1420 (SOC 17-2081)	Percent	75.4%	2.0%	1.3%	59.8%	4.9%	0.3%	6.3%	0.0%	0.0%	0.2%	0.3%	0.0%	(X)	(X)	(X)	0.3%
Environmental engineers 1420 (SOC 17-2081)	Female																
Environmental engineers 1420 (SOC 17-2081)	Number	8 405	170	165	6 230	565	45	1 075	40	70	10	0	0	(X)	(X)	(X)	35
Environmental engineers 1420 (SOC 17-2081)	Percent	24.6%	0.5%	0.5%	18.2%	1.7%	0.1%	3.1%	0.1%	0.2%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Industrial engineers including health and safety 1430	Total, both sexes																
Industrial engineers including health and safety 1430	Number	178 055	6 340	3 620	140 720	8 110	370	16 460	205	195	670	615	30	(X)	(X)	(X)	720
Industrial engineers including health and safety 1430	Percent	100.0%	3.6%	2.0%	79.0%	4.6%	0.2%	9.2%	0.1%	0.1%	0.4%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Industrial engineers including health and safety 1430	Male																
Industrial engineers including health and safety 1430	Number	144 700	5 220	2 680	116 870	5 810	340	11 880	145	140	530	465	30	(X)	(X)	(X)	600
Industrial engineers including health and safety 1430	Percent	81.3%	2.9%	1.5%	65.6%	3.3%	0.2%	6.7%	0.1%	0.1%	0.3%	0.3%	0.0%	(X)	(X)	(X)	0.3%
Industrial engineers including health and safety 1430	Female																
Industrial engineers including health and safety 1430	Number	33 355	1 125	940	23 845	2 300	35	4 580	65	55	140	150	0	(X)	(X)	(X)	120
Industrial engineers including health and safety 1430	Percent	18.7%	0.6%	0.5%	13.4%	1.3%	0.0%	2.6%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Marine engineers and naval arch tects 1440 (SOC 17-	Total, both sexes																
Marine engineers and naval arch tects 1440 (SOC 17-	Number	11 910	160	55	9 825	790	60	895	4	35	35	0	20	(X)	(X)	(X)	35
Marine engineers and naval arch tects 1440 (SOC 17-	Percent	100.0%	1.3%	0.5%	82.5%	6.6%	0.5%	7.5%	0.0%	0.3%	0.3%	0.0%	0.2%	(X)	(X)	(X)	0.3%
Marine engineers and naval arch tects 1440 (SOC 17-	Male																
Marine engineers and naval arch tects 1440 (SOC 17-	Number	10 995	150	55	9 095	710	60	810	4	35	35	0	20	(X)	(X)	(X)	25
Marine engineers and naval arch tects 1440 (SOC 17-	Percent	92.3%	1.3%	0.5%	76.4%	6.0%	0.5%	6.8%	0.0%	0.3%	0.3%	0.0%	0.2%	(X)	(X)	(X)	0.2%
Marine engineers and naval arch tects 1440 (SOC 17-	Female																
Marine engineers and naval arch tects 1440 (SOC 17-	Number	920	10	0	730	80	0	90	0	0	0	0	0	(X)	(X)	(X)	4
Marine engineers and naval arch tects 1440 (SOC 17-	Percent	7.7%	0.1%	0.0%	6.1%	0.7%	0.0%	0.8%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Materials engineers 1450 (SOC 17-2131)	Total, both sexes																
Materials engineers 1450 (SOC 17-2131)	Number	32 820	995	605	24 655	1 170	100	4 795	50	0	145	190	4	(X)	(X)	(X)	120
Materials engineers 1450 (SOC 17-2131)	Percent	100.0%	3.0%	1.8%	75.1%	3.6%	0.3%	14.6%	0.2%	0.0%	0.4%	0.6%	0.0%	(X)	(X)	(X)	0.4%
Materials engineers 1450 (SOC 17-2131)	Male																
Materials engineers 1450 (SOC 17-2131)	Number	28 865	865	500	22 095	1 005	80	3 900	50	0	130	130	4	(X)	(X)	(X)	110
Materials engineers 1450 (SOC 17-2131)	Percent	87.9%	2.6%	1.5%	67.3%	3.1%	0.2%	11.9%	0.2%	0.0%	0.4%	0.4%	0.0%	(X)	(X)	(X)	0.3%
Materials engineers 1450 (SOC 17-2131)	Female																
Materials engineers 1450 (SOC 17-2131)	Number	3 955	130	105	2 560	165	20	895	0	0	15	55	0	(X)	(X)	(X)	10
Materials engineers 1450 (SOC 17-2131)	Percent	12.1%	0.4%	0.3%	7.8%	0.5%	0.1%	2.7%	0.0%	0.0%	0.0%	0.2%	0.0%	(X)	(X)	(X)	0.0%
Mechanical engineers 1460 (SOC 17-2141)	Total, both sexes																
Mechanical engineers 1460 (SOC 17-2141)	Number	237 395	7 055	4 420	189 330	9 265	495	23 905	185	195	520	745	110	(X)	(X)	(X)	1 175
Mechanical engineers 1460 (SOC 17-2141)	Percent	100.0%	3.0%	1.9%	79.8%	3.9%	0.2%	10.1%	0.1%	0.1%	0.2%	0.3%	0.0%	(X)	(X)	(X)	0.5%
Mechanical engineers 1460 (SOC 17-2141)	Male																
Mechanical engineers 1460 (SOC 17-2141)	Number	219 865	6 530	3 995	176 370	8 255	460	21 715	185	150	460	660	80	(X)	(X)	(X)	1 010
Mechanical engineers 1460 (SOC 17-2141)	Percent	92.6%	2.8%	1.7%	74.3%	3.5%	0.2%	9.1%	0.1%	0.1%	0.2%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Mechanical engineers 1460 (SOC 17-2141)	Female																
Mechanical engineers 1460 (SOC 17-2141)	Number	17 530	525	430	12 960	1 010	35	2 190	0	40	60	85	30	(X)	(X)	(X)	165
Mechanical engineers 1460 (SOC 17-2141)	Percent	7.4%	0.2%	0.2%	5.5%	0.4%	0.0%	0.9%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Petroleum mining and geological engineers including	Total, both sexes																
Petroleum mining and geological engineers including	Number	29 665	1 465	575	23 430	1 470	105	2 105	0	30	215	120	30	(X)	(X)	(X)	125
Petroleum mining and geological engineers including	Percent	100.0%	4.9%	1.9%	79.0%	5.0%	0.4%	7.1%	0.0%	0.1%	0.7%	0.4%	0.1%	(X)	(X)	(X)	0.4%
Petroleum, mining and geological engineers, including	Male																
Petroleum mining and geological engineers including	Number	26 585	1 240	470	21 415	1 305	75	1 620	0	30	205	95	30	(X)	(X)	(X)	105
Petroleum mining and geological engineers including	Percent	89.6%	4.2%	1.6%	72.2%	4.4%	0.3%	5.5%	0.0%	0.1%	0.7%	0.3%	0.1%	(X)	(X)	(X)	0.4%
Petroleum, mining and geological engineers, including	Female																
Petroleum mining and geological engineers including	Number	3 080	225	110	2 015	165	30	480	0	0	10	20	0	(X)	(X)	(X)	20
Petroleum mining and geological engineers including	Percent	10.4%	0.8%	0.4%	6.8%	0.6%	0.1%	1.6%	0.0%	0.0%	0.0%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Miscellaneous engineers including nuclear engineers	Total, both sexes																
Miscellaneous engineers including nuclear engineers	Number	461 335	16 865	7 535	342 685	19 350	1 445	67 330	320	440	1 240	1 925	45	(X)	(X)	(X)	2 155
Miscellaneous engineers including nuclear engineers	Percent	100.0%	3.7%	1.6%	74.3%	4.2%	0.3%	14.6%	0.1%	0.1%	0.3%	0.4%	0.0%	(X)	(X)	(X)	0.5%
Miscellaneous engineers including nuclear engineers	Male																
Miscellaneous engineers including nuclear engineers	Number	405 810	14 295	6 445	307 635	15 280	1 230	55 790	235	400	990	1 595	40	(X)	(X)	(X)	1 880
Miscellaneous engineers including nuclear engineers	Percent	88.0%	3.1%	1.4%	66.7%	3.3%	0.3%	12.1%	0.1%	0.1%	0.2%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Miscellaneous engineers including nuclear engineers	Female																
Miscellaneous engineers including nuclear engineers	Number	55 520	2 570	1 095	35 050	4 070	210	11 540	90	40	250	330	4	(X)	(X)	(X)	275
Miscellaneous engineers including nuclear engineers	Percent	12.0%	0.6%	0.2%	7.6%	0.9%	0.0%	2.5%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Drafters 1540 (SOC 17-3010)	Total, both sexes																
Drafters 1540 (SOC 17-3010)	Number	212 205	12 750	7 610	167 475	8 310	900	12 345	150	155	1 080	700	55	(X)	(X)	(X)	680
Drafters 1540 (SOC 17-3010)	Percent	100.0%	6.0%	3.6%	78.9%	3.9%	0.4%	5.8%	0.1%	0.1%	0.5%	0.3%	0.0%	(X)	(X)	(X)	0.3%
Drafters 1540 (SOC 17-3010)	Male																
Drafters 1540 (SOC 17-3010)	Number	170 365	10 455	6 330	135 000	6 485	675	9 230	115	110	805	520	35	(X)	(X)	(X)	610
Drafters 1540 (SOC 17-3010)	Percent	80.3%	4.9%	3.0%	63.6%	3.1%	0.3%	4.3%	0.1%	0.1%	0.4%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Drafters 1540 (SOC 17-3010)	Female																
Drafters 1540 (SOC 17-3010)	Number	41 840	2 295	1 280	32 480	1 820	225	3 115	35	40	280	180	15	(X)	(X)	(X)	70
Drafters 1540 (SOC 17-3010)	Percent	19.7%	1.1%	0.6%	15.3%	0.9%	0.1%	1.5%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.0%
Engineering technicians except drafters 1550 (SOC 17-	Total, both sexes																
Engineering technicians, except drafters 1550 (SOC 17-	Number	438,830	26,150	17,005	311,520	40,250	2,245	34,100	655	715	2,115	1,405	445	(X)	(X)	(X)	2,220
Engineering technicians except drafters 1550 (SOC 17-	Percent	100.0%	6.0%	3.9%	71.0%	9.2%	0.5%	7.8%	0.1%	0.2%	0.5%	0.3%	0.1%	(X)	(X)	(X)	0.5%
Engineering technicians except drafters 1550 (SOC 17-	Male																
Engineering technicians, except drafters 1550 (SOC 17-	Number	353,240	20,985	13,505	256,230	30,600	1,810	24,175	565	490	1,695	1,160	255	(X)	(X)	(X)	1,775
Engineering technicians except drafters 1550 (SOC 17-	Percent	80.5%	4.8%	3.1%	58.4%	7.0%	0.4%	5.5%	0.1%	0.1%	0.4%	0.3%	0.1%	(X)	(X)	(X)	0.4%
Engineering technicians except drafters 1550 (SOC 17-	Female																
Engineering technicians, except drafters 1550 (SOC 17-	Number	85 590	5 160	3 500	55 290	9 650	440	9 930	85	225	420	250	190	(X)	(X)	(X)	445
Engineering technicians except drafters 1550 (SOC 17-	Percent	19.5%	1.2%	0.8%	12.6%	2.2%	0.1%	2.3%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Surveying and mapping technicians 1560 (SOC 17-3031)	Total, both sexes																
Surveying and mapping technicians 1560 (SOC 17-3031)	Number	87 510	4 855	2 340	73 935	3 055	930	1 060	200	65	535	210	0	(X)	(X)	(X)	325
Surveying and mapping technicians 1560 (SOC 17-3031)	Percent	100.0%	5.5%	2.7%	84.5%	3.5%	1.1%	1.2%	0.2%	0.1%	0.6%	0.2%	0.0%	(X)	(X)	(X)	0.4%
Surveying and mapping technicians 1560 (SOC 17-3031)	Male																
Surveying and mapping technicians 1560 (SOC 17-3031)	Number	79 320	4 325	2 090	67 610	2 535	745	760	195	65	485	210	0	(X)	(X)	(X)	295
Surveying and mapping technicians 1560 (SOC 17-3031)	Percent	90.6%	4.9%	2.4%	77.3%	2.9%	0.9%	0.9%	0.2%	0.1%	0.6%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Surveying and mapping technicians 1560 (SOC 17-3031)	Female																
Surveying and mapping technicians 1560 (SOC 17-3031)	Number	8 190	525	250	6 325	520	185	295	4	0	50	0	0	(X)	(X)	(X)	30
Surveying and mapping technicians 1560 (SOC 17-3031)	Percent	9.4%	0.6%	0.3%	7.2%	0.6%	0.2%	0.3%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Agricultural and food scientists 1600 (SOC 19-1010)	Total, both sexes																
Agricultural and food scientists 1600 (SOC 19-1010)	Number	30 685	930	535	25 670	765	175	2 050	35	25	285	90	4	(X)	(X)	(X)	115
Agricultural and food scientists 1600 (SOC 19-1010)	Percent	100.0%	3.0%	1.7%	83.7%	2.5%	0.6%	6.7%	0.1%	0.1%	0.9%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Agricultural and food scientists 1600 (SOC 19-1010)	Male																
Agricultural and food scientists 1600 (SOC 19-1010)	Number	22 860	735	410	19 265	585	150	1 370	35	20	165	30	0	(X)	(X)	(X)	95
Agricultural and food scientists 1600 (SOC 19-1010)	Percent	74.5%	2.4%	1.3%	62.8%	1.9%	0.5%	4.5%	0.1%	0.1%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Agricultural and food scientists 1600 (SOC 19-1010)	Female																
Agricultural and food scientists 1600 (SOC 19-1010)	Number	7 825	190	125	6 405	180	25	680	4	4	120	60	4	(X)	(X)	(X)	20
Agricultural and food scientists 1600 (SOC 19-1010)	Percent	25.5%	0.6%	0.4%	20.9%	0.6%	0.1%	2.2%	0.0%	0.0%	0.4%	0.2%	0.0%	(X)	(X)	(X)	0.1%
Biological scientists 1610 (SOC 19-1020)	Total, both sexes																
Biological scientists 1610 (SOC 19-1020)	Number	86 130	3 460	1 040	67 530	2 615	305	9 765	80	145	345	445	45	(X)	(X)	(X)	355
Biological scientists 1610 (SOC 19-1020)	Percent	100.0%	4.0%	1.2%	78.4%	3.0%	0.4%	11.3%	0.1%	0.2%	0.4%	0.5%	0.1%	(X)	(X)	(X)	0.4%
Biological scientists 1610 (SOC 19-1020)	Male																
Biological scientists 1610 (SOC 19-1020)	Number	44 630	1 685	635	35 650	1 220	175	4 490	40	65	205	285	0	(X)	(X)	(X)	175
Biological scientists 1610 (SOC 19-1020)	Percent	51.8%	2.0%	0.7%	41.4%	1.4%	0.2%	5.2%	0.0%	0.1%	0.2%	0.3%	0.0%	(X)	(X)	(X)	0.2%
Biological scientists 1610 (SOC 19-1020)	Female																
Biological scientists 1610 (SOC 19-1020)	Number	41 500	1 770	405	31 880	1 395	130	5 270	35	80	145	160	45	(X)	(X)	(X)	180
Biological scientists 1610 (SOC 19-1020)	Percent	48.2%	2.1%	0.5%	37.0%	1.6%	0.2%	6.1%	0.0%	0.1%	0.2%	0.2%	0.1%	(X)	(X)	(X)	0.2%
Conservation scientists and foresters 1640 (SOC 19-	Total, both sexes																
Conservation scientists and foresters 1640 (SOC 19-	Number	25 325	485	125	23 185	510	365	275	4	0	150	55	40	(X)	(X)	(X)	125
Conservation scientists and foresters 1640 (SOC 19-	Percent	100.0%	1.9%	0.5%	91.5%	2.0%	1.4%	1.1%	0.0%	0.0%	0.6%	0.2%	0.2%	(X)	(X)	(X)	0.5%

Conservation scientists and foresters 1640 (SOC 19-	Male																
Conservation scientists and foresters 1640 (SOC 19-	Number	20 485	405	95	18 835	455	355	155	4	0	70	20	0	(X)	(X)	(X)	95
Conservation scientists and foresters 1640 (SOC 19-	Percent	80.9%	1.6%	0.4%	74.4%	1.8%	1.4%	0.6%	0.0%	0.0%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.4%
Conservation scientists and foresters 1640 (SOC 19-	Female																
Conservation scientists and foresters 1640 (SOC 19-	Number	4 840	85	30	4 355	55	10	120	0	0	80	35	40	(X)	(X)	(X)	30
Conservation scientists and foresters 1640 (SOC 19-	Percent	19.1%	0.3%	0.1%	17.2%	0.2%	0.0%	0.5%	0.0%	0.0%	0.3%	0.1%	0.2%	(X)	(X)	(X)	0.1%
Medical scientists and l fe scientists all other 1650 (SOC	Total both sexes																
Medical scientists and l fe scientists all other 1650 (SOC	Number	118 875	3 905	1 400	69 430	4 910	125	37 305	115	50	95	620	35	(X)	(X)	(X)	880
Medical scientists and l fe scientists all other 1650 (SOC	Percent	100.0%	3.3%	1.2%	58.4%	4.1%	0.1%	31.4%	0.1%	0.0%	0.1%	0.5%	0.0%	(X)	(X)	(X)	0.7%
Medical scientists and l fe scientists all other 1650 (SOC	Male																
Medical scientists and l fe scientists all other 1650 (SOC	Number	58 470	1 685	555	33 740	1 860	85	19 745	90	15	25	215	15	(X)	(X)	(X)	435
Medical scientists and l fe scientists all other 1650 (SOC	Percent	49.2%	1.4%	0.5%	28.4%	1.6%	0.1%	16.6%	0.1%	0.0%	0.0%	0.2%	0.0%	(X)	(X)	(X)	0.4%
Medical scientists and l fe scientists all other 1650 (SOC	Female																
Medical scientists and l fe scientists all other 1650 (SOC	Number	60 405	2 220	845	35 690	3 050	40	17 560	30	35	70	405	20	(X)	(X)	(X)	450
Medical scientists and l fe scientists all other 1650 (SOC	Percent	50.8%	1.9%	0.7%	30.0%	2.6%	0.0%	14.8%	0.0%	0.0%	0.1%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Astronomers and physicists 1700 (SOC 19-2010)	Total both sexes																
Astronomers and physicists 1700 (SOC 19-2010)	Number	12 875	485	35	10 525	255	20	1 315	10	0	40	120	0	(X)	(X)	(X)	65
Astronomers and physicists 1700 (SOC 19-2010)	Percent	100.0%	3.8%	0.3%	81.7%	2.0%	0.2%	10.2%	0.1%	0.0%	0.3%	0.9%	0.0%	(X)	(X)	(X)	0.5%
Astronomers and physicists 1700 (SOC 19-2010)	Male																
Astronomers and physicists 1700 (SOC 19-2010)	Number	10 750	420	20	8 925	230	20	955	10	0	40	85	0	(X)	(X)	(X)	40
Astronomers and physicists 1700 (SOC 19-2010)	Percent	83.5%	3.3%	0.2%	69.3%	1.8%	0.2%	7.4%	0.1%	0.0%	0.3%	0.7%	0.0%	(X)	(X)	(X)	0.3%
Astronomers and physicists 1700 (SOC 19-2010)	Female																
Astronomers and physicists 1700 (SOC 19-2010)	Number	2 125	60	15	1 600	25	0	360	0	0	0	35	0	(X)	(X)	(X)	25
Astronomers and physicists 1700 (SOC 19-2010)	Percent	16.5%	0.5%	0.1%	12.4%	0.2%	0.0%	2.8%	0.0%	0.0%	0.0%	0.3%	0.0%	(X)	(X)	(X)	0.2%
Atmospheric and space scientists 1710 (SOC 19-2021)	Total both sexes																
Atmospheric and space scientists 1710 (SOC 19-2021)	Number	9,245	180	100	8,100	365	60	340	0	0	35	0	15	(X)	(X)	(X)	60
Atmospheric and space scientists 1710 (SOC 19-2021)	Percent	100.0%	1.9%	1.1%	87.6%	3.9%	0.6%	3.7%	0.0%	0.0%	0.4%	0.0%	0.2%	(X)	(X)	(X)	0.6%
Atmospheric and space scientists 1710 (SOC 19-2021)	Male																
Atmospheric and space scientists 1710 (SOC 19-2021)	Number	7,470	150	55	6,640	230	55	280	0	0	35	0	15	(X)	(X)	(X)	15
Atmospheric and space scientists 1710 (SOC 19-2021)	Percent	80.8%	1.6%	0.6%	71.8%	2.5%	0.6%	3.0%	0.0%	0.0%	0.4%	0.0%	0.2%	(X)	(X)	(X)	0.2%
Atmospheric and space scientists 1710 (SOC 19-2021)	Female																
Atmospheric and space scientists 1710 (SOC 19-2021)	Number	1 775	30	45	1 460	130	4	60	0	0	0	0	0	(X)	(X)	(X)	45
Atmospheric and space scientists 1710 (SOC 19-2021)	Percent	19.2%	0.3%	0.5%	15.8%	1.4%	0.0%	0.6%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.5%
Chemists and materials scientists 1720 (SOC 19-2030)	Total both sexes																
Chemists and materials scientists 1720 (SOC 19-2030)	Number	92 325	2 490	1 795	63 275	5 880	240	17 395	120	220	160	375	30	(X)	(X)	(X)	350
Chemists and materials scientists 1720 (SOC 19-2030)	Percent	100.0%	2.7%	1.9%	68.5%	6.4%	0.3%	18.8%	0.1%	0.2%	0.2%	0.4%	0.0%	(X)	(X)	(X)	0.4%
Chemists and materials scientists 1720 (SOC 19-2030)	Male																
Chemists and materials scientists 1720 (SOC 19-2030)	Number	57 335	1 310	995	41 410	3 385	100	9 420	80	25	125	235	30	(X)	(X)	(X)	210
Chemists and materials scientists 1720 (SOC 19-2030)	Percent	62.1%	1.4%	1.1%	44.9%	3.7%	0.1%	10.2%	0.1%	0.0%	0.1%	0.3%	0.0%	(X)	(X)	(X)	0.2%
Chemists and materials scientists 1720 (SOC 19-2030)	Female																
Chemists and materials scientists 1720 (SOC 19-2030)	Number	34 990	1 180	795	21 860	2 495	140	7 970	35	195	35	140	0	(X)	(X)	(X)	135
Chemists and materials scientists 1720 (SOC 19-2030)	Percent	37.9%	1.3%	0.9%	23.7%	2.7%	0.2%	8.6%	0.0%	0.2%	0.0%	0.2%	0.0%	(X)	(X)	(X)	0.1%
Environmental scientists and geoscientists 1740 (SOC 19-	Total both sexes																
Environmental scientists and geoscientists 1740 (SOC 19-	Number	79 130	2 355	850	68 410	3 065	445	3 165	85	80	235	230	50	(X)	(X)	(X)	155
Environmental scientists and geoscientists 1740 (SOC 19-	Percent	100.0%	3.0%	1.1%	86.5%	3.9%	0.6%	4.0%	0.1%	0.1%	0.3%	0.3%	0.1%	(X)	(X)	(X)	0.2%
Environmental scientists and geoscientists 1740 (SOC 19-	Male																
Environmental scientists and geoscientists 1740 (SOC 19-	Number	56 990	1 520	560	50 110	1 750	320	2 150	85	50	130	145	35	(X)	(X)	(X)	135
Environmental scientists and geoscientists 1740 (SOC 19-	Percent	72.0%	1.9%	0.7%	63.3%	2.2%	0.4%	2.7%	0.1%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Environmental scientists and geoscientists 1740 (SOC 19-	Female																
Environmental scientists and geoscientists 1740 (SOC 19-	Number	22 140	835	295	18 300	1 315	125	1 010	4	30	105	85	15	(X)	(X)	(X)	20
Environmental scientists and geoscientists 1740 (SOC 19-	Percent	28.0%	1.1%	0.4%	23.1%	1.7%	0.2%	1.3%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.0%
Physical scientists a l other 1760 (SOC 19-2099)	Total both sexes																
Physical scientists a l other 1760 (SOC 19-2099)	Number	170 850	5 300	2 350	112 945	5 685	450	41 255	45	190	360	1 205	30	(X)	(X)	(X)	1 030
Physical scientists, a l other 1760 (SOC 19-2099)	Percent	100.0%	3.1%	1.4%	66.1%	3.3%	0.3%	24.1%	0.0%	0.1%	0.2%	0.7%	0.0%	(X)	(X)	(X)	0.6%
Physical scientists a l other 1760 (SOC 19-2099)	Male																
Physical scientists a l other 1760 (SOC 19-2099)	Number	106 250	3 025	1 410	72 110	2 465	330	25 335	45	65	245	625	15	(X)	(X)	(X)	580
Physical scientists a l other 1760 (SOC 19-2099)	Percent	62.2%	1.8%	0.8%	42.2%	1.4%	0.2%	14.8%	0.0%	0.0%	0.1%	0.4%	0.0%	(X)	(X)	(X)	0.3%
Physical scientists a l other 1760 (SOC 19-2099)	Female																
Physical scientists a l other 1760 (SOC 19-2099)	Number	64 600	2 275	940	40 835	3 220	125	15 920	0	120	115	585	15	(X)	(X)	(X)	450
Physical scientists a l other 1760 (SOC 19-2099)	Percent	37.8%	1.3%	0.6%	23.9%	1.9%	0.1%	9.3%	0.0%	0.1%	0.1%	0.3%	0.0%	(X)	(X)	(X)	0.3%
Economists 1800 (SOC 19-3011)	Total both sexes																
Economists 1800 (SOC 19-3011)	Number	24 635	1 620	540	18 020	1 350	50	2 840	15	0	65	80	4	(X)	(X)	(X)	50
Economists 1800 (SOC 19-3011)	Percent	100.0%	6.6%	2.2%	73.1%	5.5%	0.2%	11.5%	0.1%	0.0%	0.3%	0.3%	0.0%	(X)	(X)	(X)	0.2%
Economists 1800 (SOC 19-3011)	Male																
Economists 1800 (SOC 19-3011)	Number	16 405	1 165	295	12 255	790	30	1 755	4	0	60	10	0	(X)	(X)	(X)	40
Economists 1800 (SOC 19-3011)	Percent	66.6%	4.7%	1.2%	49.7%	3.2%	0.1%	7.1%	0.0%	0.0%	0.2%	0.0%	0.0%	(X)	(X)	(X)	0.2%
Economists 1800 (SOC 19-3011)	Female																
Economists 1800 (SOC 19-3011)	Number	8 230	455	245	5 765	560	20	1 085	10	0	4	70	4	(X)	(X)	(X)	10
Economists 1800 (SOC 19-3011)	Percent	33.4%	1.8%	1.0%	23.4%	2.3%	0.1%	4.4%	0.0%	0.0%	0.0%	0.3%	0.0%	(X)	(X)	(X)	0.0%
Psychologists 1820 (SOC 19-3030)	Total both sexes																
Psychologists 1820 (SOC 19-3030)	Number	182 635	7 330	2 905	156 755	8 715	395	4 555	80	280	645	555	40	(X)	(X)	(X)	385
Psychologists 1820 (SOC 19-3030)	Percent	100.0%	4.0%	1.6%	85.8%	4.8%	0.2%	2.5%	0.0%	0.2%	0.4%	0.3%	0.0%	(X)	(X)	(X)	0.2%
Psychologists 1820 (SOC 19-3030)	Male																
Psychologists 1820 (SOC 19-3030)	Number	59 685	2 305	850	52 150	2 740	75	1 155	45	35	145	125	15	(X)	(X)	(X)	45
Psychologists 1820 (SOC 19-3030)	Percent	32.7%	1.3%	0.5%	28.6%	1.5%	0.0%	0.6%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.0%
Psychologists 1820 (SOC 19-3030)	Female																
Psychologists 1820 (SOC 19-3030)	Number	122 950	5 025	2 055	104 605	5 975	320	3 400	35	245	500	430	25	(X)	(X)	(X)	340
Psychologists 1820 (SOC 19-3030)	Percent	67.3%	2.8%	1.1%	57.3%	3.3%	0.2%	1.9%	0.0%	0.1%	0.3%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Urban and regional planners 1840 (SOC 19-3051)	Total, both sexes																
Urban and regional planners 1840 (SOC 19-3051)	Number	24 165	915	425	19 460	1 640	105	1 195	0	85	130	75	15	(X)	(X)	(X)	125
Urban and regional planners 1840 (SOC 19-3051)	Percent	100.0%	3.8%	1.8%	80.5%	6.8%	0.4%	4.9%	0.0%	0.4%	0.5%	0.3%	0.1%	(X)	(X)	(X)	0.5%
Urban and regional planners 1840 (SOC 19-3051)	Male																
Urban and regional planners 1840 (SOC 19-3051)	Number	14 340	570	220	11 905	845	40	610	0	45	55	20	15	(X)	(X)	(X)	15
Urban and regional planners 1840 (SOC 19-3051)	Percent	59.3%	2.4%	0.9%	49.3%	3.5%	0.2%	2.5%	0.0%	0.2%	0.2%	0.1%	0.1%	(X)	(X)	(X)	0.1%
Urban and regional planners 1840 (SOC 19-3051)	Female																
Urban and regional planners 1840 (SOC 19-3051)	Number	9 825	340	205	7 555	795	65	580	0	35	75	50	0	(X)	(X)	(X)	110
Urban and regional planners 1840 (SOC 19-3051)	Percent	40.7%	1.4%	0.8%	31.3%	3.3%	0.3%	2.4%	0.0%	0.1%	0.3%	0.2%	0.0%	(X)	(X)	(X)	0.5%
Miscellaneous social scientists including survey	Total both sexes																
Miscellaneous social scientists including survey	Number	49 085	2 335	870	38 060	4 235	235	2 395	30	140	300	195	15	(X)	(X)	(X)	275
Miscellaneous social scientists including survey	Percent	100.0%	4.8%	1.8%	77.5%	8.6%	0.5%	4.9%	0.1%	0.3%	0.6%	0.4%	0.0%	(X)	(X)	(X)	0.6%
Miscellaneous social scientists including survey	Male																
Miscellaneous social scientists including survey	Number	23 640	1 095	325	18 610	2 080	115	990	20	80	85	85	0	(X)	(X)	(X)	150
Miscellaneous social scientists including survey	Percent	48.2%	2.2%	0.7%	37.9%	4.2%	0.2%	2.0%	0.0%	0.2%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Miscellaneous social scientists including survey	Female																
Miscellaneous social scientists including survey	Number	25 445	1 240	545	19 445	2 155	120	1 405	10	60	220	110	15	(X)	(X)	(X)	125
Miscellaneous social scientists including survey	Percent	51.8%	2.5%	1.1%	39.6%	4.4%	0.2%	2.9%	0.0%	0.1%	0.4%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Agricultural and food science technicians 1900 (SOC 19-	Total both sexes																
Agricultural and food science technicians 1900 (SOC 19-	Number	31 295	2 560	1 695	22 360	2 240	230	1 720	115	15	45	110	0	(X)	(X)	(X)	205
Agricultural and food science technicians 1900 (SOC 19-	Percent	100.0%	8.2%	5.4%	71.4%	7.2%	0.7%	5.5%	0.4%	0.0%	0.1%	0.4%	0.0%	(X)	(X)	(X)	0.7%
Agricultural and food science technicians 1900 (SOC 19-	Male																
Agricultural and food science technicians 1900 (SOC 19-	Number	18,250	1,415	1,095	13,015	1,160	60	1,245	60	0	20	60	0	(X)	(X)	(X)	125
Agricultural and food science technicians 1900 (SOC 19-	Percent	58.3%	4.5%	3.5%	41.6%	3.7%	0.2%	4.0%	0.2%	0.0%	0.1%	0.2%	0.0%	(X)	(X)	(X)	0.4%
Agricultural and food science technicians 1900 (SOC 19-	Female																
Agricultural and food science technicians 1900 (SOC 19-	Number	13,045	1,145	600	9,350	1,080	175	475	50	15	25	50	0	(X)	(X)	(X)	80
Agricultural and food science technicians 1900 (SOC 19-	Percent	41.7%	3.7%	1.9%	29.9%	3.5%	0.6%	1.5%	0.2%	0.0%	0.1%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Biological technicians 1910 (SOC 19-4021)	Total both sexes																
Biological technicians 1910 (SOC 19-4021)	Number	24 170	1 610	790	15 780	1 635	260	3 470	25	25	235	125	35	(X)	(X)	(X)	165
Biological technicians 1910 (SOC 19-4021)	Percent	100.0%	6.7%	3.3%	65.3%	6.8%	1.1%	14.4%	0.1%	0.1%	1.0%	0.5%	0.1%	(X)	(X)	(X)	0.7%
Biological technicians 1910 (SOC 19-4021)	Male																
Biological technicians 1910 (SOC 19-4021)	Number	12 625	570	285	8 520	975	205	1 775	25	4	155	10	0	(X)	(X)	(X)	105
Biological technicians 1910 (SOC 19-4021)	Percent	52.2%	2.4%	1.2%	35.3%	4.0%	0.8%	7.3%	0.1%	0.0%	0.6%	0.0%	0.0%	(X)	(X)	(X)	0.4%
Biological technicians 1910 (SOC 19-4021)	Female																
Biological technicians 1910 (SOC 19-4021)	Number	11 545	1 045	510	7 260	660	55	1 700	4	20	80	115	35	(X)	(X)	(X)	60
Biological technicians 1910 (SOC 19-4021)	Percent	47.8%	4.3%	2.1%	30.0%	2.7%	0.2%	7.0%	0.0%	0.1%	0.3%	0.5%	0.1%	(X)	(X)	(X)	0.2%
Chemical technicians 1920 (SOC 19-4031)	Total both sexes																
Chemical technicians 1920 (SOC 19-4031)	Number	76 095	4 440	2 750	52 975	8 745	400	5 710	65	150	190	270	45	(X)	(X)	(X)	355
Chemical technicians 1920 (SOC 19-4031)	Percent	100.0%	5.8%	3.6%	69.6%	11.5%	0.5%	7.5%	0.1%	0.2%	0.2%	0.4%	0.1%	(X)	(X)	(X)	0.5%
Chemical technicians 1920 (SOC 19-4031)	Male																
Chemical technicians 1920 (SOC 19-4031)	Number	48 875	2 945	1 870	35 205	4 915	205	3 090	35	80	165	185	30	(X)	(X)	(X)	160
Chemical technicians 1920 (SOC 19-4031)	Percent	64.2%	3.9%	2.5%	46.3%	6.5%	0.3%	4.1%	0.0%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Chemical technicians 1920 (SOC 19-4031)	Female																
Chemical technicians 1920 (SOC 19-4031)	Number	27 220	1 500	880	17 775	3 830	195	2 620	35	70	25	85	15	(X)	(X)	(X)	195
Chemical technicians 1920 (SOC 19-4031)	Percent	35.8%	2.0%	1.2%	23.4%	5.0%	0.3%	3.4%	0.0%	0.1%	0.0%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Geological and petroleum technicians and nuclear	Total both sexes																
Geological and petroleum technicians and nuclear	Number	19 935	1 165	755	15 845	1 175	155	635	15	35	110	30	0	(X)	(X)	(X)	10
Geological and petroleum technicians, and nuclear	Percent	100.0%	5.8%	3.8%	79.5%	5.9%	0.8%	3.2%	0.1%	0.2%	0.6%	0.2%	0.0%	(X)	(X)	(X)	0.1%
Geological and petroleum technicians and nuclear	Male																
Geological and petroleum technicians and nuclear	Number	14 775	895	585	11 765	850	105	405	10	35	95	30	0	(X)	(X)	(X)	0
Geological and petroleum technicians, and nuclear	Percent	74.1%	4.5%	2.9%	59.0%	4.3%	0.5%	2.0%	0.1%	0.2%	0.5%	0.2%	0.0%	(X)	(X)	(X)	0.0%
Geological and petroleum technicians and nuclear	Female																
Geological and petroleum technicians and nuclear	Number	5 160	270	170	4 085	325	50	230	4	0	15	0	0	(X)	(X)	(X)	10
Geological and petroleum technicians and nuclear	Percent	25.9%	1.4%	0.9%	20.5%	1.6%	0.3%	1.2%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Miscellaneous ife physical and social science	Total both sexes																
Miscellaneous ife physical and social science	Number	179 335	9 400	6 155	123 825	14 520	1 650	19 660	320	400	790	1 325	165	(X)	(X)	(X)	1 120
Miscellaneous ife physical and social science	Percent	100.0%	5.2%	3.4%	69.0%	8.1%	0.9%	11.0%	0.2%	0.2%	0.4%	0.7%	0.1%	(X)	(X)	(X)	0.6%
Miscellaneous ife physical and social science	Male																
Miscellaneous ife physical and social science	Number	93 950	4 870	3 435	66 485	6 420	1 085	9 555	155	180	465	690	50	(X)	(X)	(X)	565
Miscellaneous ife physical and social science	Percent	52.4%	2.7%	1.9%	37.1%	3.6%	0.6%	5.3%	0.1%	0.1%	0.3%	0.4%	0.0%	(X)	(X)	(X)	0.3%

Miscellaneous ife, physical, and social science	Female																
Miscellaneous ife physical and social science	Number	85 380	4 530	2 720	57 345	8 100	560	10 110	165	220	325	635	115	(X)	(X)	(X)	555
Miscellaneous ife physical and social science	Percent	47.6%	2.5%	1.5%	32.0%	4.5%	0.3%	5.6%	0.1%	0.1%	0.2%	0.4%	0.1%	(X)	(X)	(X)	0.3%
Counselors 2000 (SOC 21-1010)	Total, both sexes																
Counselors 2000 (SOC 21-1010)	Number	689 195	37 365	27 350	447 890	139 145	6 130	17 400	1 310	2 310	3 090	2 175	990	(X)	(X)	(X)	4 035
Counselors 2000 (SOC 21-1010)	Percent	100.0%	5.4%	4.0%	65.0%	20.2%	0.9%	2.5%	0.2%	0.3%	0.4%	0.3%	0.1%	(X)	(X)	(X)	0.6%
Counselors 2000 (SOC 21-1010)	Male																
Counselors 2000 (SOC 21-1010)	Number	213 765	10 900	9 625	128 865	51 410	2 315	6 150	595	760	835	700	455	(X)	(X)	(X)	1 150
Counselors 2000 (SOC 21-1010)	Percent	31.0%	1.6%	1.4%	18.7%	7.5%	0.3%	0.9%	0.1%	0.1%	0.1%	0.1%	0.1%	(X)	(X)	(X)	0.2%
Counselors 2000 (SOC 21-1010)	Female																
Counselors 2000 (SOC 21-1010)	Number	475 430	26 465	17 720	319 025	87 735	3 820	11 250	715	1 550	2 255	1 480	540	(X)	(X)	(X)	2 885
Counselors 2000 (SOC 21-1010)	Percent	69.0%	3.8%	2.6%	46.3%	12.7%	0.6%	1.6%	0.1%	0.2%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Social workers 2010 (SOC 21-1020)	Total, both sexes																
Social workers 2010 (SOC 21-1020)	Number	779 175	49 480	36 170	482 675	170 860	5 675	20 660	885	2 230	3 200	1 785	1 470	(X)	(X)	(X)	4 090
Social workers 2010 (SOC 21-1020)	Percent	100.0%	6.4%	4.6%	61.9%	21.9%	0.7%	2.7%	0.1%	0.3%	0.4%	0.2%	0.2%	(X)	(X)	(X)	0.5%
Social workers 2010 (SOC 21-1020)	Male																
Social workers 2010 (SOC 21-1020)	Number	159 540	10 355	7 770	93 770	38 340	845	5 895	240	285	540	300	230	(X)	(X)	(X)	980
Social workers 2010 (SOC 21-1020)	Percent	20.5%	1.3%	1.0%	12.0%	4.9%	0.1%	0.8%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Social workers 2010 (SOC 21-1020)	Female																
Social workers 2010 (SOC 21-1020)	Number	619 640	39 130	28 400	388 905	132 520	4 830	14 765	645	1 945	2 660	1 485	1 240	(X)	(X)	(X)	3 110
Social workers 2010 (SOC 21-1020)	Percent	79.5%	5.0%	3.6%	49.9%	17.0%	0.6%	1.9%	0.1%	0.2%	0.3%	0.2%	0.2%	(X)	(X)	(X)	0.4%
Probation officers and correctional treatment specialists	Total, both sexes																
Probation officers and correctional treatment specialists	Number	98 525	7 775	4 720	58 355	23 015	850	1 620	270	410	330	360	375	(X)	(X)	(X)	455
Probation officers and correctional treatment specialists	Percent	100.0%	7.9%	4.8%	59.2%	23.4%	0.9%	1.6%	0.3%	0.4%	0.3%	0.4%	0.4%	(X)	(X)	(X)	0.5%
Probation officers and correctional treatment specialists	Male																
Probation officers and correctional treatment specialists	Number	48,070	3,865	2,185	29,180	10,360	400	1,045	205	150	110	255	135	(X)	(X)	(X)	190
Probation officers and correctional treatment specialists	Percent	48.8%	3.9%	2.2%	29.6%	10.5%	0.4%	1.1%	0.2%	0.2%	0.1%	0.3%	0.1%	(X)	(X)	(X)	0.2%
Probation officers and correctional treatment specialists	Female																
Probation officers and correctional treatment specialists	Number	50,455	3,915	2,540	29,175	12,655	450	575	65	260	220	105	245	(X)	(X)	(X)	260
Probation officers and correctional treatment specialists	Percent	51.2%	4.0%	2.6%	29.6%	12.8%	0.5%	0.6%	0.1%	0.3%	0.2%	0.1%	0.2%	(X)	(X)	(X)	0.3%
Social and human service assistants 2016 (SOC 21-1093)	Total, both sexes																
Social and human service assistants 2016 (SOC 21-1093)	Number	153 535	12 555	10 385	83 860	37 565	1 960	4 475	295	470	560	320	340	(X)	(X)	(X)	745
Social and human service assistants 2016 (SOC 21-1093)	Percent	100.0%	8.2%	6.8%	54.6%	24.5%	1.3%	2.9%	0.2%	0.3%	0.4%	0.2%	0.2%	(X)	(X)	(X)	0.5%
Social and human service assistants 2016 (SOC 21-1093)	Male																
Social and human service assistants 2016 (SOC 21-1093)	Number	34 600	2 335	2 560	17 160	9 975	320	1 470	125	75	130	95	105	(X)	(X)	(X)	245
Social and human service assistants 2016 (SOC 21-1093)	Percent	22.5%	1.5%	1.7%	11.2%	6.5%	0.2%	1.0%	0.1%	0.0%	0.1%	0.1%	0.1%	(X)	(X)	(X)	0.2%
Social and human service assistants 2016 (SOC 21-1093)	Female																
Social and human service assistants 2016 (SOC 21-1093)	Number	118 935	10 220	7 825	66 700	27 590	1 640	3 005	165	395	430	225	235	(X)	(X)	(X)	500
Social and human service assistants 2016 (SOC 21-1093)	Percent	77.5%	6.7%	5.1%	43.4%	18.0%	1.1%	2.0%	0.1%	0.3%	0.3%	0.1%	0.2%	(X)	(X)	(X)	0.3%
Miscellaneous community and social service specialists	Total, both sexes																
Miscellaneous community and social service specialists	Number	82 475	5 795	4 655	50 760	15 840	1 235	2 410	145	390	390	280	80	(X)	(X)	(X)	495
Miscellaneous community and social service specialists	Percent	100.0%	7.0%	5.6%	61.5%	19.2%	1.5%	2.9%	0.2%	0.5%	0.5%	0.3%	0.1%	(X)	(X)	(X)	0.6%
Miscellaneous community and social service specialists	Male																
Miscellaneous community and social service specialists	Number	27 345	2 000	1 585	17 000	5 100	330	800	70	225	50	80	0	(X)	(X)	(X)	95
Miscellaneous community and social service specialists	Percent	33.2%	2.4%	1.9%	20.6%	6.2%	0.4%	1.0%	0.1%	0.3%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Miscellaneous community and social service specialists	Female																
Miscellaneous community and social service specialists	Number	55 130	3 795	3 070	33 755	10 740	900	1 610	75	160	340	200	80	(X)	(X)	(X)	400
Miscellaneous community and social service specialists	Percent	66.8%	4.6%	3.7%	40.9%	13.0%	1.1%	2.0%	0.1%	0.2%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.5%
Clergy 2040 (SOC 21-2011)	Total, both sexes																
Clergy 2040 (SOC 21-2011)	Number	444 045	15 140	9 460	350 490	42 810	1 710	19 260	515	330	1 845	635	380	(X)	(X)	(X)	1 465
Clergy 2040 (SOC 21-2011)	Percent	100.0%	3.4%	2.1%	78.9%	9.6%	0.4%	4.3%	0.1%	0.1%	0.4%	0.1%	0.1%	(X)	(X)	(X)	0.3%
Clergy 2040 (SOC 21-2011)	Male																
Clergy 2040 (SOC 21-2011)	Number	365 825	12 965	7 975	287 700	35 015	1 335	16 615	460	200	1 555	560	245	(X)	(X)	(X)	1 190
Clergy 2040 (SOC 21-2011)	Percent	82.4%	2.9%	1.8%	64.8%	7.9%	0.3%	3.7%	0.1%	0.0%	0.4%	0.1%	0.1%	(X)	(X)	(X)	0.3%
Clergy 2040 (SOC 21-2011)	Female																
Clergy 2040 (SOC 21-2011)	Number	78 220	2 175	1 485	62 785	7 795	375	2 645	55	130	285	75	135	(X)	(X)	(X)	275
Clergy 2040 (SOC 21-2011)	Percent	17.6%	0.5%	0.3%	14.1%	1.8%	0.1%	0.6%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Directors religious activities and education 2050 (SOC 21-	Total, both sexes																
Directors religious activities and education 2050 (SOC 21-	Number	53 625	2 060	1 005	44 265	3 830	135	1 665	95	55	250	150	40	(X)	(X)	(X)	75
Directors religious activities and education 2050 (SOC 21-	Percent	100.0%	3.8%	1.9%	82.5%	7.1%	0.3%	3.1%	0.2%	0.1%	0.5%	0.3%	0.1%	(X)	(X)	(X)	0.1%
Directors religious activities and education 2050 (SOC 21-	Male																
Directors religious activities and education 2050 (SOC 21-	Number	20 600	740	490	16 295	1 875	35	985	85	0	45	35	0	(X)	(X)	(X)	15
Directors religious activities and education 2050 (SOC 21-	Percent	38.4%	1.4%	0.9%	30.4%	3.5%	0.1%	1.8%	0.2%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.0%
Directors religious activities and education 2050 (SOC 21-	Female																
Directors religious activities and education 2050 (SOC 21-	Number	33 030	1 325	515	27 970	1 960	100	680	10	55	205	115	40	(X)	(X)	(X)	60
Directors religious activities and education 2050 (SOC 21-	Percent	61.6%	2.5%	1.0%	52.2%	3.7%	0.2%	1.3%	0.0%	0.1%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.1%
Religious workers al other 2060 (SOC 21-2099)	Total, both sexes																
Religious workers al other 2060 (SOC 21-2099)	Number	90 285	4 280	2 025	71 380	6 945	270	4 110	95	125	375	145	60	(X)	(X)	(X)	475
Religious workers al other 2060 (SOC 21-2099)	Percent	100.0%	4.7%	2.2%	79.1%	7.7%	0.3%	4.6%	0.1%	0.1%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.5%
Religious workers al other 2060 (SOC 21-2099)	Male																
Religious workers al other 2060 (SOC 21-2099)	Number	35 100	1 495	955	27 550	2 350	175	1 945	35	100	170	70	15	(X)	(X)	(X)	240
Religious workers al other 2060 (SOC 21-2099)	Percent	38.9%	1.7%	1.1%	30.5%	2.6%	0.2%	2.2%	0.0%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Religious workers al other 2060 (SOC 21-2099)	Female																
Religious workers al other 2060 (SOC 21-2099)	Number	55 185	2 780	1 070	43 830	4 595	100	2 165	60	25	205	75	45	(X)	(X)	(X)	235
Religious workers al other 2060 (SOC 21-2099)	Percent	61.1%	3.1%	1.2%	48.5%	5.1%	0.1%	2.4%	0.1%	0.0%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Lawyers, and judges, magistrates, and other judicial	Total, both sexes																
Lawyers and judges magistrates and other judicial	Number	1 038 895	35 015	12 465	890 815	48 185	2 640	36 945	315	1 380	2 975	3 785	485	(X)	(X)	(X)	3 895
Lawyers and judges magistrates and other judicial	Percent	100.0%	3.4%	1.2%	85.7%	4.6%	0.3%	3.6%	0.0%	0.1%	0.3%	0.4%	0.0%	(X)	(X)	(X)	0.4%
Lawyers, and judges, magistrates, and other judicial	Male																
Lawyers and judges magistrates and other judicial	Number	691 600	20 620	6 865	615 100	21 790	1 315	19 105	200	500	1 875	1 890	175	(X)	(X)	(X)	2 160
Lawyers and judges magistrates and other judicial	Percent	66.6%	2.0%	0.7%	59.2%	2.1%	0.1%	1.8%	0.0%	0.0%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Lawyers and judges magistrates and other judicial	Female																
Lawyers and judges magistrates and other judicial	Number	347 300	14 395	5 600	275 715	26 395	1 325	17 840	120	880	1 100	1 895	305	(X)	(X)	(X)	1 735
Lawyers and judges magistrates and other judicial	Percent	33.4%	1.4%	0.5%	26.5%	2.5%	0.1%	1.7%	0.0%	0.1%	0.1%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Judicial law clerks 2105 (SOC 23-1012)	Total, both sexes																
Judicial law clerks 2105 (SOC 23-1012)	Number	11 830	630	170	9 660	615	55	575	0	35	15	70	0	(X)	(X)	(X)	10
Judicial law clerks 2105 (SOC 23-1012)	Percent	100.0%	5.3%	1.4%	81.7%	5.2%	0.5%	4.9%	0.0%	0.3%	0.1%	0.6%	0.0%	(X)	(X)	(X)	0.1%
Judicial law clerks 2105 (SOC 23-1012)	Male																
Judicial law clerks 2105 (SOC 23-1012)	Number	5 330	130	80	4 610	270	10	195	0	0	0	30	0	(X)	(X)	(X)	0
Judicial law clerks 2105 (SOC 23-1012)	Percent	45.1%	1.1%	0.7%	39.0%	2.3%	0.1%	1.6%	0.0%	0.0%	0.0%	0.3%	0.0%	(X)	(X)	(X)	0.0%
Judicial law clerks 2105 (SOC 23-1012)	Female																
Judicial law clerks 2105 (SOC 23-1012)	Number	6 500	500	90	5 045	345	45	380	0	35	15	40	0	(X)	(X)	(X)	10
Judicial law clerks 2105 (SOC 23-1012)	Percent	54.9%	4.2%	0.8%	42.6%	2.9%	0.4%	3.2%	0.0%	0.3%	0.1%	0.3%	0.0%	(X)	(X)	(X)	0.1%
Paralegals and legal assistants 2145 (SOC 23-2011)	Total, both sexes																
Paralegals and legal assistants 2145 (SOC 23-2011)	Number	395 210	28 900	15 410	291 570	36 795	1 510	14 245	495	840	1 325	1 485	290	(X)	(X)	(X)	2 345
Paralegals and legal assistants 2145 (SOC 23-2011)	Percent	100.0%	7.3%	3.9%	73.8%	9.3%	0.4%	3.6%	0.1%	0.2%	0.3%	0.4%	0.1%	(X)	(X)	(X)	0.6%
Paralegals and legal assistants 2145 (SOC 23-2011)	Male																
Paralegals and legal assistants 2145 (SOC 23-2011)	Number	64 615	5 330	2 395	43 895	7 555	265	3 895	100	120	200	420	40	(X)	(X)	(X)	405
Paralegals and legal assistants 2145 (SOC 23-2011)	Percent	16.3%	1.3%	0.6%	11.1%	1.9%	0.1%	1.0%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Paralegals and legal assistants 2145 (SOC 23-2011)	Female																
Paralegals and legal assistants 2145 (SOC 23-2011)	Number	330,595	23,570	13,020	247,675	29,240	1,240	10,350	395	720	1,125	1,065	250	(X)	(X)	(X)	1,945
Paralegals and legal assistants 2145 (SOC 23-2011)	Percent	83.7%	6.0%	3.3%	62.7%	7.4%	0.3%	2.6%	0.1%	0.2%	0.3%	0.3%	0.1%	(X)	(X)	(X)	0.5%
Miscellaneous legal support workers 2160 (SOC 23-2090)	Total, both sexes																
Miscellaneous legal support workers 2160 (SOC 23-2090)	Number	245,905	14,780	9,890	181,140	24,435	1,840	9,850	260	560	1,025	810	200	(X)	(X)	(X)	1,120
Miscellaneous legal support workers 2160 (SOC 23-2090)	Percent	100.0%	6.0%	4.0%	73.7%	9.9%	0.7%	4.0%	0.1%	0.2%	0.4%	0.3%	0.1%	(X)	(X)	(X)	0.5%
Miscellaneous legal support workers 2160 (SOC 23-2090)	Male																
Miscellaneous legal support workers 2160 (SOC 23-2090)	Number	64 580	3 545	2 015	46 750	6 380	450	4 325	30	205	290	355	40	(X)	(X)	(X)	205
Miscellaneous legal support workers 2160 (SOC 23-2090)	Percent	26.3%	1.4%	0.8%	19.0%	2.6%	0.2%	1.8%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Miscellaneous legal support workers 2160 (SOC 23-2090)	Female																
Miscellaneous legal support workers 2160 (SOC 23-2090)	Number	181 325	11 235	7 875	134 390	18 050	1 390	5 520	230	355	740	455	160	(X)	(X)	(X)	915
Miscellaneous legal support workers 2160 (SOC 23-2090)	Percent	73.7%	4.6%	3.2%	54.7%	7.3%	0.6%	2.2%	0.1%	0.1%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Postsecondary teachers 2200 (SOC 25-1000)	Total, both sexes																
Postsecondary teachers 2200 (SOC 25-1000)	Number	1 351 005	51 185	22 105	1 010 055	82 185	3 780	158 150	765	2 330	4 600	6 070	1 145	(X)	(X)	(X)	8 640
Postsecondary teachers 2200 (SOC 25-1000)	Percent	100.0%	3.8%	1.6%	74.8%	6.1%	0.3%	11.7%	0.1%	0.2%	0.3%	0.4%	0.1%	(X)	(X)	(X)	0.6%
Postsecondary teachers 2200 (SOC 25-1000)	Male																
Postsecondary teachers 2200 (SOC 25-1000)	Number	702 405	24 295	11 265	523 505	36 615	1 605	92 695	270	1 205	2 145	3 295	455	(X)	(X)	(X)	5 050
Postsecondary teachers 2200 (SOC 25-1000)	Percent	52.0%	1.8%	0.8%	38.7%	2.7%	0.1%	6.9%	0.0%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.4%
Postsecondary teachers 2200 (SOC 25-1000)	Female																
Postsecondary teachers 2200 (SOC 25-1000)	Number	648 605	26 885	10 835	486 555	45 570	2 175	65 455	495	1 125	2 455	2 775	690	(X)	(X)	(X)	3 590
Postsecondary teachers 2200 (SOC 25-1000)	Percent	48.0%	2.0%	0.8%	36.0%	3.4%	0.2%	4.8%	0.0%	0.1%	0.2%	0.2%	0.1%	(X)	(X)	(X)	0.3%
Preschool and kindergarten teachers 2300 (SOC 25-2010)	Total, both sexes																
Preschool and kindergarten teachers 2300 (SOC 25-2010)	Number	591 935	43 375	26 920	396 465	95 150	4 550	17 010	755	1 455	1 995	1 130	495	(X)	(X)	(X)	2 640
Preschool and kindergarten teachers 2300 (SOC 25-2010)	Percent	100.0%	7.3%	4.5%	67.0%	16.1%	0.8%	2.9%	0.1%	0.2%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Preschool and kindergarten teachers 2300 (SOC 25-2010)	Male																
Preschool and kindergarten teachers 2300 (SOC 25-2010)	Number	15 180	1 205	1 140	8 655	3 205	180	460	45	0	25	75	40	(X)	(X)	(X)	150
Preschool and kindergarten teachers 2300 (SOC 25-2010)	Percent	2.6%	0.2%	0.2%	1.5%	0.5%	0.0%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Preschool and kindergarten teachers 2300 (SOC 25-2010)	Female																
Preschool and kindergarten teachers 2300 (SOC 25-2010)	Number	576 760	42 170	25 780	387 810	91 940	4 365	16 550	710	1 455	1 975	1 050	455	(X)	(X)	(X)	2 490
Preschool and kindergarten teachers 2300 (SOC 25-2010)	Percent	97.4%	7.1%	4.4%	65.5%	15.5%	0.7%	2.8%	0.1%	0.2%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Elementary and middle school teachers 2310 (SOC 25-	Total, both sexes																
Elementary and middle school teachers 2310 (SOC 25-	Number	3 452 545	172 335	83 110	2 766 040	303 080	13 385	73 825	2 145	4 290	11 100	7 910	2 710	(X)	(X)	(X)	12 615
Elementary and middle school teachers 2310 (SOC 25-	Percent	100.0%	5.0%	2.4%	80.1%	8.8%	0.4%	2.1%	0.1%	0.1%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Elementary and middle school teachers 2310 (SOC 25-	Male																
Elementary and middle school teachers 2310 (SOC 25-	Number	714 765	38 080	18 330	568 780	63 150	3 040	14 150	365	985	2 540	1 855	555	(X)	(X)	(X)	2 925
Elementary and middle school teachers 2310 (SOC 25-	Percent	20.7%	1.1%	0.5%	16.5%	1.8%	0.1%	0.4%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Elementary and middle school teachers 2310 (SOC 25-	Female																
Elementary and middle school teachers 2310 (SOC 25-	Number	2 737 785	134 255	64 775	2 197 265	239 930	10 345	59 675	1 780	3 305	8 555	6 055	2 155	(X)	(X)	(X)	9 690
Elementary and middle school teachers 2310 (SOC 25-	Percent	79.3%	3.9%	1.9%	63.6%	6.9%	0.3%	1.7%	0.1%	0.1%	0.2%	0.2%	0.1%	(X)	(X)	(X)	0.3%

Secondary school teachers 2320 (SOC 25-2030)	Total, both sexes																
Secondary school teachers 2320 (SOC 25-2030)	Number	812 130	40 880	21 350	649 520	67 415	3 430	18 340	770	1 340	3 195	2 075	540	(X)	(X)	(X)	3 285
Secondary school teachers 2320 (SOC 25-2030)	Percent	100.0%	5.0%	2.6%	80.0%	8.3%	0.4%	2.3%	0.1%	0.2%	0.4%	0.3%	0.1%	(X)	(X)	(X)	0.4%
Secondary school teachers 2320 (SOC 25-2030)	Male																
Secondary school teachers 2320 (SOC 25-2030)	Number	335 740	16 205	8 560	269 285	28 750	1 325	7 005	465	555	1 240	740	230	(X)	(X)	(X)	1 385
Secondary school teachers 2320 (SOC 25-2030)	Percent	41.3%	2.0%	1.1%	33.2%	3.5%	0.2%	0.9%	0.1%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Secondary school teachers 2320 (SOC 25-2030)	Female																
Secondary school teachers 2320 (SOC 25-2030)	Number	476 390	24 675	12 790	380 240	38 665	2 100	11 330	305	780	1 955	1 335	310	(X)	(X)	(X)	1 900
Secondary school teachers 2320 (SOC 25-2030)	Percent	58.7%	3.0%	1.6%	46.8%	4.8%	0.3%	1.4%	0.0%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Special education teachers 2330 (SOC 25-2050)	Total, both sexes																
Special education teachers 2330 (SOC 25-2050)	Number	227 105	10 460	5 780	179 100	22 455	1 290	4 670	240	480	1 180	385	150	(X)	(X)	(X)	910
Special education teachers 2330 (SOC 25-2050)	Percent	100.0%	4.6%	2.5%	78.9%	9.9%	0.6%	2.1%	0.1%	0.2%	0.5%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Special education teachers 2330 (SOC 25-2050)	Male																
Special education teachers 2330 (SOC 25-2050)	Number	32 555	1 810	1 165	23 950	4 205	130	725	60	170	85	35	0	(X)	(X)	(X)	215
Special education teachers 2330 (SOC 25-2050)	Percent	14.3%	0.8%	0.5%	10.5%	1.9%	0.1%	0.3%	0.0%	0.1%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Special education teachers 2330 (SOC 25-2050)	Female																
Special education teachers 2330 (SOC 25-2050)	Number	194 550	8 650	4 615	155 145	18 250	1 160	3 945	185	310	1 095	350	150	(X)	(X)	(X)	695
Special education teachers 2330 (SOC 25-2050)	Percent	85.7%	3.8%	2.0%	68.3%	8.0%	0.5%	1.7%	0.1%	0.1%	0.5%	0.2%	0.1%	(X)	(X)	(X)	0.3%
Other teachers and instructors 2340 (SOC 25-3000)	Total, both sexes																
Other teachers and instructors 2340 (SOC 25-3000)	Number	854 840	47 505	29 550	614 170	91 915	4 895	48 910	1 445	2 710	4 100	3 650	890	(X)	(X)	(X)	5 095
Other teachers and instructors 2340 (SOC 25-3000)	Percent	100.0%	5.6%	3.5%	71.8%	10.8%	0.6%	5.7%	0.2%	0.3%	0.5%	0.4%	0.1%	(X)	(X)	(X)	0.6%
Other teachers and instructors 2340 (SOC 25-3000)	Male																
Other teachers and instructors 2340 (SOC 25-3000)	Number	317 900	19 310	10 835	226 180	34 095	1 580	18 990	620	810	1 600	1 550	275	(X)	(X)	(X)	2 045
Other teachers and instructors 2340 (SOC 25-3000)	Percent	37.2%	2.3%	1.3%	26.5%	4.0%	0.2%	2.2%	0.1%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Other teachers and instructors 2340 (SOC 25-3000)	Female																
Other teachers and instructors 2340 (SOC 25-3000)	Number	536,940	28,190	18,710	387,990	57,815	3,315	29,920	825	1,900	2,500	2,100	615	(X)	(X)	(X)	3,055
Other teachers and instructors 2340 (SOC 25-3000)	Percent	62.8%	3.3%	2.2%	45.4%	6.8%	0.4%	3.5%	0.1%	0.2%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Archivists curators and museum technicians 2400 (SOC	Total both sexes																
Archivists, curators, and museum technicians 2400 (SOC	Number	44,480	1,070	730	37,805	2,505	245	1,440	0	115	185	95	10	(X)	(X)	(X)	285
Archivists curators and museum technicians 2400 (SOC	Percent	100.0%	2.4%	1.6%	85.0%	5.6%	0.6%	3.2%	0.0%	0.3%	0.4%	0.2%	0.0%	(X)	(X)	(X)	0.6%
Archivists curators and museum technicians 2400 (SOC	Male																
Archivists curators and museum technicians 2400 (SOC	Number	17 825	380	280	15 365	955	100	495	0	75	20	50	10	(X)	(X)	(X)	100
Archivists curators and museum technicians 2400 (SOC	Percent	40.1%	0.9%	0.6%	34.5%	2.1%	0.2%	1.1%	0.0%	0.2%	0.0%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Archivists curators and museum technicians 2400 (SOC	Female																
Archivists curators and museum technicians 2400 (SOC	Number	26 650	690	450	22 440	1 550	145	945	0	40	160	45	0	(X)	(X)	(X)	185
Archivists curators and museum technicians 2400 (SOC	Percent	59.9%	1.6%	1.0%	50.4%	3.5%	0.3%	2.1%	0.0%	0.1%	0.4%	0.1%	0.0%	(X)	(X)	(X)	0.4%
Librarians 2430 (SOC 25-4021)	Total both sexes																
Librarians 2430 (SOC 25-4021)	Number	181 670	5 460	2 565	153 065	10 425	795	6 815	55	230	735	695	130	(X)	(X)	(X)	695
Librarians 2430 (SOC 25-4021)	Percent	100.0%	3.0%	1.4%	84.3%	5.7%	0.4%	3.8%	0.0%	0.1%	0.4%	0.4%	0.1%	(X)	(X)	(X)	0.4%
Librarians 2430 (SOC 25-4021)	Male																
Librarians 2430 (SOC 25-4021)	Number	29 795	1 035	450	24 830	1 495	100	1 350	0	55	85	265	35	(X)	(X)	(X)	95
Librarians 2430 (SOC 25-4021)	Percent	16.4%	0.6%	0.2%	13.7%	0.8%	0.1%	0.7%	0.0%	0.0%	0.0%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Librarians 2430 (SOC 25-4021)	Female																
Librarians 2430 (SOC 25-4021)	Number	151 875	4 425	2 115	128 240	8 930	695	5 465	55	180	650	430	95	(X)	(X)	(X)	595
Librarians 2430 (SOC 25-4021)	Percent	83.6%	2.4%	1.2%	70.6%	4.9%	0.4%	3.0%	0.0%	0.1%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.3%
Library technicians 2440 (SOC 25-4031)	Total both sexes																
Library technicians 2440 (SOC 25-4031)	Number	60 375	3 200	2 060	44 340	5 505	350	3 630	100	115	340	240	60	(X)	(X)	(X)	430
Library technicians 2440 (SOC 25-4031)	Percent	100.0%	5.3%	3.4%	73.4%	9.1%	0.6%	6.0%	0.2%	0.2%	0.6%	0.4%	0.1%	(X)	(X)	(X)	0.7%
Library technicians 2440 (SOC 25-4031)	Male																
Library technicians 2440 (SOC 25-4031)	Number	14 450	975	440	9 620	1 645	85	1 230	45	60	115	100	10	(X)	(X)	(X)	125
Library technicians 2440 (SOC 25-4031)	Percent	23.9%	1.6%	0.7%	15.9%	2.7%	0.1%	2.0%	0.1%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Library technicians 2440 (SOC 25-4031)	Female																
Library technicians 2440 (SOC 25-4031)	Number	45 920	2 220	1 620	34 725	3 860	270	2 395	55	55	225	140	50	(X)	(X)	(X)	305
Library technicians 2440 (SOC 25-4031)	Percent	76.1%	3.7%	2.7%	57.5%	6.4%	0.4%	4.0%	0.1%	0.1%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.5%
Teacher assistants 2540 (SOC 25-9041)	Total both sexes																
Teacher assistants 2540 (SOC 25-9041)	Number	1 051 485	91 815	70 790	683 295	150 470	9 225	29 565	1 745	2 335	4 320	1 930	935	(X)	(X)	(X)	5 070
Teacher assistants 2540 (SOC 25-9041)	Percent	100.0%	8.7%	6.7%	65.0%	14.3%	0.9%	2.8%	0.2%	0.2%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.5%
Teacher assistants 2540 (SOC 25-9041)	Male																
Teacher assistants 2540 (SOC 25-9041)	Number	100 025	9 235	8 205	53 285	20 755	1 020	5 375	215	440	375	360	110	(X)	(X)	(X)	645
Teacher assistants 2540 (SOC 25-9041)	Percent	9.5%	0.9%	0.8%	5.1%	2.0%	0.1%	0.5%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Teacher assistants 2540 (SOC 25-9041)	Female																
Teacher assistants 2540 (SOC 25-9041)	Number	951 460	82 580	62 580	630 010	129 715	8 205	24 185	1 530	1 895	3 945	1 570	825	(X)	(X)	(X)	4 420
Teacher assistants 2540 (SOC 25-9041)	Percent	90.5%	7.9%	6.0%	59.9%	12.3%	0.8%	2.3%	0.1%	0.2%	0.4%	0.1%	0.1%	(X)	(X)	(X)	0.4%
Other education training and ibrary workers 2550 (SOC	Total both sexes																
Other education training and ibrary workers 2550 (SOC	Number	91 460	4 830	3 065	67 345	10 750	795	3 015	180	245	410	325	80	(X)	(X)	(X)	430
Other education training and ibrary workers 2550 (SOC	Percent	100.0%	5.3%	3.4%	73.6%	11.8%	0.9%	3.3%	0.2%	0.3%	0.4%	0.4%	0.1%	(X)	(X)	(X)	0.5%
Other education training and ibrary workers 2550 (SOC	Male																
Other education training and ibrary workers 2550 (SOC	Number	25 575	980	795	18 990	3 175	115	970	20	40	120	160	60	(X)	(X)	(X)	140
Other education training and ibrary workers 2550 (SOC	Percent	28.0%	1.1%	0.9%	20.8%	3.5%	0.1%	1.1%	0.0%	0.0%	0.1%	0.2%	0.1%	(X)	(X)	(X)	0.2%
Other education training and ibrary workers 2550 (SOC	Female																
Other education training and ibrary workers 2550 (SOC	Number	65 885	3 845	2 265	48 350	7 570	680	2 045	160	205	285	165	20	(X)	(X)	(X)	290
Other education training and ibrary workers 2550 (SOC	Percent	72.0%	4.2%	2.5%	52.9%	8.3%	0.7%	2.2%	0.2%	0.2%	0.3%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Artists and related workers 2600 (SOC 27-1010)	Total both sexes																
Artists and related workers 2600 (SOC 27-1010)	Number	207 590	9 750	5 725	169 970	6 490	1 565	10 285	180	385	1 255	925	50	(X)	(X)	(X)	1 010
Artists and related workers 2600 (SOC 27-1010)	Percent	100.0%	4.7%	2.8%	81.9%	3.1%	0.8%	5.0%	0.1%	0.2%	0.6%	0.4%	0.0%	(X)	(X)	(X)	0.5%
Artists and related workers 2600 (SOC 27-1010)	Male																
Artists and related workers 2600 (SOC 27-1010)	Number	115 165	6 675	3 845	91 305	4 260	1 110	5 890	125	230	595	530	50	(X)	(X)	(X)	550
Artists and related workers 2600 (SOC 27-1010)	Percent	55.5%	3.2%	1.9%	44.0%	2.1%	0.5%	2.8%	0.1%	0.1%	0.3%	0.3%	0.0%	(X)	(X)	(X)	0.3%
Artists and related workers 2600 (SOC 27-1010)	Female																
Artists and related workers 2600 (SOC 27-1010)	Number	92 420	3 075	1 880	78 665	2 230	455	4 400	55	155	660	395	0	(X)	(X)	(X)	455
Artists and related workers 2600 (SOC 27-1010)	Percent	44.5%	1.5%	0.9%	37.9%	1.1%	0.2%	2.1%	0.0%	0.1%	0.3%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Designers 2630 (SOC 27-1020)	Total both sexes																
Designers 2630 (SOC 27-1020)	Number	820 855	48 435	27 625	640 880	32 845	1 845	56 065	635	1 425	3 080	3 685	295	(X)	(X)	(X)	4 040
Designers 2630 (SOC 27-1020)	Percent	100.0%	5.9%	3.4%	78.1%	4.0%	0.2%	6.8%	0.1%	0.2%	0.4%	0.4%	0.0%	(X)	(X)	(X)	0.5%
Designers 2630 (SOC 27-1020)	Male																
Designers 2630 (SOC 27-1020)	Number	377 915	25 555	14 990	287 080	17 180	885	25 795	455	740	1 320	1 700	135	(X)	(X)	(X)	2 080
Designers 2630 (SOC 27-1020)	Percent	46.0%	3.1%	1.8%	35.0%	2.1%	0.1%	3.1%	0.1%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Designers 2630 (SOC 27-1020)	Female																
Designers 2630 (SOC 27-1020)	Number	442 940	22 880	12 635	353 800	15 665	960	30 270	185	680	1 760	1 990	160	(X)	(X)	(X)	1 960
Designers 2630 (SOC 27-1020)	Percent	54.0%	2.8%	1.5%	43.1%	1.9%	0.1%	3.7%	0.0%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Actors 2700 (SOC 27-2011)	Total both sexes																
Actors 2700 (SOC 27-2011)	Number	47 455	2 230	1 555	34 815	5 260	210	1 350	40	460	380	370	185	(X)	(X)	(X)	605
Actors 2700 (SOC 27-2011)	Percent	100.0%	4.7%	3.3%	73.4%	11.1%	0.4%	2.8%	0.1%	1.0%	0.8%	0.8%	0.4%	(X)	(X)	(X)	1.3%
Actors 2700 (SOC 27-2011)	Male																
Actors 2700 (SOC 27-2011)	Number	27 035	1 175	935	20 070	3 205	100	680	40	175	185	140	80	(X)	(X)	(X)	250
Actors 2700 (SOC 27-2011)	Percent	57.0%	2.5%	2.0%	42.3%	6.8%	0.2%	1.4%	0.1%	0.4%	0.4%	0.3%	0.2%	(X)	(X)	(X)	0.5%
Actors 2700 (SOC 27-2011)	Female																
Actors 2700 (SOC 27-2011)	Number	20 420	1 050	625	14 745	2 055	105	670	0	285	195	230	105	(X)	(X)	(X)	355
Actors 2700 (SOC 27-2011)	Percent	43.0%	2.2%	1.3%	31.1%	4.3%	0.2%	1.4%	0.0%	0.6%	0.4%	0.5%	0.2%	(X)	(X)	(X)	0.7%
Producers and directors 2710 (SOC 27-2012)	Total both sexes																
Producers and directors 2710 (SOC 27-2012)	Number	146,165	8,525	3,645	113,810	11,085	330	5,950	80	430	410	940	200	(X)	(X)	(X)	760
Producers and directors 2710 (SOC 27-2012)	Percent	100.0%	5.8%	2.5%	77.9%	7.6%	0.2%	4.1%	0.1%	0.3%	0.3%	0.6%	0.1%	(X)	(X)	(X)	0.5%
Producers and directors 2710 (SOC 27-2012)	Male																
Producers and directors 2710 (SOC 27-2012)	Number	91,410	5,445	2,050	72,645	6,700	135	3,005	65	165	200	450	140	(X)	(X)	(X)	405
Producers and directors 2710 (SOC 27-2012)	Percent	62.5%	3.7%	1.4%	49.7%	4.6%	0.1%	2.1%	0.0%	0.1%	0.1%	0.3%	0.1%	(X)	(X)	(X)	0.3%
Producers and directors 2710 (SOC 27-2012)	Female																
Producers and directors 2710 (SOC 27-2012)	Number	54 755	3 080	1 595	41 160	4 385	195	2 945	15	265	210	490	60	(X)	(X)	(X)	355
Producers and directors 2710 (SOC 27-2012)	Percent	37.5%	2.1%	1.1%	28.2%	3.0%	0.1%	2.0%	0.0%	0.2%	0.1%	0.3%	0.0%	(X)	(X)	(X)	0.2%
Athletes coaches umpires and related workers 2720	Total both sexes																
Athletes coaches umpires and related workers 2720	Number	268 000	12 570	7 880	208 900	23 775	1 175	7 310	395	1 195	940	1 645	230	(X)	(X)	(X)	1 995
Athletes coaches umpires and related workers 2720	Percent	100.0%	4.7%	2.9%	77.9%	8.9%	0.4%	2.7%	0.1%	0.4%	0.4%	0.6%	0.1%	(X)	(X)	(X)	0.7%
Athletes coaches umpires and related workers 2720	Male																
Athletes coaches umpires and related workers 2720	Number	174 745	8 780	5 525	131 270	18 970	860	5 150	300	790	495	980	150	(X)	(X)	(X)	1 480
Athletes coaches umpires and related workers 2720	Percent	65.2%	3.3%	2.1%	49.0%	7.1%	0.3%	1.9%	0.1%	0.3%	0.2%	0.4%	0.1%	(X)	(X)	(X)	0.6%
Athletes coaches umpires and related workers 2720	Female																
Athletes coaches umpires and related workers 2720	Number	93 260	3 790	2 355	77 625	4 805	310	2 160	90	405	445	665	80	(X)	(X)	(X)	515
Athletes coaches umpires and related workers 2720	Percent	34.8%	1.4%	0.9%	29.0%	1.8%	0.1%	0.8%	0.0%	0.2%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Dancers and choreographers 2740 (SOC 27-2030)	Total both sexes																
Dancers and choreographers 2740 (SOC 27-2030)	Number	24 415	2 355	1 780	14 720	3 005	120	895	305	145	185	285	0	(X)	(X)	(X)	630
Dancers and choreographers 2740 (SOC 27-2030)	Percent	100.0%	9.6%	7.3%	60.3%	12.3%	0.5%	3.7%	1.2%	0.6%	0.8%	1.2%	0.0%	(X)	(X)	(X)	2.6%
Dancers and choreographers 2740 (SOC 27-2030)	Male																
Dancers and choreographers 2740 (SOC 27-2030)	Number	4 495	460	505	2 145	780	40	290	90	45	0	55	0	(X)	(X)	(X)	80
Dancers and choreographers 2740 (SOC 27-2030)	Percent	18.4%	1.9%	2.1%	8.8%	3.2%	0.2%	1.2%	0.4%	0.2%	0.0%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Dancers and choreographers 2740 (SOC 27-2030)	Female																
Dancers and choreographers 2740 (SOC 27-2030)	Number	19 920	1 895	1 270	12 570	2 225	80	600	215	100	185	230	0	(X)	(X)	(X)	545
Dancers and choreographers 2740 (SOC 27-2030)	Percent	81.6%	7.8%	5.2%	51.5%	9.1%	0.3%	2.5%	0.9%	0.4%	0.8%	0.9%	0.0%	(X)	(X)	(X)	2.2%
Musicians singers and related workers 2750 (SOC 27-	Total both sexes																
Musicians singers and related workers 2750 (SOC 27-	Number	189 510	10 015	6 015	140 200	22 520	495	6 045	285	760	760	825	260	(X)	(X)	(X)	1 340
Musicians, singers, and related workers 2750 (SOC 27-	Percent	100.0%	5.3%	3.2%	74.0%	11.9%	0.3%	3.2%	0.2%	0.4%	0.4%	0.4%	0.1%	(X)	(X)	(X)	0.7%
Musicians singers and related workers 2750 (SOC 27-	Male																
Musicians singers and related workers 2750 (SOC 27-	Number	124 360	8 350	5 140	86 050	18 380	355	3 265	205	605	365	505	205	(X)	(X)	(X)	940
Musicians singers and related workers 2750 (SOC 27-	Percent	65.6%	4.4%	2.7%	45.4%	9.7%	0.2%	1.7%	0.1%	0.3%	0.2%	0.3%	0.1%	(X)	(X)	(X)	0.5%
Musicians singers and related workers 2750 (SOC 27-	Female																
Musicians singers and related workers 2750 (SOC 27-	Number	65 150	1 665	875	54 150	4 140	140	2 780	80	155	395	320	50	(X)	(X)	(X)	400
Musicians singers and related workers 2750 (SOC 27-	Percent	34.4%	0.9%	0.5%	28.6%	2.2%	0.1%	1.5%	0.0%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Entertainers and performers sports and related workers	Total both sexes																
Entertainers and performers sports and related workers	Number	45 080	3 015	2 210	32 040	4 615	290	1 120	165	265	420	230	160	(X)	(X)	(X)	545
Entertainers and performers sports and related workers	Percent	100.0%	6.7%	4.9%	71.1%	10.2%	0.6%	2.5%	0.4%	0.6%	0.9%	0.5%	0.4%	(X)	(X)	(X)	1.2%

Entertainers and performers, sports and related workers,	Male																
Entertainers and performers sports and related workers	Number	23 810	1 685	1 065	16 775	2 805	90	430	100	185	195	100	80	(X)	(X)	(X)	295
Entertainers and performers sports and related workers	Percent	52.8%	3.7%	2.4%	37.2%	6.2%	0.2%	1.0%	0.2%	0.4%	0.4%	0.2%	0.2%	(X)	(X)	(X)	0.7%
Entertainers and performers, sports and related workers,	Female																
Entertainers and performers sports and related workers	Number	21 270	1 330	1 140	15 265	1 810	200	690	70	80	225	130	80	(X)	(X)	(X)	245
Entertainers and performers sports and related workers	Percent	47.2%	3.0%	2.5%	33.9%	4.0%	0.4%	1.5%	0.2%	0.2%	0.5%	0.3%	0.2%	(X)	(X)	(X)	0.5%
Announcers 2800 (SOC 27-3010)	Total both sexes																
Announcers 2800 (SOC 27-3010)	Number	54 380	4 265	2 745	38 540	5 865	265	1 515	60	195	275	310	75	(X)	(X)	(X)	275
Announcers 2800 (SOC 27-3010)	Percent	100.0%	7.8%	5.0%	70.9%	10.8%	0.5%	2.8%	0.1%	0.4%	0.5%	0.6%	0.1%	(X)	(X)	(X)	0.5%
Announcers 2800 (SOC 27-3010)	Male																
Announcers 2800 (SOC 27-3010)	Number	42 335	3 565	2 425	30 000	4 435	180	965	60	150	140	195	50	(X)	(X)	(X)	170
Announcers 2800 (SOC 27-3010)	Percent	77.9%	6.6%	4.5%	55.2%	8.2%	0.3%	1.8%	0.1%	0.3%	0.3%	0.4%	0.1%	(X)	(X)	(X)	0.3%
Announcers 2800 (SOC 27-3010)	Female																
Announcers 2800 (SOC 27-3010)	Number	12 045	700	315	8 540	1 430	85	555	0	45	135	110	25	(X)	(X)	(X)	105
Announcers 2800 (SOC 27-3010)	Percent	22.1%	1.3%	0.6%	15.7%	2.6%	0.2%	1.0%	0.0%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.2%
News analysts reporters and correspondents 2810 (SOC	Total both sexes																
News analysts reporters and correspondents 2810 (SOC	Number	86 045	4 785	1 970	68 765	5 040	285	3 425	25	315	360	610	70	(X)	(X)	(X)	395
News analysts reporters and correspondents 2810 (SOC	Percent	100.0%	5.6%	2.3%	79.9%	5.9%	0.3%	4.0%	0.0%	0.4%	0.4%	0.7%	0.1%	(X)	(X)	(X)	0.5%
News analysts reporters and correspondents 2810 (SOC	Male																
News analysts reporters and correspondents 2810 (SOC	Number	46 695	2 315	1 060	38 230	2 445	120	1 725	15	185	210	145	35	(X)	(X)	(X)	200
News analysts reporters and correspondents 2810 (SOC	Percent	54.3%	2.7%	1.2%	44.4%	2.8%	0.1%	2.0%	0.0%	0.2%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.2%
News analysts reporters and correspondents 2810 (SOC	Female																
News analysts reporters and correspondents 2810 (SOC	Number	39 350	2 470	910	30 535	2 590	165	1 700	10	130	150	465	35	(X)	(X)	(X)	195
News analysts reporters and correspondents 2810 (SOC	Percent	45.7%	2.9%	1.1%	35.5%	3.0%	0.2%	2.0%	0.0%	0.2%	0.2%	0.5%	0.0%	(X)	(X)	(X)	0.2%
Public relations specialists 2825 (SOC 27-3031)	Total both sexes																
Public relations specialists 2825 (SOC 27-3031)	Number	138,955	6,370	3,360	111,250	10,665	605	4,770	80	270	320	545	60	(X)	(X)	(X)	670
Public relations specialists 2825 (SOC 27-3031)	Percent	100.0%	4.6%	2.4%	80.1%	7.7%	0.4%	3.4%	0.1%	0.2%	0.2%	0.4%	0.0%	(X)	(X)	(X)	0.5%
Public relations specialists 2825 (SOC 27-3031)	Male																
Public relations specialists 2825 (SOC 27-3031)	Number	49,825	2,140	1,220	40,545	3,455	275	1,565	30	60	150	185	0	(X)	(X)	(X)	190
Public relations specialists 2825 (SOC 27-3031)	Percent	35.9%	1.5%	0.9%	29.2%	2.5%	0.2%	1.1%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Public relations specialists 2825 (SOC 27-3031)	Female																
Public relations specialists 2825 (SOC 27-3031)	Number	89 130	4 230	2 140	70 705	7 210	330	3 205	45	205	165	355	60	(X)	(X)	(X)	475
Public relations specialists 2825 (SOC 27-3031)	Percent	64.1%	3.0%	1.5%	50.9%	5.2%	0.2%	2.3%	0.0%	0.1%	0.1%	0.3%	0.0%	(X)	(X)	(X)	0.3%
Editors 2830 (SOC 27-3041)	Total both sexes																
Editors 2830 (SOC 27-3041)	Number	180 915	6 640	3 025	152 635	7 720	420	7 445	140	550	530	1 050	85	(X)	(X)	(X)	675
Editors 2830 (SOC 27-3041)	Percent	100.0%	3.7%	1.7%	84.4%	4.3%	0.2%	4.1%	0.1%	0.3%	0.3%	0.6%	0.0%	(X)	(X)	(X)	0.4%
Editors 2830 (SOC 27-3041)	Male																
Editors 2830 (SOC 27-3041)	Number	81 625	3 515	1 835	68 415	3 180	205	3 030	80	365	285	445	0	(X)	(X)	(X)	270
Editors 2830 (SOC 27-3041)	Percent	45.1%	1.9%	1.0%	37.8%	1.8%	0.1%	1.7%	0.0%	0.2%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.1%
Editors 2830 (SOC 27-3041)	Female																
Editors 2830 (SOC 27-3041)	Number	99 290	3 125	1 195	84 215	4 535	215	4 415	65	185	245	605	85	(X)	(X)	(X)	400
Editors 2830 (SOC 27-3041)	Percent	54.9%	1.7%	0.7%	46.5%	2.5%	0.1%	2.4%	0.0%	0.1%	0.1%	0.3%	0.0%	(X)	(X)	(X)	0.2%
Technical writers 2840 (SOC 27-3042)	Total both sexes																
Technical writers 2840 (SOC 27-3042)	Number	64 080	1 665	515	54 130	3 780	235	2 645	10	165	230	330	15	(X)	(X)	(X)	355
Technical writers 2840 (SOC 27-3042)	Percent	100.0%	2.6%	0.8%	84.5%	5.9%	0.4%	4.1%	0.0%	0.3%	0.4%	0.5%	0.0%	(X)	(X)	(X)	0.6%
Technical writers 2840 (SOC 27-3042)	Male																
Technical writers 2840 (SOC 27-3042)	Number	28 400	910	240	24 465	1 380	75	890	10	80	85	85	15	(X)	(X)	(X)	165
Technical writers 2840 (SOC 27-3042)	Percent	44.3%	1.4%	0.4%	38.2%	2.2%	0.1%	1.4%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Technical writers 2840 (SOC 27-3042)	Female																
Technical writers 2840 (SOC 27-3042)	Number	35 680	755	275	29 670	2 405	160	1 755	0	85	140	245	0	(X)	(X)	(X)	190
Technical writers 2840 (SOC 27-3042)	Percent	55.7%	1.2%	0.4%	46.3%	3.8%	0.2%	2.7%	0.0%	0.1%	0.2%	0.4%	0.0%	(X)	(X)	(X)	0.3%
Writers and authors 2850 (SOC 27-3043)	Total both sexes																
Writers and authors 2850 (SOC 27-3043)	Number	194 250	5 070	2 230	166 370	9 875	870	6 420	85	535	1 165	790	155	(X)	(X)	(X)	690
Writers and authors 2850 (SOC 27-3043)	Percent	100.0%	2.6%	1.1%	85.6%	5.1%	0.4%	3.3%	0.0%	0.3%	0.6%	0.4%	0.1%	(X)	(X)	(X)	0.4%
Writers and authors 2850 (SOC 27-3043)	Male																
Writers and authors 2850 (SOC 27-3043)	Number	83 845	2 030	865	72 470	3 945	430	2 740	25	210	370	375	25	(X)	(X)	(X)	360
Writers and authors 2850 (SOC 27-3043)	Percent	43.2%	1.0%	0.4%	37.3%	2.0%	0.2%	1.4%	0.0%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Writers and authors 2850 (SOC 27-3043)	Female																
Writers and authors 2850 (SOC 27-3043)	Number	110 405	3 035	1 365	93 900	5 930	435	3 685	60	325	795	415	130	(X)	(X)	(X)	330
Writers and authors 2850 (SOC 27-3043)	Percent	56.8%	1.6%	0.7%	48.3%	3.1%	0.2%	1.9%	0.0%	0.2%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.2%
Miscellaneous media and communication workers 2860	Total both sexes																
Miscellaneous media and communication workers 2860	Number	85 660	19 185	10 745	40 000	4 375	455	9 620	50	115	160	360	60	(X)	(X)	(X)	535
Miscellaneous media and communication workers 2860	Percent	100.0%	22.4%	12.5%	46.7%	5.1%	0.5%	11.2%	0.1%	0.1%	0.2%	0.4%	0.1%	(X)	(X)	(X)	0.6%
Miscellaneous media and communication workers 2860	Male																
Miscellaneous media and communication workers 2860	Number	26 310	4 590	2 405	13 465	1 710	135	3 405	30	105	25	235	15	(X)	(X)	(X)	185
Miscellaneous media and communication workers 2860	Percent	30.7%	5.4%	2.8%	15.7%	2.0%	0.2%	4.0%	0.0%	0.1%	0.0%	0.3%	0.0%	(X)	(X)	(X)	0.2%
Miscellaneous media and communication workers 2860	Female																
Miscellaneous media and communication workers 2860	Number	59 350	14 595	8 335	26 540	2 660	320	6 215	20	10	135	125	40	(X)	(X)	(X)	350
Miscellaneous media and communication workers 2860	Percent	69.3%	17.0%	9.7%	31.0%	3.1%	0.4%	7.3%	0.0%	0.0%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.4%
Broadcast and sound engineering technicians and radio	Total both sexes																
Broadcast and sound engineering technicians and radio	Number	94 080	5 490	3 615	70 265	9 280	475	2 995	105	295	370	375	110	(X)	(X)	(X)	710
Broadcast and sound engineering technicians and radio	Percent	100.0%	5.8%	3.8%	74.7%	9.9%	0.5%	3.2%	0.1%	0.3%	0.4%	0.4%	0.1%	(X)	(X)	(X)	0.8%
Broadcast and sound engineering technicians and radio	Male																
Broadcast and sound engineering technicians and radio	Number	83 070	4 735	3 290	62 630	7 900	395	2 500	65	245	335	325	90	(X)	(X)	(X)	555
Broadcast and sound engineering technicians and radio	Percent	88.3%	5.0%	3.5%	66.6%	8.4%	0.4%	2.7%	0.1%	0.3%	0.4%	0.3%	0.1%	(X)	(X)	(X)	0.6%
Broadcast and sound engineering technicians and radio	Female																
Broadcast and sound engineering technicians and radio	Number	11 010	755	325	7 630	1 375	80	495	45	50	30	50	20	(X)	(X)	(X)	155
Broadcast and sound engineering technicians and radio	Percent	11.7%	0.8%	0.3%	8.1%	1.5%	0.1%	0.5%	0.0%	0.1%	0.0%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Photographers 2910 (SOC 27-4021)	Total, both sexes																
Photographers 2910 (SOC 27-4021)	Number	153 930	8 990	5 215	121 530	8 760	470	5 985	145	335	740	845	80	(X)	(X)	(X)	830
Photographers 2910 (SOC 27-4021)	Percent	100.0%	5.8%	3.4%	79.0%	5.7%	0.3%	3.9%	0.1%	0.2%	0.5%	0.5%	0.1%	(X)	(X)	(X)	0.5%
Photographers 2910 (SOC 27-4021)	Male																
Photographers 2910 (SOC 27-4021)	Number	84 310	4 990	2 915	65 555	5 170	240	4 110	75	125	320	415	0	(X)	(X)	(X)	395
Photographers 2910 (SOC 27-4021)	Percent	54.8%	3.2%	1.9%	42.6%	3.4%	0.2%	2.7%	0.0%	0.1%	0.2%	0.3%	0.0%	(X)	(X)	(X)	0.3%
Photographers 2910 (SOC 27-4021)	Female																
Photographers 2910 (SOC 27-4021)	Number	69 620	4 000	2 300	55 975	3 590	230	1 875	70	215	420	430	80	(X)	(X)	(X)	430
Photographers 2910 (SOC 27-4021)	Percent	45.2%	2.6%	1.5%	36.4%	2.3%	0.1%	1.2%	0.0%	0.1%	0.3%	0.3%	0.1%	(X)	(X)	(X)	0.3%
Television video and motion picture camera operators and	Total both sexes																
Television video and motion picture camera operators and	Number	48 400	2 880	1 615	37 185	3 330	100	2 115	80	145	205	360	30	(X)	(X)	(X)	355
Television video and motion picture camera operators and	Percent	100.0%	6.0%	3.3%	76.8%	6.9%	0.2%	4.4%	0.2%	0.3%	0.4%	0.7%	0.1%	(X)	(X)	(X)	0.7%
Television video and motion picture camera operators and	Male																
Television video and motion picture camera operators and	Number	39 435	2 425	1 425	30 320	2 675	80	1 590	65	75	160	335	30	(X)	(X)	(X)	260
Television video and motion picture camera operators and	Percent	81.5%	5.0%	2.9%	62.6%	5.5%	0.2%	3.3%	0.1%	0.2%	0.3%	0.7%	0.1%	(X)	(X)	(X)	0.5%
Television video and motion picture camera operators and	Female																
Television video and motion picture camera operators and	Number	8 965	450	195	6 870	650	25	525	15	70	45	25	0	(X)	(X)	(X)	100
Television video and motion picture camera operators and	Percent	18.5%	0.9%	0.4%	14.2%	1.3%	0.1%	1.1%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Chiropractors 3000 (SOC 29-1011)	Total both sexes																
Chiropractors 3000 (SOC 29-1011)	Number	56 755	1 415	610	50 530	1 150	120	2 230	35	10	195	260	35	(X)	(X)	(X)	160
Chiropractors 3000 (SOC 29-1011)	Percent	100.0%	2.5%	1.1%	89.0%	2.0%	0.2%	3.9%	0.1%	0.0%	0.3%	0.5%	0.1%	(X)	(X)	(X)	0.3%
Chiropractors 3000 (SOC 29-1011)	Male																
Chiropractors 3000 (SOC 29-1011)	Number	42,335	930	375	38,175	650	75	1,680	25	10	110	145	35	(X)	(X)	(X)	120
Chiropractors 3000 (SOC 29-1011)	Percent	74.6%	1.6%	0.7%	67.3%	1.1%	0.1%	3.0%	0.0%	0.0%	0.2%	0.3%	0.1%	(X)	(X)	(X)	0.2%
Chiropractors 3000 (SOC 29-1011)	Female																
Chiropractors 3000 (SOC 29-1011)	Number	14,420	485	235	12,355	500	45	550	10	0	85	115	0	(X)	(X)	(X)	40
Chiropractors 3000 (SOC 29-1011)	Percent	25.4%	0.9%	0.4%	21.8%	0.9%	0.1%	1.0%	0.0%	0.0%	0.1%	0.2%	0.0%	(X)	(X)	(X)	0.1%
Dentists 3010 (SOC 29-1020)	Total both sexes																
Dentists 3010 (SOC 29-1020)	Number	165 835	7 275	2 000	126 200	5 425	190	22 850	70	155	320	590	75	(X)	(X)	(X)	680
Dentists 3010 (SOC 29-1020)	Percent	100.0%	4.4%	1.2%	76.1%	3.3%	0.1%	13.8%	0.0%	0.1%	0.2%	0.4%	0.0%	(X)	(X)	(X)	0.4%
Dentists 3010 (SOC 29-1020)	Male																
Dentists 3010 (SOC 29-1020)	Number	127 595	4 410	1 260	103 735	3 275	165	13 440	60	120	280	375	40	(X)	(X)	(X)	445
Dentists 3010 (SOC 29-1020)	Percent	76.9%	2.7%	0.8%	62.6%	2.0%	0.1%	8.1%	0.0%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Dentists 3010 (SOC 29-1020)	Female																
Dentists 3010 (SOC 29-1020)	Number	38 240	2 865	740	22 470	2 155	25	9 410	10	35	45	215	35	(X)	(X)	(X)	235
Dentists 3010 (SOC 29-1020)	Percent	23.1%	1.7%	0.4%	13.5%	1.3%	0.0%	5.7%	0.0%	0.0%	0.0%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Dietitians and nutritionists 3030 (SOC 29-1031)	Total both sexes																
Dietitians and nutritionists 3030 (SOC 29-1031)	Number	90 140	4 805	2 715	62 630	13 350	625	4 975	50	85	265	245	110	(X)	(X)	(X)	285
Dietitians and nutritionists 3030 (SOC 29-1031)	Percent	100.0%	5.3%	3.0%	69.5%	14.8%	0.7%	5.5%	0.1%	0.1%	0.3%	0.3%	0.1%	(X)	(X)	(X)	0.3%
Dietitians and nutritionists 3030 (SOC 29-1031)	Male																
Dietitians and nutritionists 3030 (SOC 29-1031)	Number	8 830	600	615	5 175	1 875	40	345	4	10	45	20	15	(X)	(X)	(X)	85
Dietitians and nutritionists 3030 (SOC 29-1031)	Percent	9.8%	0.7%	0.7%	5.7%	2.1%	0.0%	0.4%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Dietitians and nutritionists 3030 (SOC 29-1031)	Female																
Dietitians and nutritionists 3030 (SOC 29-1031)	Number	81 310	4 205	2 100	57 455	11 475	580	4 635	45	75	220	225	95	(X)	(X)	(X)	205
Dietitians and nutritionists 3030 (SOC 29-1031)	Percent	90.2%	4.7%	2.3%	63.7%	12.7%	0.6%	5.1%	0.0%	0.1%	0.2%	0.2%	0.1%	(X)	(X)	(X)	0.2%
Optometrists 3040 (SOC 29-1041)	Total both sexes																
Optometrists 3040 (SOC 29-1041)	Number	35 155	705	335	28 720	460	100	4 550	45	0	65	50	15	(X)	(X)	(X)	110
Optometrists 3040 (SOC 29-1041)	Percent	100.0%	2.0%	1.0%	81.7%	1.3%	0.3%	12.9%	0.1%	0.0%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Optometrists 3040 (SOC 29-1041)	Male																
Optometrists 3040 (SOC 29-1041)	Number	22 680	270	250	19 985	190	35	1 790	25	0	40	35	15	(X)	(X)	(X)	55
Optometrists 3040 (SOC 29-1041)	Percent	64.5%	0.8%	0.7%	56.8%	0.5%	0.1%	5.1%	0.1%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Optometrists 3040 (SOC 29-1041)	Female																
Optometrists 3040 (SOC 29-1041)	Number	12 475	435	90	8 740	275	65	2 760	20	0	25	15	0	(X)	(X)	(X)	55
Optometrists 3040 (SOC 29-1041)	Percent	35.5%	1.2%	0.3%	24.9%	0.8%	0.2%	7.9%	0.1%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.2%
Pharmacists 3050 (SOC 29-1051)	Total both sexes																
Pharmacists 3050 (SOC 29-1051)	Number	253 925	6 970	2 410	186 115	14 370	645	40 695	175	195	400	865	80	(X)	(X)	(X)	1 005
Pharmacists 3050 (SOC 29-1051)	Percent	100.0%	2.7%	0.9%	73.3%	5.7%	0.3%	16.0%	0.1%	0.1%	0.2%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Pharmacists 3050 (SOC 29-1051)	Male																
Pharmacists 3050 (SOC 29-1051)	Number	120 245	2 875	1 120	94 040	5 125	320	15 475	90	110	215	300	20	(X)	(X)	(X)	565
Pharmacists 3050 (SOC 29-1051)	Percent	47.4%	1.1%	0.4%	37.0%	2.0%	0.1%	6.1%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%

Pharmacists 3050 (SOC 29-1051)	Female																
Pharmacists 3050 (SOC 29-1051)	Number	133 680	4 095	1 290	92 075	9 245	325	25 220	80	90	190	570	60	(X)	(X)	(X)	440
Pharmacists 3050 (SOC 29-1051)	Percent	52.6%	1.6%	0.5%	36.3%	3.6%	0.1%	9.9%	0.0%	0.0%	0.1%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Physicians and surgeons 3060 (SOC 29-1060)	Total, both sexes																
Physicians and surgeons 3060 (SOC 29-1060)	Number	834 265	37 650	11 125	575 355	40 940	1 585	154 970	315	835	1 280	4 230	320	(X)	(X)	(X)	5 665
Physicians and surgeons 3060 (SOC 29-1060)	Percent	100.0%	4.5%	1.3%	69.0%	4.9%	0.2%	18.6%	0.0%	0.1%	0.2%	0.5%	0.0%	(X)	(X)	(X)	0.7%
Physicians and surgeons 3060 (SOC 29-1060)	Male																
Physicians and surgeons 3060 (SOC 29-1060)	Number	563 595	25 620	7 110	407 440	21 750	1 065	93 240	145	550	710	2 350	130	(X)	(X)	(X)	3 485
Physicians and surgeons 3060 (SOC 29-1060)	Percent	67.6%	3.1%	0.9%	48.8%	2.6%	0.1%	11.2%	0.0%	0.1%	0.1%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Physicians and surgeons 3060 (SOC 29-1060)	Female																
Physicians and surgeons 3060 (SOC 29-1060)	Number	270 670	12 030	4 015	167 915	19 190	520	61 730	170	285	570	1 880	190	(X)	(X)	(X)	2 180
Physicians and surgeons 3060 (SOC 29-1060)	Percent	32.4%	1.4%	0.5%	20.1%	2.3%	0.1%	7.4%	0.0%	0.0%	0.1%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Physician assistants 3110 (SOC 29-1071)	Total, both sexes																
Physician assistants 3110 (SOC 29-1071)	Number	103 945	6 730	3 345	75 365	8 735	490	7 500	25	205	270	440	120	(X)	(X)	(X)	720
Physician assistants 3110 (SOC 29-1071)	Percent	100.0%	6.5%	3.2%	72.5%	8.4%	0.5%	7.2%	0.0%	0.2%	0.3%	0.4%	0.1%	(X)	(X)	(X)	0.7%
Physician assistants 3110 (SOC 29-1071)	Male																
Physician assistants 3110 (SOC 29-1071)	Number	34 485	2 505	1 130	24 340	2 905	185	2 750	20	45	85	90	100	(X)	(X)	(X)	330
Physician assistants 3110 (SOC 29-1071)	Percent	33.2%	2.4%	1.1%	23.4%	2.8%	0.2%	2.6%	0.0%	0.0%	0.1%	0.1%	0.1%	(X)	(X)	(X)	0.3%
Physician assistants 3110 (SOC 29-1071)	Female																
Physician assistants 3110 (SOC 29-1071)	Number	69 460	4 225	2 210	51 025	5 830	305	4 750	4	160	185	350	20	(X)	(X)	(X)	390
Physician assistants 3110 (SOC 29-1071)	Percent	66.8%	4.1%	2.1%	49.1%	5.6%	0.3%	4.6%	0.0%	0.2%	0.2%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Podiatrists 3120 (SOC 29-1081)	Total, both sexes																
Podiatrists 3120 (SOC 29-1081)	Number	9 840	340	130	8 160	465	0	690	15	0	0	10	0	(X)	(X)	(X)	30
Podiatrists 3120 (SOC 29-1081)	Percent	100.0%	3.5%	1.3%	82.9%	4.7%	0.0%	7.0%	0.2%	0.0%	0.0%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Podiatrists 3120 (SOC 29-1081)	Male																
Podiatrists 3120 (SOC 29-1081)	Number	7,920	295	85	6,760	325	0	420	15	0	0	0	0	(X)	(X)	(X)	20
Podiatrists 3120 (SOC 29-1081)	Percent	80.5%	3.0%	0.9%	68.7%	3.3%	0.0%	4.3%	0.2%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.2%
Podiatrists 3120 (SOC 29-1081)	Female																
Podiatrists 3120 (SOC 29-1081)	Number	1,920	45	45	1,400	135	0	270	0	0	0	10	0	(X)	(X)	(X)	10
Podiatrists 3120 (SOC 29-1081)	Percent	19.5%	0.5%	0.5%	14.2%	1.4%	0.0%	2.7%	0.0%	0.0%	0.0%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Audiologists 3140 (SOC 29-1181)	Total, both sexes																
Audiologists 3140 (SOC 29-1181)	Number	13 920	240	210	12 550	515	10	270	0	0	30	4	60	(X)	(X)	(X)	35
Audiologists 3140 (SOC 29-1181)	Percent	100.0%	1.7%	1.5%	90.2%	3.7%	0.1%	1.9%	0.0%	0.0%	0.2%	0.0%	0.4%	(X)	(X)	(X)	0.3%
Audiologists 3140 (SOC 29-1181)	Male																
Audiologists 3140 (SOC 29-1181)	Number	2 860	30	80	2 660	25	0	20	0	0	4	0	20	(X)	(X)	(X)	15
Audiologists 3140 (SOC 29-1181)	Percent	20.5%	0.2%	0.6%	19.1%	0.2%	0.0%	0.1%	0.0%	0.0%	0.0%	0.0%	0.1%	(X)	(X)	(X)	0.1%
Audiologists 3140 (SOC 29-1181)	Female																
Audiologists 3140 (SOC 29-1181)	Number	11 060	210	130	9 885	490	10	250	0	0	25	4	40	(X)	(X)	(X)	20
Audiologists 3140 (SOC 29-1181)	Percent	79.5%	1.5%	0.9%	71.0%	3.5%	0.1%	1.8%	0.0%	0.0%	0.2%	0.0%	0.3%	(X)	(X)	(X)	0.1%
Occupational therapists 3150 (SOC 29-1122)	Total, both sexes																
Occupational therapists 3150 (SOC 29-1122)	Number	84 920	2 530	1 230	71 010	4 170	160	4 885	35	75	210	255	10	(X)	(X)	(X)	345
Occupational therapists 3150 (SOC 29-1122)	Percent	100.0%	3.0%	1.4%	83.6%	4.9%	0.2%	5.8%	0.0%	0.1%	0.2%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Occupational therapists 3150 (SOC 29-1122)	Male																
Occupational therapists 3150 (SOC 29-1122)	Number	8 685	325	305	6 505	685	10	705	0	20	4	60	0	(X)	(X)	(X)	70
Occupational therapists 3150 (SOC 29-1122)	Percent	10.2%	0.4%	0.4%	7.7%	0.8%	0.0%	0.8%	0.0%	0.0%	0.0%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Occupational therapists 3150 (SOC 29-1122)	Female																
Occupational therapists 3150 (SOC 29-1122)	Number	76 235	2 210	925	64 505	3 485	150	4 180	35	60	205	195	10	(X)	(X)	(X)	275
Occupational therapists 3150 (SOC 29-1122)	Percent	89.8%	2.6%	1.1%	76.0%	4.1%	0.2%	4.9%	0.0%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Physical therapists 3160 (SOC 29-1123)	Total, both sexes																
Physical therapists 3160 (SOC 29-1123)	Number	185 185	5 380	3 035	149 795	7 150	490	17 415	155	180	345	715	20	(X)	(X)	(X)	505
Physical therapists 3160 (SOC 29-1123)	Percent	100.0%	2.9%	1.6%	80.9%	3.9%	0.3%	9.4%	0.1%	0.1%	0.2%	0.4%	0.0%	(X)	(X)	(X)	0.3%
Physical therapists 3160 (SOC 29-1123)	Male																
Physical therapists 3160 (SOC 29-1123)	Number	55 405	1 785	1 150	42 695	2 225	100	6 685	105	80	185	225	20	(X)	(X)	(X)	150
Physical therapists 3160 (SOC 29-1123)	Percent	29.9%	1.0%	0.6%	23.1%	1.2%	0.1%	3.6%	0.1%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Physical therapists 3160 (SOC 29-1123)	Female																
Physical therapists 3160 (SOC 29-1123)	Number	129 780	3 595	1 890	107 100	4 925	390	10 730	45	105	165	490	0	(X)	(X)	(X)	355
Physical therapists 3160 (SOC 29-1123)	Percent	70.1%	1.9%	1.0%	57.8%	2.7%	0.2%	5.8%	0.0%	0.1%	0.1%	0.3%	0.0%	(X)	(X)	(X)	0.2%
Radiation therapists 3200 (SOC 29-1124)	Total, both sexes																
Radiation therapists 3200 (SOC 29-1124)	Number	13 565	415	275	11 455	515	35	740	0	4	20	75	30	(X)	(X)	(X)	0
Radiation therapists 3200 (SOC 29-1124)	Percent	100.0%	3.1%	2.0%	84.4%	3.8%	0.3%	5.5%	0.0%	0.0%	0.1%	0.6%	0.2%	(X)	(X)	(X)	0.0%
Radiation therapists 3200 (SOC 29-1124)	Male																
Radiation therapists 3200 (SOC 29-1124)	Number	3 600	185	135	2 670	205	10	370	0	0	20	0	0	(X)	(X)	(X)	0
Radiation therapists 3200 (SOC 29-1124)	Percent	26.5%	1.4%	1.0%	19.7%	1.5%	0.1%	2.7%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Radiation therapists 3200 (SOC 29-1124)	Female																
Radiation therapists 3200 (SOC 29-1124)	Number	9 965	225	135	8 780	310	30	365	0	4	0	75	30	(X)	(X)	(X)	0
Radiation therapists 3200 (SOC 29-1124)	Percent	73.5%	1.7%	1.0%	64.7%	2.3%	0.2%	2.7%	0.0%	0.0%	0.0%	0.6%	0.2%	(X)	(X)	(X)	0.0%
Recreational therapists 3210 (SOC 29-1125)	Total, both sexes																
Recreational therapists 3210 (SOC 29-1125)	Number	14 510	430	270	10 670	2 445	105	490	0	20	40	15	0	(X)	(X)	(X)	25
Recreational therapists 3210 (SOC 29-1125)	Percent	100.0%	3.0%	1.9%	73.5%	16.9%	0.7%	3.4%	0.0%	0.1%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Recreational therapists 3210 (SOC 29-1125)	Male																
Recreational therapists 3210 (SOC 29-1125)	Number	3 160	155	90	2 050	655	50	135	0	0	10	0	0	(X)	(X)	(X)	10
Recreational therapists 3210 (SOC 29-1125)	Percent	21.8%	1.1%	0.6%	14.1%	4.5%	0.3%	0.9%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Recreational therapists 3210 (SOC 29-1125)	Female																
Recreational therapists 3210 (SOC 29-1125)	Number	11 350	275	180	8 625	1 790	55	355	0	20	25	15	0	(X)	(X)	(X)	10
Recreational therapists 3210 (SOC 29-1125)	Percent	78.2%	1.9%	1.2%	59.4%	12.3%	0.4%	2.4%	0.0%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Respiratory therapists 3220 (SOC 29-1126)	Total, both sexes																
Respiratory therapists 3220 (SOC 29-1126)	Number	100 170	4 220	2 830	73 880	11 785	310	5 615	65	210	435	315	75	(X)	(X)	(X)	430
Respiratory therapists 3220 (SOC 29-1126)	Percent	100.0%	4.2%	2.8%	73.8%	11.8%	0.3%	5.6%	0.1%	0.2%	0.4%	0.3%	0.1%	(X)	(X)	(X)	0.4%
Respiratory therapists 3220 (SOC 29-1126)	Male																
Respiratory therapists 3220 (SOC 29-1126)	Number	36 030	2 010	1 295	25 270	3 785	45	3 010	45	60	155	100	10	(X)	(X)	(X)	240
Respiratory therapists 3220 (SOC 29-1126)	Percent	36.0%	2.0%	1.3%	25.2%	3.8%	0.0%	3.0%	0.0%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Respiratory therapists 3220 (SOC 29-1126)	Female																
Respiratory therapists 3220 (SOC 29-1126)	Number	64 140	2 205	1 540	48 610	8 000	265	2 605	20	150	280	215	60	(X)	(X)	(X)	190
Respiratory therapists 3220 (SOC 29-1126)	Percent	64.0%	2.2%	1.5%	48.5%	8.0%	0.3%	2.6%	0.0%	0.1%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.2%
Speech-language pathologists 3230 (SOC 29-1127)	Total, both sexes																
Speech-language pathologists 3230 (SOC 29-1127)	Number	117 190	4 185	1 515	102 355	5 515	305	2 380	25	100	180	215	25	(X)	(X)	(X)	385
Speech-language pathologists 3230 (SOC 29-1127)	Percent	100.0%	3.6%	1.3%	87.3%	4.7%	0.3%	2.0%	0.0%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Speech-language pathologists 3230 (SOC 29-1127)	Male																
Speech-language pathologists 3230 (SOC 29-1127)	Number	4 970	150	55	4 295	250	35	150	0	0	0	15	0	(X)	(X)	(X)	20
Speech-language pathologists 3230 (SOC 29-1127)	Percent	4.2%	0.1%	0.0%	3.7%	0.2%	0.0%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Speech-language pathologists 3230 (SOC 29-1127)	Female																
Speech-language pathologists 3230 (SOC 29-1127)	Number	112 220	4 035	1 460	98 055	5 265	270	2 230	25	100	180	200	25	(X)	(X)	(X)	365
Speech-language pathologists 3230 (SOC 29-1127)	Percent	95.8%	3.4%	1.2%	83.7%	4.5%	0.2%	1.9%	0.0%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Other therapists including exercise physiologists 3245	Total, both sexes																
Other therapists including exercise physiologists 3245	Number	125 855	5 855	3 670	95 065	13 670	525	4 600	130	205	610	590	145	(X)	(X)	(X)	795
Other therapists including exercise physiologists 3245	Percent	100.0%	4.7%	2.9%	75.5%	10.9%	0.4%	3.7%	0.1%	0.2%	0.5%	0.5%	0.1%	(X)	(X)	(X)	0.6%
Other therapists including exercise physiologists 3245	Male																
Other therapists including exercise physiologists 3245	Number	26 930	1 385	715	19 465	3 580	135	1 005	100	40	140	155	40	(X)	(X)	(X)	160
Other therapists including exercise physiologists 3245	Percent	21.4%	1.1%	0.6%	15.5%	2.8%	0.1%	0.8%	0.1%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Other therapists including exercise physiologists 3245	Female																
Other therapists, including exercise physiologists 3245	Number	98,930	4,470	2,950	75,600	10,090	390	3,595	25	160	475	435	105	(X)	(X)	(X)	635
Other therapists including exercise physiologists 3245	Percent	78.6%	3.6%	2.3%	60.1%	8.0%	0.3%	2.9%	0.0%	0.1%	0.4%	0.3%	0.1%	(X)	(X)	(X)	0.5%
Veterinarians 3250 (SOC 29-1131)	Total, both sexes																
Veterinarians 3250 (SOC 29-1131)	Number	72,680	1,795	650	66,250	1,290	130	1,935	15	65	215	160	60	(X)	(X)	(X)	115
Veterinarians 3250 (SOC 29-1131)	Percent	100.0%	2.5%	0.9%	91.2%	1.8%	0.2%	2.7%	0.0%	0.1%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.2%
Veterinarians 3250 (SOC 29-1131)	Male																
Veterinarians 3250 (SOC 29-1131)	Number	36 355	975	415	33 210	410	75	1 000	0	55	105	25	15	(X)	(X)	(X)	75
Veterinarians 3250 (SOC 29-1131)	Percent	50.0%	1.3%	0.6%	45.7%	0.6%	0.1%	1.4%	0.0%	0.1%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Veterinarians 3250 (SOC 29-1131)	Female																
Veterinarians 3250 (SOC 29-1131)	Number	36 325	820	235	33 040	880	60	930	15	10	105	140	45	(X)	(X)	(X)	40
Veterinarians 3250 (SOC 29-1131)	Percent	50.0%	1.1%	0.3%	45.5%	1.2%	0.1%	1.3%	0.0%	0.0%	0.1%	0.2%	0.1%	(X)	(X)	(X)	0.1%
Registered nurses 3255 (SOC 29-1141)	Total, both sexes																
Registered nurses 3255 (SOC 29-1141)	Number	2 639 750	82 200	40 740	1 997 830	262 965	10 305	212 815	2 195	3 035	8 990	6 135	1 450	(X)	(X)	(X)	11 090
Registered nurses 3255 (SOC 29-1141)	Percent	100.0%	3.1%	1.5%	75.7%	10.0%	0.4%	8.1%	0.1%	0.1%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Registered nurses 3255 (SOC 29-1141)	Male																
Registered nurses 3255 (SOC 29-1141)	Number	231 525	11 130	5 570	157 845	23 600	1 025	28 925	265	235	945	655	145	(X)	(X)	(X)	1 185
Registered nurses 3255 (SOC 29-1141)	Percent	8.8%	0.4%	0.2%	6.0%	0.9%	0.0%	1.1%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Registered nurses 3255 (SOC 29-1141)	Female																
Registered nurses 3255 (SOC 29-1141)	Number	2 408 225	71 070	35 175	1 839 985	239 360	9 280	183 890	1 930	2 800	8 045	5 480	1 305	(X)	(X)	(X)	9 905
Registered nurses 3255 (SOC 29-1141)	Percent	91.2%	2.7%	1.3%	69.7%	9.1%	0.4%	7.0%	0.1%	0.1%	0.3%	0.2%	0.0%	(X)	(X)	(X)	0.4%
Nurse anesthetists 3256 (SOC 29-1151)	Total, both sexes																
Nurse anesthetists 3256 (SOC 29-1151)	Number	23 095	415	340	20 430	790	30	775	0	45	55	125	0	(X)	(X)	(X)	90
Nurse anesthetists 3256 (SOC 29-1151)	Percent	100.0%	1.8%	1.5%	88.5%	3.4%	0.1%	3.4%	0.0%	0.2%	0.2%	0.5%	0.0%	(X)	(X)	(X)	0.4%
Nurse anesthetists 3256 (SOC 29-1151)	Male																
Nurse anesthetists 3256 (SOC 29-1151)	Number	9 760	225	175	8 615	305	30	295	0	0	40	35	0	(X)	(X)	(X)	45
Nurse anesthetists 3256 (SOC 29-1151)	Percent	42.3%	1.0%	0.8%	37.3%	1.3%	0.1%	1.3%	0.0%	0.0%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Nurse anesthetists 3256 (SOC 29-1151)	Female																
Nurse anesthetists 3256 (SOC 29-1151)	Number	13 335	190	170	11 815	485	0	475	0	45	15	90	0	(X)	(X)	(X)	45
Nurse anesthetists 3256 (SOC 29-1151)	Percent	57.7%	0.8%	0.7%	51.2%	2.1%	0.0%	2.1%	0.0%	0.2%	0.1%	0.4%	0.0%	(X)	(X)	(X)	0.2%
Nurse practitioners and nurse midwives 3258 (SOC 29-	Total, both sexes																
Nurse practitioners and nurse midwives 3258 (SOC 29-	Number	81 805	2 450	740	70 150	3 830	75	3 545	10	140	280	240	35	(X)	(X)	(X)	315
Nurse practitioners and nurse midwives 3258 (SOC 29-	Percent	100.0%	3.0%	0.9%	85.8%	4.7%	0.1%	4.3%	0.0%	0.2%	0.3%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Nurse practitioners and nurse midwives 3258 (SOC 29-	Male																
Nurse practitioners and nurse midwives 3258 (SOC 29-	Number	5 940	355	65	4 990	210	10	240	0	60	0	0	0	(X)	(X)	(X)	15
Nurse practitioners and nurse midwives 3258 (SOC 29-	Percent	7.3%	0.4%	0.1%	6.1%	0.3%	0.0%	0.3%	0.0%	0.1%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Nurse practitioners and nurse midwives 3258 (SOC 29-	Female																
Nurse practitioners and nurse midwives 3258 (SOC 29-	Number	75 865	2 095	675	65 165	3 615	65	3 305	10	80	280	240	35	(X)	(X)	(X)	300
Nurse practitioners and nurse midwives 3258 (SOC 29-	Percent	92.7%	2.6%	0.8%	79.7%	4.4%	0.1%	4.0%	0.0%	0.1%	0.3%	0.3%	0.0%	(X)	(X)	(X)	0.4%

Health diagnosing and treating practitioners, a l other 3260	Total, both sexes																
Health diagnosing and treating practitioners a l other 3260	Number	18 770	530	295	12 285	385	115	4 740	10	20	125	110	0	(X)	(X)	(X)	155
Health diagnosing and treating practitioners a l other 3260	Percent	100.0%	2.8%	1.6%	65.5%	2.1%	0.6%	25.3%	0.1%	0.1%	0.7%	0.6%	0.0%	(X)	(X)	(X)	0.8%
Health diagnosing and treating practitioners a l other 3260	Male																
Health diagnosing and treating practitioners a l other 3260	Number	6 255	275	155	3 205	195	20	2 285	10	0	85	20	0	(X)	(X)	(X)	15
Health diagnosing and treating practitioners a l other 3260	Percent	33.3%	1.5%	0.8%	17.1%	1.0%	0.1%	12.2%	0.1%	0.0%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Health diagnosing and treating practitioners a l other 3260	Female																
Health diagnosing and treating practitioners a l other 3260	Number	12 515	255	145	9 080	195	95	2 455	0	20	40	90	0	(X)	(X)	(X)	135
Health diagnosing and treating practitioners a l other 3260	Percent	66.7%	1.4%	0.8%	48.4%	1.0%	0.5%	13.1%	0.0%	0.1%	0.2%	0.5%	0.0%	(X)	(X)	(X)	0.7%
Clinical laboratory technologists and technicians 3300	Total both sexes																
Clinical laboratory technologists and technicians 3300	Number	345 965	18 855	11 345	217 910	48 580	1 525	41 365	500	755	1 005	1 855	430	(X)	(X)	(X)	1 845
Clinical laboratory technologists and technicians 3300	Percent	100.0%	5.4%	3.3%	63.0%	14.0%	0.4%	12.0%	0.1%	0.2%	0.3%	0.5%	0.1%	(X)	(X)	(X)	0.5%
Clinical laboratory technologists and technicians 3300	Male																
Clinical laboratory technologists and technicians 3300	Number	89 700	6 460	3 830	51 555	12 265	290	13 265	170	250	290	715	70	(X)	(X)	(X)	540
Clinical laboratory technologists and technicians 3300	Percent	25.9%	1.9%	1.1%	14.9%	3.5%	0.1%	3.8%	0.0%	0.1%	0.1%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Clinical laboratory technologists and technicians 3300	Female																
Clinical laboratory technologists and technicians 3300	Number	256 265	12 395	7 515	166 355	36 315	1 235	28 100	325	510	715	1 140	360	(X)	(X)	(X)	1 305
Clinical laboratory technologists and technicians 3300	Percent	74.1%	3.6%	2.2%	48.1%	10.5%	0.4%	8.1%	0.1%	0.1%	0.2%	0.3%	0.1%	(X)	(X)	(X)	0.4%
Dental hygienists 3310 (SOC 29-2021)	Total both sexes																
Dental hygienists 3310 (SOC 29-2021)	Number	148 390	6 125	2 980	128 285	3 860	365	4 745	70	160	615	545	75	(X)	(X)	(X)	565
Dental hygienists 3310 (SOC 29-2021)	Percent	100.0%	4.1%	2.0%	86.5%	2.6%	0.2%	3.2%	0.0%	0.1%	0.4%	0.4%	0.1%	(X)	(X)	(X)	0.4%
Dental hygienists 3310 (SOC 29-2021)	Male																
Dental hygienists 3310 (SOC 29-2021)	Number	4 905	685	370	2 840	440	4	405	0	0	10	40	20	(X)	(X)	(X)	90
Dental hygienists 3310 (SOC 29-2021)	Percent	3.3%	0.5%	0.2%	1.9%	0.3%	0.0%	0.3%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Dental hygienists 3310 (SOC 29-2021)	Female																
Dental hygienists 3310 (SOC 29-2021)	Number	143,485	5,440	2,610	125,445	3,420	365	4,345	70	160	605	500	55	(X)	(X)	(X)	475
Dental hygienists 3310 (SOC 29-2021)	Percent	96.7%	3.7%	1.8%	84.5%	2.3%	0.2%	2.9%	0.0%	0.1%	0.4%	0.3%	0.0%	(X)	(X)	(X)	0.3%
Diagnostic related technologists and technicians 3320	Total both sexes																
Diagnostic related technologists and technicians 3320	Number	306,190	16,645	9,880	234,955	25,780	900	13,890	290	510	1,225	870	130	(X)	(X)	(X)	1,115
Diagnostic related technologists and technicians 3320	Percent	100.0%	5.4%	3.2%	76.7%	8.4%	0.3%	4.5%	0.1%	0.2%	0.4%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Diagnostic related technologists and technicians 3320	Male																
Diagnostic related technologists and technicians 3320	Number	86 265	7 585	4 415	55 895	9 230	185	7 420	175	190	415	260	60	(X)	(X)	(X)	440
Diagnostic related technologists and technicians 3320	Percent	28.2%	2.5%	1.4%	18.3%	3.0%	0.1%	2.4%	0.1%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Diagnostic related technologists and technicians 3320	Female																
Diagnostic related technologists and technicians 3320	Number	219 925	9 060	5 465	179 060	16 555	715	6 470	115	320	815	605	70	(X)	(X)	(X)	670
Diagnostic related technologists and technicians 3320	Percent	71.8%	3.0%	1.8%	58.5%	5.4%	0.2%	2.1%	0.0%	0.1%	0.3%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Emergency medical technicians and paramedics 3400	Total both sexes																
Emergency medical technicians and paramedics 3400	Number	172 115	10 735	5 375	140 100	9 800	1 385	2 505	45	210	975	445	30	(X)	(X)	(X)	510
Emergency medical technicians and paramedics 3400	Percent	100.0%	6.2%	3.1%	81.4%	5.7%	0.8%	1.5%	0.0%	0.1%	0.6%	0.3%	0.0%	(X)	(X)	(X)	0.3%
Emergency medical technicians and paramedics 3400	Male																
Emergency medical technicians and paramedics 3400	Number	117 760	8 245	3 730	96 135	5 830	770	1 820	25	140	520	255	0	(X)	(X)	(X)	285
Emergency medical technicians and paramedics 3400	Percent	68.4%	4.8%	2.2%	55.9%	3.4%	0.4%	1.1%	0.0%	0.1%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Emergency medical technicians and paramedics 3400	Female																
Emergency medical technicians and paramedics 3400	Number	54 355	2 490	1 645	43 965	3 970	615	685	20	70	460	190	30	(X)	(X)	(X)	225
Emergency medical technicians and paramedics 3400	Percent	31.6%	1.4%	1.0%	25.5%	2.3%	0.4%	0.4%	0.0%	0.0%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Health practitioner support technologists and technicians	Total both sexes																
Health practitioner support technologists and technicians	Number	509 925	31 690	21 535	348 960	64 140	2 990	31 115	825	1 030	2 390	2 060	390	(X)	(X)	(X)	2 790
Health practitioner support technologists and technicians	Percent	100.0%	6.2%	4.2%	68.4%	12.6%	0.6%	6.1%	0.2%	0.2%	0.5%	0.4%	0.1%	(X)	(X)	(X)	0.5%
Health practitioner support technologists and technicians	Male																
Health practitioner support technologists and technicians	Number	102 675	8 035	5 655	59 050	15 910	605	11 110	215	180	400	620	160	(X)	(X)	(X)	735
Health practitioner support technologists and technicians	Percent	20.1%	1.6%	1.1%	11.6%	3.1%	0.1%	2.2%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Health practitioner support technologists and technicians	Female																
Health practitioner support technologists and technicians	Number	407 245	23 660	15 880	289 910	48 230	2 385	20 010	610	850	1 990	1 440	230	(X)	(X)	(X)	2 055
Health practitioner support technologists and technicians	Percent	79.9%	4.6%	3.1%	56.9%	9.5%	0.5%	3.9%	0.1%	0.2%	0.4%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Licensed practical and licensed vocational nurses 3500	Total both sexes																
Licensed practical and licensed vocational nurses 3500	Number	680 945	29 710	19 620	434 975	158 990	4 035	24 295	530	1 340	2 825	1 040	645	(X)	(X)	(X)	2 930
Licensed practical and licensed vocational nurses 3500	Percent	100.0%	4.4%	2.9%	63.9%	23.3%	0.6%	3.6%	0.1%	0.2%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Licensed practical and licensed vocational nurses 3500	Male																
Licensed practical and licensed vocational nurses 3500	Number	50 330	3 220	2 345	26 820	12 485	300	4 355	125	120	95	120	0	(X)	(X)	(X)	340
Licensed practical and licensed vocational nurses 3500	Percent	7.4%	0.5%	0.3%	3.9%	1.8%	0.0%	0.6%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Licensed practical and licensed vocational nurses 3500	Female																
Licensed practical and licensed vocational nurses 3500	Number	630 615	26 490	17 275	408 155	146 505	3 735	19 945	405	1 220	2 730	920	645	(X)	(X)	(X)	2 590
Licensed practical and licensed vocational nurses 3500	Percent	92.6%	3.9%	2.5%	59.9%	21.5%	0.5%	2.9%	0.1%	0.2%	0.4%	0.1%	0.1%	(X)	(X)	(X)	0.4%
Medical records and health information technicians 3510	Total both sexes																
Medical records and health information technicians 3510	Number	110 065	8 355	5 730	68 155	19 135	1 700	5 475	160	315	365	270	120	(X)	(X)	(X)	285
Medical records and health information technicians 3510	Percent	100.0%	7.6%	5.2%	61.9%	17.4%	1.5%	5.0%	0.1%	0.3%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.3%
Medical records and health information technicians 3510	Male																
Medical records and health information technicians 3510	Number	11 415	1 070	645	5 385	2 485	195	1 485	0	30	0	30	65	(X)	(X)	(X)	25
Medical records and health information technicians 3510	Percent	10.4%	1.0%	0.6%	4.9%	2.3%	0.2%	1.3%	0.0%	0.0%	0.0%	0.0%	0.1%	(X)	(X)	(X)	0.0%
Medical records and health information technicians 3510	Female																
Medical records and health information technicians 3510	Number	98 650	7 280	5 085	62 770	16 650	1 505	3 990	160	285	365	240	55	(X)	(X)	(X)	260
Medical records and health information technicians 3510	Percent	89.6%	6.6%	4.6%	57.0%	15.1%	1.4%	3.6%	0.1%	0.3%	0.3%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Opticians dispensing 3520 (SOC 29-2081)	Total both sexes																
Opticians dispensing 3520 (SOC 29-2081)	Number	52 960	3 710	2 095	40 875	3 250	270	1 690	30	145	170	225	140	(X)	(X)	(X)	355
Opticians dispensing 3520 (SOC 29-2081)	Percent	100.0%	7.0%	4.0%	77.2%	6.1%	0.5%	3.2%	0.1%	0.3%	0.3%	0.4%	0.3%	(X)	(X)	(X)	0.7%
Opticians, dispensing 3520 (SOC 29-2081)	Male																
Opticians dispensing 3520 (SOC 29-2081)	Number	15 820	1 195	710	12 280	765	60	540	0	20	35	60	30	(X)	(X)	(X)	125
Opticians dispensing 3520 (SOC 29-2081)	Percent	29.9%	2.3%	1.3%	23.2%	1.4%	0.1%	1.0%	0.0%	0.0%	0.1%	0.1%	0.1%	(X)	(X)	(X)	0.2%
Opticians, dispensing 3520 (SOC 29-2081)	Female																
Opticians dispensing 3520 (SOC 29-2081)	Number	37 140	2 515	1 385	28 600	2 485	210	1 150	30	130	135	165	110	(X)	(X)	(X)	230
Opticians dispensing 3520 (SOC 29-2081)	Percent	70.1%	4.7%	2.6%	54.0%	4.7%	0.4%	2.2%	0.1%	0.2%	0.3%	0.3%	0.2%	(X)	(X)	(X)	0.4%
Miscellaneous health technologists and technicians 3535	Total both sexes																
Miscellaneous health technologists and technicians 3535	Number	123 560	6 825	4 665	74 855	25 545	925	8 515	135	245	405	490	190	(X)	(X)	(X)	760
Miscellaneous health technologists and technicians 3535	Percent	100.0%	5.5%	3.8%	60.6%	20.7%	0.7%	6.9%	0.1%	0.2%	0.3%	0.4%	0.2%	(X)	(X)	(X)	0.6%
Miscellaneous health technologists and technicians 3535	Male																
Miscellaneous health technologists and technicians 3535	Number	41 955	2 390	1 775	26 005	6 810	160	4 085	4	85	115	230	35	(X)	(X)	(X)	250
Miscellaneous health technologists and technicians 3535	Percent	34.0%	1.9%	1.4%	21.0%	5.5%	0.1%	3.3%	0.0%	0.1%	0.1%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Miscellaneous health technologists and technicians 3535	Female																
Miscellaneous health technologists and technicians 3535	Number	81 605	4 435	2 895	48 850	18 735	765	4 430	125	160	290	265	155	(X)	(X)	(X)	505
Miscellaneous health technologists and technicians 3535	Percent	66.0%	3.6%	2.3%	39.5%	15.2%	0.6%	3.6%	0.1%	0.1%	0.2%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Other healthcare practitioners and technical occupations	Total both sexes																
Other healthcare practitioners and technical occupations	Number	73 480	3 755	2 270	55 270	7 775	590	2 575	55	65	320	315	15	(X)	(X)	(X)	465
Other healthcare practitioners and technical occupations	Percent	100.0%	5.1%	3.1%	75.2%	10.6%	0.8%	3.5%	0.1%	0.1%	0.4%	0.4%	0.0%	(X)	(X)	(X)	0.6%
Other healthcare practitioners and technical occupations	Male																
Other healthcare practitioners and technical occupations	Number	42 730	2 210	1 535	31 945	4 490	340	1 480	45	35	170	235	15	(X)	(X)	(X)	240
Other healthcare practitioners and technical occupations	Percent	58.2%	3.0%	2.1%	43.5%	6.1%	0.5%	2.0%	0.1%	0.0%	0.2%	0.3%	0.0%	(X)	(X)	(X)	0.3%
Other healthcare practitioners and technical occupations	Female																
Other healthcare practitioners and technical occupations	Number	30 750	1 550	735	23 325	3 290	250	1 100	10	30	150	85	0	(X)	(X)	(X)	225
Other healthcare practitioners and technical occupations	Percent	41.8%	2.1%	1.0%	31.7%	4.5%	0.3%	1.5%	0.0%	0.0%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Nursing psychiatric and home health aides 3600 (SOC	Total both sexes																
Nursing, psychiatric, and home health aides 3600 (SOC	Number	2,207,375	152,920	128,915	1,040,750	730,795	19,805	90,410	4,495	7,195	10,795	3,295	3,965	(X)	(X)	(X)	14,040
Nursing psychiatric and home health aides 3600 (SOC	Percent	100.0%	6.9%	5.8%	47.1%	33.1%	0.9%	4.1%	0.2%	0.3%	0.5%	0.1%	0.2%	(X)	(X)	(X)	0.6%
Nursing psychiatric and home health aides 3600 (SOC	Male																
Nursing, psychiatric, and home health aides 3600 (SOC	Number	265,755	18,790	14,010	123,405	80,735	2,300	20,075	750	905	1,340	695	780	(X)	(X)	(X)	1,970
Nursing psychiatric and home health aides 3600 (SOC	Percent	12.0%	0.9%	0.6%	5.6%	3.7%	0.1%	0.9%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Nursing psychiatric and home health aides 3600 (SOC	Female																
Nursing psychiatric and home health aides 3600 (SOC	Number	1 941 620	134 130	114 905	917 345	650 060	17 505	70 335	3 745	6 290	9 450	2 605	3 185	(X)	(X)	(X)	12 065
Nursing psychiatric and home health aides 3600 (SOC	Percent	88.0%	6.1%	5.2%	41.6%	29.4%	0.8%	3.2%	0.2%	0.3%	0.4%	0.1%	0.1%	(X)	(X)	(X)	0.5%
Occupational therapy assistants and aides 3610 (SOC 31-	Total both sexes																
Occupational therapy assistants and aides 3610 (SOC 31-	Number	13 580	710	350	10 515	1 295	55	480	20	55	10	25	35	(X)	(X)	(X)	30
Occupational therapy assistants and aides 3610 (SOC 31-	Percent	100.0%	5.2%	2.6%	77.4%	9.5%	0.4%	3.5%	0.1%	0.4%	0.1%	0.2%	0.3%	(X)	(X)	(X)	0.2%
Occupational therapy assistants and aides 3610 (SOC 31-	Male																
Occupational therapy assistants and aides 3610 (SOC 31-	Number	1 175	170	60	855	40	4	25	0	0	0	15	0	(X)	(X)	(X)	0
Occupational therapy assistants and aides 3610 (SOC 31-	Percent	8.7%	1.3%	0.4%	6.3%	0.3%	0.0%	0.2%	0.0%	0.0%	0.0%	0.1%	0.0%	(X)	(X)	(X)	0.0%
Occupational therapy assistants and aides 3610 (SOC 31-	Female																
Occupational therapy assistants and aides 3610 (SOC 31-	Number	12 405	540	290	9 660	1 255	50	450	20	55	10	4	35	(X)	(X)	(X)	30
Occupational therapy assistants and aides 3610 (SOC 31-	Percent	91.3%	4.0%	2.1%	71.1%	9.2%	0.4%	3.3%	0.1%	0.4%	0.1%	0.0%	0.3%	(X)	(X)	(X)	0.2%
Physical therapist assistants and aides 3620 (SOC 31-	Total both sexes																
Physical therapist assistants and aides 3620 (SOC 31-	Number	67 410	4 300	2 360	49 845	6 255	285	3 350	205	135	280	140	15	(X)	(X)	(X)	230
Physical therapist assistants and aides 3620 (SOC 31-	Percent	100.0%	6.4%	3.5%	73.9%	9.3%	0.4%	5.0%	0.3%	0.2%	0.4%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Physical therapist assistants and aides 3620 (SOC 31-	Male																
Physical therapist assistants and aides 3620 (SOC 31-	Number	17 200	1 555	795	11 045	1 645	85	1 730	100	50	70	35	15	(X)	(X)	(X)	75
Physical therapist assistants and aides 3620 (SOC 31-	Percent	25.5%	2.3%	1.2%	16.4%	2.4%	0.1%	2.6%	0.1%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Physical therapist assistants and aides 3620 (SOC 31-	Female																
Physical therapist assistants and aides 3620 (SOC 31-	Number	50 215	2 750	1 570	38 805	4 610	200	1 620	110	85	210	100	0	(X)	(X)	(X)	155
Physical therapist assistants and aides 3620 (SOC 31-	Percent	74.5%	4.1%	2.3%	57.6%	6.8%	0.3%	2.4%	0.2%	0.1%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Massage therapists 3630 (SOC 31-9011)	Total both sexes																
Massage therapists 3630 (SOC 31-9011)	Number	133 790	7 140	4 580	105 140	5 445	655	7 150	175	510	945	760	230	(X)	(X)	(X)	1 060
Massage therapists 3630 (SOC 31-9011)	Percent	100.0%	5.3%	3.4%	78.6%	4.1%	0.5%	5.3%	0.1%	0.4%	0.7%	0.6%	0.2%	(X)	(X)	(X)	0.8%
Massage therapists 3630 (SOC 31-9011)	Male																
Massage therapists 3630 (SOC 31-9011)	Number	22 300	1 750	1 055	15 495	1 055	115	2 200	55	30	150	155	20	(X)	(X)	(X)	225
Massage therapists 3630 (SOC 31-9011)	Percent	16.7%	1.3%	0.8%	11.6%	0.8%	0.1%	1.6%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Massage therapists 3630 (SOC 31-9011)	Female																
Massage therapists 3630 (SOC 31-9011)	Number	111 490	5 390	3 525	89 645	4 390	540	4 945	120	480	800	605	210	(X)	(X)	(X)	835
Massage therapists 3630 (SOC 31-9011)	Percent	83.3%	4.0%	2.6%	67.0%	3.3%	0.4%	3.7%	0.1%	0.4%	0.6%	0.5%	0.2%	(X)	(X)	(X)	0.6%
Dental assistants 3640 (SOC 31-9091)	Total both sexes																
Dental assistants 3640 (SOC 31-9091)	Number	275 095	30 835	21 970	185 685	16 695	2 125	13 205	530	500	1 385	790	105	(X)	(X)	(X)	1 270
Dental assistants 3640 (SOC 31-9091)	Percent	100.0%	11.2%	8.0%	67.5%	6.1%	0.8%	4.8%	0.2%	0.2%	0.5%	0.3%	0.0%	(X)	(X)	(X)	0.5%

Dental assistants 3640 (SOC 31-9091)	Male																
Dental assistants 3640 (SOC 31-9091)	Number	10 140	1 905	1 490	3 470	1 000	110	2 000	0	35	40	15	4	(X)	(X)	(X)	70
Dental assistants 3640 (SOC 31-9091)	Percent	3.7%	0.7%	0.5%	1.3%	0.4%	0.0%	0.7%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Dental assistants 3640 (SOC 31-9091)	Female																
Dental assistants 3640 (SOC 31-9091)	Number	264 960	28 925	20 480	182 215	15 700	2 015	11 205	530	465	1 345	775	105	(X)	(X)	(X)	1 200
Dental assistants 3640 (SOC 31-9091)	Percent	96.3%	10.5%	7.4%	66.2%	5.7%	0.7%	4.1%	0.2%	0.2%	0.5%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Medical assistants 3645 (SOC 31-9092)	Total, both sexes																
Medical assistants 3645 (SOC 31-9092)	Number	393 055	51 650	39 680	222 760	53 510	2 035	16 000	1 265	1 015	1 625	870	185	(X)	(X)	(X)	2 460
Medical assistants 3645 (SOC 31-9092)	Percent	100.0%	13.1%	10.1%	56.7%	13.6%	0.5%	4.1%	0.3%	0.3%	0.4%	0.2%	0.0%	(X)	(X)	(X)	0.6%
Medical assistants 3645 (SOC 31-9092)	Male																
Medical assistants 3645 (SOC 31-9092)	Number	23 845	3 965	2 145	11 090	3 920	115	1 815	130	95	140	135	0	(X)	(X)	(X)	295
Medical assistants 3645 (SOC 31-9092)	Percent	6.1%	1.0%	0.5%	2.8%	1.0%	0.0%	0.5%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Medical assistants 3645 (SOC 31-9092)	Female																
Medical assistants 3645 (SOC 31-9092)	Number	369 210	47 685	37 540	211 670	49 590	1 920	14 190	1 135	920	1 480	730	185	(X)	(X)	(X)	2 160
Medical assistants 3645 (SOC 31-9092)	Percent	93.9%	12.1%	9.6%	53.9%	12.6%	0.5%	3.6%	0.3%	0.2%	0.4%	0.2%	0.0%	(X)	(X)	(X)	0.5%
Medical transcriptionists 3646 (SOC 31-9094)	Total, both sexes																
Medical transcriptionists 3646 (SOC 31-9094)	Number	78 065	2 365	1 170	68 980	3 305	180	995	85	125	505	140	35	(X)	(X)	(X)	175
Medical transcriptionists 3646 (SOC 31-9094)	Percent	100.0%	3.0%	1.5%	88.4%	4.2%	0.2%	1.3%	0.1%	0.2%	0.6%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Medical transcriptionists 3646 (SOC 31-9094)	Male																
Medical transcriptionists 3646 (SOC 31-9094)	Number	1 830	35	0	1 570	110	0	115	0	0	0	0	0	(X)	(X)	(X)	0
Medical transcriptionists 3646 (SOC 31-9094)	Percent	2.3%	0.0%	0.0%	2.0%	0.1%	0.0%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Medical transcriptionists 3646 (SOC 31-9094)	Female																
Medical transcriptionists 3646 (SOC 31-9094)	Number	76 230	2 330	1 170	67 410	3 200	180	880	85	125	505	140	35	(X)	(X)	(X)	175
Medical transcriptionists 3646 (SOC 31-9094)	Percent	97.6%	3.0%	1.5%	86.4%	4.1%	0.2%	1.1%	0.1%	0.2%	0.6%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Pharmacy aides 3647 (SOC 31-9095)	Total, both sexes																
Pharmacy aides 3647 (SOC 31-9095)	Number	43,825	4,635	2,790	25,795	5,490	200	4,250	90	60	140	65	85	(X)	(X)	(X)	235
Pharmacy aides 3647 (SOC 31-9095)	Percent	100.0%	10.6%	6.4%	58.9%	12.5%	0.5%	9.7%	0.2%	0.1%	0.3%	0.1%	0.2%	(X)	(X)	(X)	0.5%
Pharmacy aides 3647 (SOC 31-9095)	Male																
Pharmacy aides 3647 (SOC 31-9095)	Number	10,155	1,190	510	5,140	1,195	45	1,885	0	25	40	45	10	(X)	(X)	(X)	65
Pharmacy aides 3647 (SOC 31-9095)	Percent	23.2%	2.7%	1.2%	11.7%	2.7%	0.1%	4.3%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Pharmacy aides 3647 (SOC 31-9095)	Female																
Pharmacy aides 3647 (SOC 31-9095)	Number	33 665	3 440	2 280	20 655	4 295	155	2 365	90	35	100	20	70	(X)	(X)	(X)	165
Pharmacy aides 3647 (SOC 31-9095)	Percent	76.8%	7.8%	5.2%	47.1%	9.8%	0.4%	5.4%	0.2%	0.1%	0.2%	0.0%	0.2%	(X)	(X)	(X)	0.4%
Veterinary assistants and laboratory animal caretakers	Total, both sexes																
Veterinary assistants and laboratory animal caretakers	Number	43 690	2 490	1 445	35 835	2 220	150	745	20	140	260	165	20	(X)	(X)	(X)	200
Veterinary assistants and laboratory animal caretakers	Percent	100.0%	5.7%	3.3%	82.0%	5.1%	0.3%	1.7%	0.0%	0.3%	0.6%	0.4%	0.0%	(X)	(X)	(X)	0.5%
Veterinary assistants and laboratory animal caretakers	Male																
Veterinary assistants and laboratory animal caretakers	Number	8 745	1 070	495	5 585	1 095	35	345	0	30	15	35	20	(X)	(X)	(X)	20
Veterinary assistants and laboratory animal caretakers	Percent	20.0%	2.4%	1.1%	12.8%	2.5%	0.1%	0.8%	0.0%	0.1%	0.0%	0.1%	0.0%	(X)	(X)	(X)	0.0%
Veterinary assistants and laboratory animal caretakers	Female																
Veterinary assistants and laboratory animal caretakers	Number	34 945	1 420	950	30 250	1 125	115	400	20	115	245	130	0	(X)	(X)	(X)	175
Veterinary assistants and laboratory animal caretakers	Percent	80.0%	3.3%	2.2%	69.2%	2.6%	0.3%	0.9%	0.0%	0.3%	0.6%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Phlebotomists 3649 (SOC 31-9097)	Total, both sexes																
Phlebotomists 3649 (SOC 31-9097)	Number	88 335	7 970	5 065	51 600	17 575	550	3 845	165	275	670	195	40	(X)	(X)	(X)	380
Phlebotomists 3649 (SOC 31-9097)	Percent	100.0%	9.0%	5.7%	58.4%	19.9%	0.6%	4.4%	0.2%	0.3%	0.8%	0.2%	0.0%	(X)	(X)	(X)	0.4%
Phlebotomists 3649 (SOC 31-9097)	Male																
Phlebotomists 3649 (SOC 31-9097)	Number	11 680	980	740	6 765	1 825	25	1 070	20	45	90	30	0	(X)	(X)	(X)	90
Phlebotomists 3649 (SOC 31-9097)	Percent	13.2%	1.1%	0.8%	7.7%	2.1%	0.0%	1.2%	0.0%	0.1%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Phlebotomists 3649 (SOC 31-9097)	Female																
Phlebotomists 3649 (SOC 31-9097)	Number	76 650	6 985	4 325	44 835	15 750	525	2 775	150	230	580	165	40	(X)	(X)	(X)	290
Phlebotomists 3649 (SOC 31-9097)	Percent	86.8%	7.9%	4.9%	50.8%	17.8%	0.6%	3.1%	0.2%	0.3%	0.7%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Healthcare support workers, all other, including medical	Total, both sexes																
Healthcare support workers, all other, including medical	Number	154 475	10 050	7 280	87 650	38 695	980	6 865	355	520	660	345	245	(X)	(X)	(X)	830
Healthcare support workers, all other, including medical	Percent	100.0%	6.5%	4.7%	56.7%	25.0%	0.6%	4.4%	0.2%	0.3%	0.4%	0.2%	0.2%	(X)	(X)	(X)	0.5%
Healthcare support workers, all other, including medical	Male																
Healthcare support workers, all other, including medical	Number	36 300	2 570	1 930	17 865	10 320	165	2 665	60	170	85	140	4	(X)	(X)	(X)	330
Healthcare support workers, all other, including medical	Percent	23.5%	1.7%	1.2%	11.6%	6.7%	0.1%	1.7%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Healthcare support workers, all other, including medical	Female																
Healthcare support workers, all other, including medical	Number	118 170	7 485	5 350	69 785	28 375	815	4 200	300	345	575	205	240	(X)	(X)	(X)	500
Healthcare support workers, all other, including medical	Percent	76.5%	4.8%	3.5%	45.2%	18.4%	0.5%	2.7%	0.2%	0.2%	0.4%	0.1%	0.2%	(X)	(X)	(X)	0.3%
First-line supervisors of correctional officers 3700 (SOC	Total, both sexes																
First-line supervisors of correctional officers 3700 (SOC	Number	58 265	2 980	1 935	37 670	13 890	485	470	35	75	340	110	80	(X)	(X)	(X)	195
First-line supervisors of correctional officers 3700 (SOC	Percent	100.0%	5.1%	3.3%	64.7%	23.8%	0.8%	0.8%	0.1%	0.1%	0.6%	0.2%	0.1%	(X)	(X)	(X)	0.3%
First-line supervisors of correctional officers 3700 (SOC	Male																
First-line supervisors of correctional officers 3700 (SOC	Number	42 685	2 175	1 485	29 115	8 755	285	370	35	25	205	80	10	(X)	(X)	(X)	150
First-line supervisors of correctional officers 3700 (SOC	Percent	73.3%	3.7%	2.5%	50.0%	15.0%	0.5%	0.6%	0.1%	0.0%	0.4%	0.1%	0.0%	(X)	(X)	(X)	0.3%
First-line supervisors of correctional officers 3700 (SOC	Female																
First-line supervisors of correctional officers 3700 (SOC	Number	15 580	805	450	8 560	5 135	200	100	0	50	135	30	70	(X)	(X)	(X)	45
First-line supervisors of correctional officers 3700 (SOC	Percent	26.7%	1.4%	0.8%	14.7%	8.8%	0.3%	0.2%	0.0%	0.1%	0.2%	0.1%	0.1%	(X)	(X)	(X)	0.1%
First-line supervisors of police and detectives 3710 (SOC	Total, both sexes																
First-line supervisors of police and detectives 3710 (SOC	Number	119 270	6 405	2 935	92 620	13 565	790	1 275	135	165	505	385	115	(X)	(X)	(X)	370
First-line supervisors of police and detectives 3710 (SOC	Percent	100.0%	5.4%	2.5%	77.7%	11.4%	0.7%	1.1%	0.1%	0.1%	0.4%	0.3%	0.1%	(X)	(X)	(X)	0.3%
First-line supervisors of police and detectives 3710 (SOC	Male																
First-line supervisors of police and detectives 3710 (SOC	Number	100 530	5 385	2 185	80 665	9 215	660	1 010	125	120	415	305	115	(X)	(X)	(X)	325
First-line supervisors of police and detectives 3710 (SOC	Percent	84.3%	4.5%	1.8%	67.6%	7.7%	0.6%	0.8%	0.1%	0.1%	0.3%	0.3%	0.1%	(X)	(X)	(X)	0.3%
First-line supervisors of police and detectives 3710 (SOC	Female																
First-line supervisors of police and detectives 3710 (SOC	Number	18 740	1 020	750	11 955	4 350	135	265	10	45	85	80	0	(X)	(X)	(X)	45
First-line supervisors of police and detectives 3710 (SOC	Percent	15.7%	0.9%	0.6%	10.0%	3.6%	0.1%	0.2%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.0%
First-line supervisors of fire fighting and prevention	Total, both sexes																
First-line supervisors of fire fighting and prevention	Number	53 010	1 840	765	44 965	3 575	645	360	140	90	265	125	0	(X)	(X)	(X)	235
First-line supervisors of fire fighting and prevention	Percent	100.0%	3.5%	1.4%	84.8%	6.7%	1.2%	0.7%	0.3%	0.2%	0.5%	0.2%	0.0%	(X)	(X)	(X)	0.4%
First-line supervisors of fire fighting and prevention	Male																
First-line supervisors of fire fighting and prevention	Number	51 035	1 810	710	43 540	3 285	580	360	130	90	190	110	0	(X)	(X)	(X)	225
First-line supervisors of fire fighting and prevention	Percent	96.3%	3.4%	1.3%	82.1%	6.2%	1.1%	0.7%	0.2%	0.2%	0.4%	0.2%	0.0%	(X)	(X)	(X)	0.4%
First-line supervisors of fire fighting and prevention	Female																
First-line supervisors of fire fighting and prevention	Number	1 975	30	50	1 425	295	65	0	10	0	80	15	0	(X)	(X)	(X)	10
First-line supervisors of fire fighting and prevention	Percent	3.7%	0.1%	0.1%	2.7%	0.6%	0.1%	0.0%	0.0%	0.0%	0.2%	0.0%	0.0%	(X)	(X)	(X)	0.0%
First-line supervisors of protective service workers, all	Total, both sexes																
First-line supervisors of protective service workers, all	Number	94 325	5 750	4 025	61 085	18 950	815	1 940	300	200	325	240	140	(X)	(X)	(X)	555
First-line supervisors of protective service workers, all	Percent	100.0%	6.1%	4.3%	64.8%	20.1%	0.9%	2.1%	0.3%	0.2%	0.3%	0.3%	0.1%	(X)	(X)	(X)	0.6%
First-line supervisors of protective service workers, all	Male																
First-line supervisors of protective service workers, all	Number	71 355	4 460	3 110	47 325	13 060	575	1 420	255	180	260	185	105	(X)	(X)	(X)	420
First-line supervisors of protective service workers, all	Percent	75.6%	4.7%	3.3%	50.2%	13.8%	0.6%	1.5%	0.3%	0.2%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.4%
First-line supervisors of protective service workers, all	Female																
First-line supervisors of protective service workers, all	Number	22 970	1 290	915	13 760	5 890	235	520	45	20	65	55	35	(X)	(X)	(X)	135
First-line supervisors of protective service workers, all	Percent	24.4%	1.4%	1.0%	14.6%	6.2%	0.2%	0.6%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Firefighters 3740 (SOC 33-2011)	Total, both sexes																
Firefighters 3740 (SOC 33-2011)	Number	276 860	15 195	8 220	219 550	22 600	3 590	3 120	335	555	1 445	730	230	(X)	(X)	(X)	1 295
Firefighters 3740 (SOC 33-2011)	Percent	100.0%	5.5%	3.0%	79.3%	8.2%	1.3%	1.1%	0.1%	0.2%	0.5%	0.3%	0.1%	(X)	(X)	(X)	0.5%
Firefighters 3740 (SOC 33-2011)	Male																
Firefighters 3740 (SOC 33-2011)	Number	265,545	14,720	7,945	210,645	21,560	3,265	3,070	310	555	1,340	685	230	(X)	(X)	(X)	1,225
Firefighters 3740 (SOC 33-2011)	Percent	95.9%	5.3%	2.9%	76.1%	7.8%	1.2%	1.1%	0.1%	0.2%	0.5%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Firefighters 3740 (SOC 33-2011)	Female																
Firefighters 3740 (SOC 33-2011)	Number	11,315	470	275	8,905	1,035	330	50	25	0	105	50	0	(X)	(X)	(X)	70
Firefighters 3740 (SOC 33-2011)	Percent	4.1%	0.2%	0.1%	3.2%	0.4%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Fire inspectors 3750 (SOC 33-2020)	Total, both sexes																
Fire inspectors 3750 (SOC 33-2020)	Number	20 025	960	625	16 120	1 520	225	240	10	30	175	40	4	(X)	(X)	(X)	65
Fire inspectors 3750 (SOC 33-2020)	Percent	100.0%	4.8%	3.1%	80.5%	7.6%	1.1%	1.2%	0.0%	0.1%	0.9%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Fire inspectors 3750 (SOC 33-2020)	Male																
Fire inspectors 3750 (SOC 33-2020)	Number	17 935	945	515	14 450	1 395	175	200	10	30	135	10	4	(X)	(X)	(X)	65
Fire inspectors 3750 (SOC 33-2020)	Percent	89.6%	4.7%	2.6%	72.2%	7.0%	0.9%	1.0%	0.0%	0.1%	0.7%	0.0%	0.0%	(X)	(X)	(X)	0.3%
Fire inspectors 3750 (SOC 33-2020)	Female																
Fire inspectors 3750 (SOC 33-2020)	Number	2 090	15	105	1 670	125	50	45	0	0	40	30	0	(X)	(X)	(X)	0
Fire inspectors 3750 (SOC 33-2020)	Percent	10.4%	0.1%	0.5%	8.3%	0.6%	0.2%	0.2%	0.0%	0.0%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.0%
Bailiffs, correctional officers, and jailers 3800 (SOC 33-	Total, both sexes																
Bailiffs, correctional officers, and jailers 3800 (SOC 33-	Number	441 185	30 725	19 645	272 285	103 730	3 895	4 150	910	795	1 800	965	570	(X)	(X)	(X)	1 710
Bailiffs, correctional officers, and jailers 3800 (SOC 33-	Percent	100.0%	7.0%	4.5%	61.7%	23.5%	0.9%	0.9%	0.2%	0.2%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Bailiffs, correctional officers, and jailers 3800 (SOC 33-	Male																
Bailiffs, correctional officers, and jailers 3800 (SOC 33-	Number	316 085	22 950	14 425	212 600	55 490	2 505	3 250	795	525	1 345	690	385	(X)	(X)	(X)	1 125
Bailiffs, correctional officers, and jailers 3800 (SOC 33-	Percent	71.6%	5.2%	3.3%	48.2%	12.6%	0.6%	0.7%	0.2%	0.1%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.3%
Bailiffs, correctional officers, and jailers 3800 (SOC 33-	Female																
Bailiffs, correctional officers, and jailers 3800 (SOC 33-	Number	125 100	7 775	5 220	59 685	48 240	1 390	905	115	270	455	280	185	(X)	(X)	(X)	585
Bailiffs, correctional officers, and jailers 3800 (SOC 33-	Percent	28.4%	1.8%	1.2%	13.5%	10.9%	0.3%	0.2%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Detectives and criminal investigators 3820 (SOC 33-3021)	Total, both sexes																
Detectives and criminal investigators 3820 (SOC 33-3021)	Number	131 215	9 985	4 860	95 830	15 355	1 000	2 250	140	180	420	535	110	(X)	(X)	(X)	550
Detectives and criminal investigators 3820 (SOC 33-3021)	Percent	100.0%	7.6%	3.7%	73.0%	11.7%	0.8%	1.7%	0.1%	0.1%	0.3%	0.4%	0.1%	(X)	(X)	(X)	0.4%
Detectives and criminal investigators 3820 (SOC 33-3021)	Male																
Detectives and criminal investigators 3820 (SOC 33-3021)	Number	100 170	7 535	3 330	75 770	9 695	725	1 740	95	150	320	355	70	(X)	(X)	(X)	390
Detectives and criminal investigators 3820 (SOC 33-3021)	Percent	76.3%	5.7%	2.5%	57.7%	7.4%	0.6%	1.3%	0.1%	0.1%	0.2%	0.3%	0.1%	(X)	(X)	(X)	0.3%
Detectives and criminal investigators 3820 (SOC 33-3021)	Female																
Detectives and criminal investigators 3820 (SOC 33-3021)	Number	31 045	2 450	1 530	20 060	5 660	275	510	45	35	100	180	40	(X)	(X)	(X)	165
Detectives and criminal investigators 3820 (SOC 33-3021)	Percent	23.7%	1.9%	1.2%	15.3%	4.3%	0.2%	0.4%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Miscellaneous law enforcement workers 3840 (SOC 33-	Total, both sexes																
Miscellaneous law enforcement workers 3840 (SOC 33-	Number	11 530	930	455	7 105	2 075	235	420	4	60	135	30	35	(X)	(X)	(X)	45
Miscellaneous law enforcement workers 3840 (SOC 33-	Percent	100.0%	8.1%	3.9%	61.6%	18.0%	2.0%	3.6%	0.0%	0.5%	1.2%	0.3%	0.3%	(X)	(X)	(X)	0.4%
Miscellaneous law enforcement workers 3840 (SOC 33-	Male																
Miscellaneous law enforcement workers 3840 (SOC 33-	Number	8 005	630	355	5 140	1 140	210	320	4	40	100	30	15	(X)	(X)	(X)	20
Miscellaneous law enforcement workers 3840 (SOC 33-	Percent	69.4%	5.5%	3.1%	44.6%	9.9%	1.8%	2.8%	0.0%	0.3%	0.9%	0.3%	0.1%	(X)	(X)	(X)	0.2%

Miscellaneous law enforcement workers 3840 (SOC 33-	Female																
Miscellaneous law enforcement workers 3840 (SOC 33-	Number	3 525	300	100	1 965	935	25	100	4	20	35	0	20	(X)	(X)	(X)	25
Miscellaneous law enforcement workers 3840 (SOC 33-	Percent	30.6%	2.6%	0.9%	17.0%	8.1%	0.2%	0.9%	0.0%	0.2%	0.3%	0.0%	0.2%	(X)	(X)	(X)	0.2%
Police officers 3850 (SOC 33-3050)	Total, both sexes																
Police officers 3850 (SOC 33-3050)	Number	663 600	55 125	27 565	469 535	81 985	4 315	13 260	1 415	1 475	2 485	1 885	660	(X)	(X)	(X)	3 900
Police officers 3850 (SOC 33-3050)	Percent	100.0%	8.3%	4.2%	70.8%	12.4%	0.7%	2.0%	0.2%	0.2%	0.4%	0.3%	0.1%	(X)	(X)	(X)	0.6%
Police officers 3850 (SOC 33-3050)	Male																
Police officers 3850 (SOC 33-3050)	Number	565 100	45 730	22 320	412 960	58 630	3 680	11 845	1 300	1 205	2 155	1 570	560	(X)	(X)	(X)	3 145
Police officers 3850 (SOC 33-3050)	Percent	85.2%	6.9%	3.4%	62.2%	8.8%	0.6%	1.8%	0.2%	0.2%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.5%
Police officers 3850 (SOC 33-3050)	Female																
Police officers 3850 (SOC 33-3050)	Number	98 500	9 395	5 245	56 575	23 350	635	1 415	115	270	325	320	100	(X)	(X)	(X)	755
Police officers 3850 (SOC 33-3050)	Percent	14.8%	1.4%	0.8%	8.5%	3.5%	0.1%	0.2%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Animal control workers 3900 (SOC 33-9011)	Total, both sexes																
Animal control workers 3900 (SOC 33-9011)	Number	10 770	795	330	8 705	645	110	35	0	0	125	15	0	(X)	(X)	(X)	10
Animal control workers 3900 (SOC 33-9011)	Percent	100.0%	7.4%	3.1%	80.8%	6.0%	1.0%	0.3%	0.0%	0.0%	1.2%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Animal control workers 3900 (SOC 33-9011)	Male																
Animal control workers 3900 (SOC 33-9011)	Number	6 545	585	165	5 035	575	75	35	0	0	45	15	0	(X)	(X)	(X)	10
Animal control workers 3900 (SOC 33-9011)	Percent	60.8%	5.4%	1.5%	46.8%	5.3%	0.7%	0.3%	0.0%	0.0%	0.4%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Animal control workers 3900 (SOC 33-9011)	Female																
Animal control workers 3900 (SOC 33-9011)	Number	4 225	210	165	3 665	70	35	0	0	0	80	0	0	(X)	(X)	(X)	0
Animal control workers 3900 (SOC 33-9011)	Percent	39.2%	1.9%	1.5%	34.0%	0.6%	0.3%	0.0%	0.0%	0.0%	0.7%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Private detectives and investigators 3910 (SOC 33-9021)	Total, both sexes																
Private detectives and investigators 3910 (SOC 33-9021)	Number	86 635	6 530	3 840	60 520	11 185	675	2 020	230	155	520	405	25	(X)	(X)	(X)	530
Private detectives and investigators 3910 (SOC 33-9021)	Percent	100.0%	7.5%	4.4%	69.9%	12.9%	0.8%	2.3%	0.3%	0.2%	0.6%	0.5%	0.0%	(X)	(X)	(X)	0.6%
Private detectives and investigators 3910 (SOC 33-9021)	Male																
Private detectives and investigators 3910 (SOC 33-9021)	Number	52,175	3,985	2,260	37,450	5,805	255	1,220	125	100	380	280	15	(X)	(X)	(X)	305
Private detectives and investigators 3910 (SOC 33-9021)	Percent	60.2%	4.6%	2.6%	43.2%	6.7%	0.3%	1.4%	0.1%	0.1%	0.4%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Private detectives and investigators 3910 (SOC 33-9021)	Female																
Private detectives and investigators 3910 (SOC 33-9021)	Number	34,455	2,545	1,575	23,070	5,380	425	800	105	60	140	125	10	(X)	(X)	(X)	225
Private detectives and investigators 3910 (SOC 33-9021)	Percent	39.8%	2.9%	1.8%	26.6%	6.2%	0.5%	0.9%	0.1%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Security guards and gaming surveillance officers 3930	Total, both sexes																
Security guards and gaming surveillance officers 3930	Number	1 014 210	84 120	62 135	508 560	290 495	10 610	31 825	4 925	3 455	4 950	2 935	1 665	(X)	(X)	(X)	8 525
Security guards and gaming surveillance officers 3930	Percent	100.0%	8.3%	6.1%	50.1%	28.6%	1.0%	3.1%	0.5%	0.3%	0.5%	0.3%	0.2%	(X)	(X)	(X)	0.8%
Security guards and gaming surveillance officers 3930	Male																
Security guards and gaming surveillance officers 3930	Number	787 525	68 255	49 635	413 760	201 230	7 610	26 985	3 475	2 810	3 665	2 410	1 215	(X)	(X)	(X)	6 480
Security guards and gaming surveillance officers 3930	Percent	77.6%	6.7%	4.9%	40.8%	19.8%	0.8%	2.7%	0.3%	0.3%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.6%
Security guards and gaming surveillance officers 3930	Female																
Security guards and gaming surveillance officers 3930	Number	226 685	15 865	12 500	94 805	89 265	3 000	4 840	1 455	650	1 285	530	450	(X)	(X)	(X)	2 050
Security guards and gaming surveillance officers 3930	Percent	22.4%	1.6%	1.2%	9.3%	8.8%	0.3%	0.5%	0.1%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Crossing guards 3940 (SOC 33-9091)	Total, both sexes																
Crossing guards 3940 (SOC 33-9091)	Number	60 090	5 470	3 215	36 580	12 580	675	720	35	135	330	45	105	(X)	(X)	(X)	205
Crossing guards 3940 (SOC 33-9091)	Percent	100.0%	9.1%	5.4%	60.9%	20.9%	1.1%	1.2%	0.1%	0.2%	0.5%	0.1%	0.2%	(X)	(X)	(X)	0.3%
Crossing guards 3940 (SOC 33-9091)	Male																
Crossing guards 3940 (SOC 33-9091)	Number	24 170	2 545	1 230	14 880	4 365	350	395	4	100	105	45	20	(X)	(X)	(X)	135
Crossing guards 3940 (SOC 33-9091)	Percent	40.2%	4.2%	2.0%	24.8%	7.3%	0.6%	0.7%	0.0%	0.2%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Crossing guards 3940 (SOC 33-9091)	Female																
Crossing guards 3940 (SOC 33-9091)	Number	35 920	2 930	1 985	21 695	8 215	325	330	30	35	225	0	85	(X)	(X)	(X)	70
Crossing guards 3940 (SOC 33-9091)	Percent	59.8%	4.9%	3.3%	36.1%	13.7%	0.5%	0.5%	0.0%	0.1%	0.4%	0.0%	0.1%	(X)	(X)	(X)	0.1%
Transportation security screeners 3945 (SOC 33-9093)	Total, both sexes																
Transportation security screeners 3945 (SOC 33-9093)	Number	27 210	2 520	1 660	13 700	6 900	150	1 515	170	95	85	85	0	(X)	(X)	(X)	325
Transportation security screeners 3945 (SOC 33-9093)	Percent	100.0%	9.3%	6.1%	50.3%	25.4%	0.6%	5.6%	0.6%	0.3%	0.3%	0.3%	0.0%	(X)	(X)	(X)	1.2%
Transportation security screeners 3945 (SOC 33-9093)	Male																
Transportation security screeners 3945 (SOC 33-9093)	Number	17 215	1 640	960	8 910	3 935	105	1 165	50	85	50	85	0	(X)	(X)	(X)	235
Transportation security screeners 3945 (SOC 33-9093)	Percent	63.3%	6.0%	3.5%	32.7%	14.5%	0.4%	4.3%	0.2%	0.3%	0.2%	0.3%	0.0%	(X)	(X)	(X)	0.9%
Transportation security screeners 3945 (SOC 33-9093)	Female																
Transportation security screeners 3945 (SOC 33-9093)	Number	9 995	880	700	4 790	2 965	45	355	120	10	35	0	0	(X)	(X)	(X)	90
Transportation security screeners 3945 (SOC 33-9093)	Percent	36.7%	3.2%	2.6%	17.6%	10.9%	0.2%	1.3%	0.4%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.3%
Lifeguards and other recreational and a l other protective	Total, both sexes																
Lifeguards and other recreational and a l other protective	Number	189 105	9 950	7 160	146 010	15 960	1 000	3 495	405	1 035	1 280	1 180	175	(X)	(X)	(X)	1 455
Lifeguards and other recreational and a l other protective	Percent	100.0%	5.3%	3.8%	77.2%	8.4%	0.5%	1.8%	0.2%	0.5%	0.7%	0.6%	0.1%	(X)	(X)	(X)	0.8%
Lifeguards and other recreational and a l other protective	Male																
Lifeguards and other recreational and a l other protective	Number	88 210	4 865	3 240	69 275	6 115	500	1 675	105	450	585	485	0	(X)	(X)	(X)	920
Lifeguards and other recreational and a l other protective	Percent	46.6%	2.6%	1.7%	36.6%	3.2%	0.3%	0.9%	0.1%	0.2%	0.3%	0.3%	0.0%	(X)	(X)	(X)	0.5%
Lifeguards and other recreational and a l other protective	Female																
Lifeguards and other recreational and a l other protective	Number	100 895	5 080	3 925	76 735	9 845	500	1 820	300	585	700	700	175	(X)	(X)	(X)	535
Lifeguards and other recreational and a l other protective	Percent	53.4%	2.7%	2.1%	40.6%	5.2%	0.3%	1.0%	0.2%	0.3%	0.4%	0.4%	0.1%	(X)	(X)	(X)	0.3%
Chefs and head cooks 4000 (SOC 35-1011)	Total, both sexes																
Chefs and head cooks 4000 (SOC 35-1011)	Number	336 595	36 025	29 980	167 540	39 000	1 210	56 435	635	890	1 010	1 150	330	(X)	(X)	(X)	2 390
Chefs and head cooks 4000 (SOC 35-1011)	Percent	100.0%	10.7%	8.9%	49.8%	11.6%	0.4%	16.8%	0.2%	0.3%	0.3%	0.3%	0.1%	(X)	(X)	(X)	0.7%
Chefs and head cooks 4000 (SOC 35-1011)	Male																
Chefs and head cooks 4000 (SOC 35-1011)	Number	267 920	29 195	25 640	128 295	29 180	810	49 350	530	745	715	990	320	(X)	(X)	(X)	2 155
Chefs and head cooks 4000 (SOC 35-1011)	Percent	79.6%	8.7%	7.6%	38.1%	8.7%	0.2%	14.7%	0.2%	0.2%	0.2%	0.3%	0.1%	(X)	(X)	(X)	0.6%
Chefs and head cooks 4000 (SOC 35-1011)	Female																
Chefs and head cooks 4000 (SOC 35-1011)	Number	68 670	6 830	4 340	39 245	9 820	400	7 085	110	145	300	160	10	(X)	(X)	(X)	230
Chefs and head cooks 4000 (SOC 35-1011)	Percent	20.4%	2.0%	1.3%	11.7%	2.9%	0.1%	2.1%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
First-line supervisors of food preparation and serving	Total, both sexes																
First-line supervisors of food preparation and serving	Number	593 090	57 400	42 745	365 025	87 240	4 410	24 645	1 065	2 170	2 745	1 790	680	(X)	(X)	(X)	3 165
First-line supervisors of food preparation and serving	Percent	100.0%	9.7%	7.2%	61.5%	14.7%	0.7%	4.2%	0.2%	0.4%	0.5%	0.3%	0.1%	(X)	(X)	(X)	0.5%
First-line supervisors of food preparation and serving	Male																
First-line supervisors of food preparation and serving	Number	245 265	26 695	20 110	148 525	31 105	1 450	12 340	315	910	1 000	945	330	(X)	(X)	(X)	1 535
First-line supervisors of food preparation and serving	Percent	41.4%	4.5%	3.4%	25.0%	5.2%	0.2%	2.1%	0.1%	0.2%	0.2%	0.2%	0.1%	(X)	(X)	(X)	0.3%
First-line supervisors of food preparation and serving	Female																
First-line supervisors of food preparation and serving	Number	347 825	30 705	22 635	216 495	56 135	2 960	12 305	750	1 260	1 745	845	350	(X)	(X)	(X)	1 630
First-line supervisors of food preparation and serving	Percent	58.6%	5.2%	3.8%	36.5%	9.5%	0.5%	2.1%	0.1%	0.2%	0.3%	0.1%	0.1%	(X)	(X)	(X)	0.3%
Cooks 4020 (SOC 35-2010)	Total, both sexes																
Cooks 4020 (SOC 35-2010)	Number	2 300 210	382 125	284 090	1 059 905	393 790	20 020	117 535	4 825	8 295	10 555	4 850	2 355	(X)	(X)	(X)	11 865
Cooks 4020 (SOC 35-2010)	Percent	100.0%	16.6%	12.4%	46.1%	17.1%	0.9%	5.1%	0.2%	0.4%	0.5%	0.2%	0.1%	(X)	(X)	(X)	0.5%
Cooks 4020 (SOC 35-2010)	Male																
Cooks 4020 (SOC 35-2010)	Number	1 342 460	238 245	183 575	577 505	225 585	9 845	79 270	3 025	6 085	6 175	3 495	1 465	(X)	(X)	(X)	8 195
Cooks 4020 (SOC 35-2010)	Percent	58.4%	10.4%	8.0%	25.1%	9.8%	0.4%	3.4%	0.1%	0.3%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Cooks 4020 (SOC 35-2010)	Female																
Cooks 4020 (SOC 35-2010)	Number	957 750	143 880	100 515	482 400	168 205	10 180	38 265	1 800	2 210	4 385	1 355	885	(X)	(X)	(X)	3 670
Cooks 4020 (SOC 35-2010)	Percent	41.6%	6.3%	4.4%	21.0%	7.3%	0.4%	1.7%	0.1%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Food preparation workers 4030 (SOC 35-2021)	Total, both sexes																
Food preparation workers 4030 (SOC 35-2021)	Number	865 550	116 440	92 930	470 530	107 645	5 940	52 045	2 040	3 275	4 680	3 945	805	(X)	(X)	(X)	5 285
Food preparation workers 4030 (SOC 35-2021)	Percent	100.0%	13.5%	10.7%	54.4%	12.4%	0.7%	6.0%	0.2%	0.4%	0.5%	0.5%	0.1%	(X)	(X)	(X)	0.6%
Food preparation workers 4030 (SOC 35-2021)	Male																
Food preparation workers 4030 (SOC 35-2021)	Number	356 210	53 195	43 455	179 650	44 255	1 980	24 135	1 095	1 600	1 805	1 975	370	(X)	(X)	(X)	2 695
Food preparation workers 4030 (SOC 35-2021)	Percent	41.2%	6.1%	5.0%	20.8%	5.1%	0.2%	2.8%	0.1%	0.2%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Food preparation workers 4030 (SOC 35-2021)	Female																
Food preparation workers 4030 (SOC 35-2021)	Number	509,340	63,245	49,475	290,875	63,390	3,960	27,905	945	1,675	2,875	1,970	435	(X)	(X)	(X)	2,590
Food preparation workers 4030 (SOC 35-2021)	Percent	58.8%	7.3%	5.7%	33.6%	7.3%	0.5%	3.2%	0.1%	0.2%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.3%
Bartenders 4040 (SOC 35-3011)	Total, both sexes																
Bartenders 4040 (SOC 35-3011)	Number	423,135	28,360	17,735	337,315	17,870	2,810	9,925	765	960	2,355	2,140	300	(X)	(X)	(X)	2,600
Bartenders 4040 (SOC 35-3011)	Percent	100.0%	6.7%	4.2%	79.7%	4.2%	0.7%	2.3%	0.2%	0.2%	0.6%	0.5%	0.1%	(X)	(X)	(X)	0.6%
Bartenders 4040 (SOC 35-3011)	Male																
Bartenders 4040 (SOC 35-3011)	Number	180 090	16 835	9 590	133 460	9 800	855	5 530	480	385	705	1 010	115	(X)	(X)	(X)	1 320
Bartenders 4040 (SOC 35-3011)	Percent	42.6%	4.0%	2.3%	31.5%	2.3%	0.2%	1.3%	0.1%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Bartenders 4040 (SOC 35-3011)	Female																
Bartenders 4040 (SOC 35-3011)	Number	243 045	11 520	8 145	203 855	8 075	1 955	4 395	285	575	1 650	1 125	185	(X)	(X)	(X)	1 280
Bartenders 4040 (SOC 35-3011)	Percent	57.4%	2.7%	1.9%	48.2%	1.9%	0.5%	1.0%	0.1%	0.1%	0.4%	0.3%	0.0%	(X)	(X)	(X)	0.3%
Combined food preparation and serving workers including	Total, both sexes																
Combined food preparation and serving workers including	Number	353 535	31 830	25 810	218 490	55 220	2 580	11 225	670	1 820	2 300	940	490	(X)	(X)	(X)	2 165
Combined food preparation and serving workers including	Percent	100.0%	9.0%	7.3%	61.8%	15.6%	0.7%	3.2%	0.2%	0.5%	0.7%	0.3%	0.1%	(X)	(X)	(X)	0.6%
Combined food preparation and serving workers including	Male																
Combined food preparation and serving workers including	Number	117 825	11 950	10 750	66 515	20 135	725	5 060	240	470	490	450	155	(X)	(X)	(X)	890
Combined food preparation and serving workers including	Percent	33.3%	3.4%	3.0%	18.8%	5.7%	0.2%	1.4%	0.1%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Combined food preparation and serving workers including	Female																
Combined food preparation and serving workers including	Number	235 715	19 880	15 060	151 975	35 085	1 855	6 165	430	1 355	1 815	490	335	(X)	(X)	(X)	1 275
Combined food preparation and serving workers including	Percent	66.7%	5.6%	4.3%	43.0%	9.9%	0.5%	1.7%	0.1%	0.4%	0.5%	0.1%	0.1%	(X)	(X)	(X)	0.4%
Counter attendants cafeteria food concession and coffee	Total, both sexes																
Counter attendants cafeteria food concession and coffee	Number	275 630	23 885	17 600	180 770	33 440	1 655	10 375	560	1 850	1 560	1 520	210	(X)	(X)	(X)	2 205
Counter attendants cafeteria food concession and coffee	Percent	100.0%	8.7%	6.4%	65.6%	12.1%	0.6%	3.8%	0.2%	0.7%	0.6%	0.6%	0.1%	(X)	(X)	(X)	0.8%
Counter attendants cafeteria food concession and coffee	Male																
Counter attendants cafeteria food concession and coffee	Number	91 005	8 905	5 795	57 505	11 520	470	4 135	200	700	390	635	50	(X)	(X)	(X)	705
Counter attendants cafeteria food concession and coffee	Percent	33.0%	3.2%	2.1%	20.9%	4.2%	0.2%	1.5%	0.1%	0.3%	0.1%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Counter attendants cafeteria food concession and coffee	Female																
Counter attendants cafeteria food concession and coffee	Number	184 625	14 980	11 805	123 265	21 925	1 185	6 240	360	1 150	1 170	885	160	(X)	(X)	(X)	1 500
Counter attendants, cafeteria, food concession, and coffee	Percent	67.0%	5.4%	4.3%	44.7%	8.0%	0.4%	2.3%	0.1%	0.4%	0.4%	0.3%	0.1%	(X)	(X)	(X)	0.5%
Waiters and waitresses 4110 (SOC 35-3031)	Total, both sexes																
Waiters and waitresses 4110 (SOC 35-3031)	Number	2 275 425	224 885	146 940	1 552 220	162 930	13 005	124 415	2 850	9 885	11 970	11 260	980	(X)	(X)	(X)	14 095
Waiters and waitresses 4110 (SOC 35-3031)	Percent	100.0%	9.9%	6.5%	68.2%	7.2%	0.6%	5.5%	0.1%	0.4%	0.5%	0.5%	0.0%	(X)	(X)	(X)	0.6%
Waiters and waitresses 4110 (SOC 35-3031)	Male																
Waiters and waitresses 4110 (SOC 35-3031)	Number	623 275	86 940	57 615	362 035	52 825	2 860	45 030	1 180	2 605	2 405	4 090	325	(X)	(X)	(X)	5 360
Waiters and waitresses 4110 (SOC 35-3031)	Percent	27.4%	3.8%	2.5%	15.9%	2.3%	0.1%	2.0%	0.1%	0.1%	0.1%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Waiters and waitresses 4110 (SOC 35-3031)	Female																
Waiters and waitresses 4110 (SOC 35-3031)	Number	1 652 155	137 945	89 325	1 190 185	110 105	10 145	79 385	1 670	7 280	9 565	7 170	650	(X)	(X)	(X)	8 735
Waiters and waitresses 4110 (SOC 35-3031)	Percent	72.6%	6.1%	3.9%	52.3%	4.8%	0.4%	3.5%	0.1%	0.3%	0.4%	0.3%	0.0%	(X)	(X)	(X)	0.4%

Food servers, nonrestaurant 4120 (SOC 35-3041)	Total, both sexes																
Food servers nonrestaurant 4120 (SOC 35-3041)	Number	209 140	20 550	16 045	106 445	48 170	1 320	12 210	510	770	740	600	250	(X)	(X)	(X)	1 535
Food servers nonrestaurant 4120 (SOC 35-3041)	Percent	100.0%	9.8%	7.7%	50.9%	23.0%	0.6%	5.8%	0.2%	0.4%	0.4%	0.3%	0.1%	(X)	(X)	(X)	0.7%
Food servers, nonrestaurant 4120 (SOC 35-3041)	Male																
Food servers nonrestaurant 4120 (SOC 35-3041)	Number	67 460	8 565	7 635	29 255	14 610	225	5 440	195	275	215	265	85	(X)	(X)	(X)	685
Food servers nonrestaurant 4120 (SOC 35-3041)	Percent	32.3%	4.1%	3.7%	14.0%	7.0%	0.1%	2.6%	0.1%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Food servers nonrestaurant 4120 (SOC 35-3041)	Female																
Food servers nonrestaurant 4120 (SOC 35-3041)	Number	141 680	11 985	8 410	77 190	33 555	1 095	6 770	315	490	520	335	165	(X)	(X)	(X)	845
Food servers nonrestaurant 4120 (SOC 35-3041)	Percent	67.7%	5.7%	4.0%	36.9%	16.0%	0.5%	3.2%	0.2%	0.2%	0.2%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Miscellaneous food preparation and serving related	Total both sexes																
Miscellaneous food preparation and serving related	Number	385 195	67 970	52 105	191 050	43 105	3 060	20 060	930	1 185	1 575	1 515	260	(X)	(X)	(X)	2 380
Miscellaneous food preparation and serving related	Percent	100.0%	17.6%	13.5%	49.6%	11.2%	0.8%	5.2%	0.2%	0.3%	0.4%	0.4%	0.1%	(X)	(X)	(X)	0.6%
Miscellaneous food preparation and serving related	Male																
Miscellaneous food preparation and serving related	Number	216 275	42 125	35 635	99 425	21 735	1 250	11 125	575	890	695	1 115	205	(X)	(X)	(X)	1 500
Miscellaneous food preparation and serving related	Percent	56.1%	10.9%	9.3%	25.8%	5.6%	0.3%	2.9%	0.1%	0.2%	0.2%	0.3%	0.1%	(X)	(X)	(X)	0.4%
Miscellaneous food preparation and serving related	Female																
Miscellaneous food preparation and serving related	Number	168 920	25 850	16 465	91 625	21 370	1 810	8 935	355	295	880	400	50	(X)	(X)	(X)	880
Miscellaneous food preparation and serving related	Percent	43.9%	6.7%	4.3%	23.8%	5.5%	0.5%	2.3%	0.1%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Dishwashers 4140 (SOC 35-9021)	Total both sexes																
Dishwashers 4140 (SOC 35-9021)	Number	333 210	62 665	49 385	151 975	49 235	3 075	9 945	720	1 630	1 785	745	240	(X)	(X)	(X)	1 810
Dishwashers 4140 (SOC 35-9021)	Percent	100.0%	18.8%	14.8%	45.6%	14.8%	0.9%	3.0%	0.2%	0.5%	0.5%	0.2%	0.1%	(X)	(X)	(X)	0.5%
Dishwashers 4140 (SOC 35-9021)	Male																
Dishwashers 4140 (SOC 35-9021)	Number	260 000	49 670	40 270	113 875	41 245	2 185	6 935	600	1 410	1 405	665	190	(X)	(X)	(X)	1 555
Dishwashers 4140 (SOC 35-9021)	Percent	78.0%	14.9%	12.1%	34.2%	12.4%	0.7%	2.1%	0.2%	0.4%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.5%
Dishwashers 4140 (SOC 35-9021)	Female																
Dishwashers 4140 (SOC 35-9021)	Number	73,205	12,995	9,115	38,100	7,990	890	3,010	120	215	380	80	55	(X)	(X)	(X)	255
Dishwashers 4140 (SOC 35-9021)	Percent	22.0%	3.9%	2.7%	11.4%	2.4%	0.3%	0.9%	0.0%	0.1%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Hosts and hostesses restaurant lounge and coffee shop	Total both sexes																
Hosts and hostesses, restaurant, lounge, and coffee shop	Number	296,970	28,200	18,020	203,835	25,255	1,565	11,490	395	1,925	1,510	2,115	345	(X)	(X)	(X)	2,325
Hosts and hostesses restaurant lounge and coffee shop	Percent	100.0%	9.5%	6.1%	68.6%	8.5%	0.5%	3.9%	0.1%	0.6%	0.5%	0.7%	0.1%	(X)	(X)	(X)	0.8%
Hosts and hostesses restaurant lounge and coffee shop	Male																
Hosts and hostesses restaurant lounge and coffee shop	Number	38 980	4 160	2 895	24 640	4 045	230	1 885	105	265	230	175	100	(X)	(X)	(X)	245
Hosts and hostesses restaurant lounge and coffee shop	Percent	13.1%	1.4%	1.0%	8.3%	1.4%	0.1%	0.6%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Hosts and hostesses restaurant lounge and coffee shop	Female																
Hosts and hostesses restaurant lounge and coffee shop	Number	257 995	24 040	15 125	179 195	21 215	1 335	9 605	290	1 655	1 280	1 940	245	(X)	(X)	(X)	2 080
Hosts and hostesses restaurant lounge and coffee shop	Percent	86.9%	8.1%	5.1%	60.3%	7.1%	0.4%	3.2%	0.1%	0.6%	0.4%	0.7%	0.1%	(X)	(X)	(X)	0.7%
First-line supervisors of housekeeping and janitorial	Total both sexes																
First-line supervisors of housekeeping and janitorial	Number	268 370	32 480	25 965	151 500	45 305	2 085	6 670	610	445	1 080	265	290	(X)	(X)	(X)	1 675
First-line supervisors of housekeeping and janitorial	Percent	100.0%	12.1%	9.7%	56.5%	16.9%	0.8%	2.5%	0.2%	0.2%	0.4%	0.1%	0.1%	(X)	(X)	(X)	0.6%
First-line supervisors of housekeeping and janitorial	Male																
First-line supervisors of housekeeping and janitorial	Number	163 215	18 650	14 720	97 315	25 250	925	3 940	250	325	515	220	200	(X)	(X)	(X)	905
First-line supervisors of housekeeping and janitorial	Percent	60.8%	6.9%	5.5%	36.3%	9.4%	0.3%	1.5%	0.1%	0.1%	0.2%	0.1%	0.1%	(X)	(X)	(X)	0.3%
First-line supervisors of housekeeping and janitorial	Female																
First-line supervisors of housekeeping and janitorial	Number	105 155	13 830	11 245	54 180	20 050	1 165	2 735	365	120	565	50	95	(X)	(X)	(X)	765
First-line supervisors of housekeeping and janitorial	Percent	39.2%	5.2%	4.2%	20.2%	7.5%	0.4%	1.0%	0.1%	0.0%	0.2%	0.0%	0.0%	(X)	(X)	(X)	0.3%
First-line supervisors of landscaping lawn service and	Total both sexes																
First-line supervisors of landscaping lawn service and	Number	200 480	23 140	16 805	144 970	10 500	835	1 670	435	135	1 095	250	55	(X)	(X)	(X)	585
First-line supervisors of landscaping lawn service and	Percent	100.0%	11.5%	8.4%	72.3%	5.2%	0.4%	0.8%	0.2%	0.1%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.3%
First-line supervisors of landscaping lawn service and	Male																
First-line supervisors of landscaping lawn service and	Number	187 500	22 350	16 330	134 365	9 940	785	1 490	395	130	925	195	55	(X)	(X)	(X)	535
First-line supervisors of landscaping, lawn service, and	Percent	93.5%	11.1%	8.1%	67.0%	5.0%	0.4%	0.7%	0.2%	0.1%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.3%
First-line supervisors of landscaping lawn service and	Female																
First-line supervisors of landscaping lawn service and	Number	12 980	790	475	10 610	555	50	180	35	10	170	55	0	(X)	(X)	(X)	50
First-line supervisors of landscaping, lawn service, and	Percent	6.5%	0.4%	0.2%	5.3%	0.3%	0.0%	0.1%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Jan tors and building cleaners 4220 (SOC 37-201X)	Total both sexes																
Jan tors and building cleaners 4220 (SOC 37-201X)	Number	2 607 880	377 075	314 615	1 321 200	458 795	23 820	73 075	4 520	4 630	10 965	2 935	2 670	(X)	(X)	(X)	13 590
Jan tors and building cleaners 4220 (SOC 37-201X)	Percent	100.0%	14.5%	12.1%	50.7%	17.6%	0.9%	2.8%	0.2%	0.2%	0.4%	0.1%	0.1%	(X)	(X)	(X)	0.5%
Jan tors and building cleaners 4220 (SOC 37-201X)	Male																
Jan tors and building cleaners 4220 (SOC 37-201X)	Number	1 781 815	233 930	196 575	938 865	317 265	16 480	51 355	3 025	3 385	7 095	2 150	2 175	(X)	(X)	(X)	9 515
Jan tors and building cleaners 4220 (SOC 37-201X)	Percent	68.3%	9.0%	7.5%	36.0%	12.2%	0.6%	2.0%	0.1%	0.1%	0.3%	0.1%	0.1%	(X)	(X)	(X)	0.4%
Jan tors and building cleaners 4220 (SOC 37-201X)	Female																
Jan tors and building cleaners 4220 (SOC 37-201X)	Number	826 065	143 145	118 040	382 335	141 530	7 335	21 725	1 490	1 245	3 870	785	495	(X)	(X)	(X)	4 075
Jan tors and building cleaners 4220 (SOC 37-201X)	Percent	31.7%	5.5%	4.5%	14.7%	5.4%	0.3%	0.8%	0.1%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.2%
Maids and housekeeping cleaners 4230 (SOC 37-2012)	Total both sexes																
Maids and housekeeping cleaners 4230 (SOC 37-2012)	Number	1 566 300	364 895	282 350	549 045	270 320	13 985	57 935	2 720	2 315	5 515	1 235	1 050	(X)	(X)	(X)	14 940
Maids and housekeeping cleaners 4230 (SOC 37-2012)	Percent	100.0%	23.3%	18.0%	35.1%	17.3%	0.9%	3.7%	0.2%	0.1%	0.4%	0.1%	0.1%	(X)	(X)	(X)	1.0%
Maids and housekeeping cleaners 4230 (SOC 37-2012)	Male																
Maids and housekeeping cleaners 4230 (SOC 37-2012)	Number	183 870	32 100	29 325	57 750	46 610	2 195	12 445	535	330	390	295	265	(X)	(X)	(X)	1 625
Maids and housekeeping cleaners 4230 (SOC 37-2012)	Percent	11.7%	2.0%	1.9%	3.7%	3.0%	0.1%	0.8%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Maids and housekeeping cleaners 4230 (SOC 37-2012)	Female																
Maids and housekeeping cleaners 4230 (SOC 37-2012)	Number	1 382 430	332 795	253 030	491 295	223 705	11 785	45 490	2 185	1 980	5 125	940	785	(X)	(X)	(X)	13 315
Maids and housekeeping cleaners 4230 (SOC 37-2012)	Percent	88.3%	21.2%	16.2%	31.4%	14.3%	0.8%	2.9%	0.1%	0.1%	0.3%	0.1%	0.1%	(X)	(X)	(X)	0.9%
Pest control workers 4240 (SOC 37-2021)	Total both sexes																
Pest control workers 4240 (SOC 37-2021)	Number	69 515	6 545	3 345	50 960	6 310	235	880	135	185	405	140	85	(X)	(X)	(X)	290
Pest control workers 4240 (SOC 37-2021)	Percent	100.0%	9.4%	4.8%	73.3%	9.1%	0.3%	1.3%	0.2%	0.3%	0.6%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Pest control workers 4240 (SOC 37-2021)	Male																
Pest control workers 4240 (SOC 37-2021)	Number	65 960	6 235	3 265	48 240	6 050	195	850	95	185	355	115	85	(X)	(X)	(X)	290
Pest control workers 4240 (SOC 37-2021)	Percent	94.9%	9.0%	4.7%	69.4%	8.7%	0.3%	1.2%	0.1%	0.3%	0.5%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Pest control workers 4240 (SOC 37-2021)	Female																
Pest control workers 4240 (SOC 37-2021)	Number	3 550	310	80	2 720	260	40	30	40	0	50	30	0	(X)	(X)	(X)	0
Pest control workers 4240 (SOC 37-2021)	Percent	5.1%	0.4%	0.1%	3.9%	0.4%	0.1%	0.0%	0.1%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Grounds maintenance workers 4250 (SOC 37-3010)	Total both sexes																
Grounds maintenance workers 4250 (SOC 37-3010)	Number	1 384 225	314 675	232 440	672 500	119 290	9 390	16 480	2 560	2 135	5 770	1 625	950	(X)	(X)	(X)	6 405
Grounds maintenance workers 4250 (SOC 37-3010)	Percent	100.0%	22.7%	16.8%	48.6%	8.6%	0.7%	1.2%	0.2%	0.2%	0.4%	0.1%	0.1%	(X)	(X)	(X)	0.5%
Grounds maintenance workers 4250 (SOC 37-3010)	Male																
Grounds maintenance workers 4250 (SOC 37-3010)	Number	1 294 995	304 285	225 515	611 720	112 390	8 115	14 995	2 230	2 075	5 340	1 415	850	(X)	(X)	(X)	6 065
Grounds maintenance workers 4250 (SOC 37-3010)	Percent	93.6%	22.0%	16.3%	44.2%	8.1%	0.6%	1.1%	0.2%	0.1%	0.4%	0.1%	0.1%	(X)	(X)	(X)	0.4%
Grounds maintenance workers 4250 (SOC 37-3010)	Female																
Grounds maintenance workers 4250 (SOC 37-3010)	Number	89 235	10 390	6 925	60 780	6 900	1 280	1 485	330	60	430	210	100	(X)	(X)	(X)	340
Grounds maintenance workers 4250 (SOC 37-3010)	Percent	6.4%	0.8%	0.5%	4.4%	0.5%	0.1%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
First-line supervisors of gaming workers 4300 (SOC 39-	Total both sexes																
First-line supervisors of gaming workers 4300 (SOC 39-	Number	80 390	4 100	2 625	59 935	5 080	2 350	4 800	160	170	580	220	50	(X)	(X)	(X)	320
First-line supervisors of gaming workers 4300 (SOC 39-	Percent	100.0%	5.1%	3.3%	74.6%	6.3%	2.9%	6.0%	0.2%	0.2%	0.7%	0.3%	0.1%	(X)	(X)	(X)	0.4%
First-line supervisors of gaming workers 4300 (SOC 39-	Male																
First-line supervisors of gaming workers 4300 (SOC 39-	Number	44 870	2 550	1 550	33 810	2 485	1 135	2 510	80	105	335	95	50	(X)	(X)	(X)	165
First-line supervisors of gaming workers 4300 (SOC 39-	Percent	55.8%	3.2%	1.9%	42.1%	3.1%	1.4%	3.1%	0.1%	0.1%	0.4%	0.1%	0.1%	(X)	(X)	(X)	0.2%
First-line supervisors of gaming workers 4300 (SOC 39-	Female																
First-line supervisors of gaming workers 4300 (SOC 39-	Number	35 520	1 550	1 070	26 130	2 595	1 215	2 290	80	65	245	125	0	(X)	(X)	(X)	155
First-line supervisors of gaming workers 4300 (SOC 39-	Percent	44.2%	1.9%	1.3%	32.5%	3.2%	1.5%	2.8%	0.1%	0.1%	0.3%	0.2%	0.0%	(X)	(X)	(X)	0.2%
First-line supervisors of personal service workers 4320	Total both sexes																
First-line supervisors of personal service workers 4320	Number	188,200	11,280	6,345	133,345	14,995	875	18,305	190	535	930	545	165	(X)	(X)	(X)	695
First-line supervisors of personal service workers 4320	Percent	100.0%	6.0%	3.4%	70.9%	8.0%	0.5%	9.7%	0.1%	0.3%	0.5%	0.3%	0.1%	(X)	(X)	(X)	0.4%
First-line supervisors of personal service workers 4320	Male																
First-line supervisors of personal service workers 4320	Number	72,035	4,200	2,820	50,280	5,505	295	8,030	4	250	200	120	75	(X)	(X)	(X)	260
First-line supervisors of personal service workers 4320	Percent	38.3%	2.2%	1.5%	26.7%	2.9%	0.2%	4.3%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
First-line supervisors of personal service workers 4320	Female																
First-line supervisors of personal service workers 4320	Number	116 165	7 075	3 520	83 065	9 490	580	10 275	190	285	725	425	95	(X)	(X)	(X)	435
First-line supervisors of personal service workers 4320 (SOC 39-1021)	Percent	61.7%	3.8%	1.9%	44.1%	5.0%	0.3%	5.5%	0.1%	0.2%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.2%
Animal trainers 4340 (SOC 39-2011)	Total both sexes																
Animal trainers 4340 (SOC 39-2011)	Number	40 480	2 325	1 250	34 385	985	315	620	45	95	260	65	15	(X)	(X)	(X)	120
Animal trainers 4340 (SOC 39-2011)	Percent	100.0%	5.7%	3.1%	84.9%	2.4%	0.8%	1.5%	0.1%	0.2%	0.6%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Animal trainers 4340 (SOC 39-2011)	Male																
Animal trainers 4340 (SOC 39-2011)	Number	19 305	1 805	1 040	14 890	830	170	270	0	30	140	25	15	(X)	(X)	(X)	95
Animal trainers 4340 (SOC 39-2011)	Percent	47.7%	4.5%	2.6%	36.8%	2.1%	0.4%	0.7%	0.0%	0.1%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Animal trainers 4340 (SOC 39-2011)	Female																
Animal trainers 4340 (SOC 39-2011)	Number	21 170	520	205	19 495	155	145	350	45	65	120	45	0	(X)	(X)	(X)	25
Animal trainers 4340 (SOC 39-2011)	Percent	52.3%	1.3%	0.5%	48.2%	0.4%	0.4%	0.9%	0.1%	0.2%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Nonfarm animal caretakers 4350 (SOC 39-2021)	Total both sexes																
Nonfarm animal caretakers 4350 (SOC 39-2021)	Number	183 055	11 685	7 550	150 150	6 770	780	2 320	75	635	1 565	685	130	(X)	(X)	(X)	710
Nonfarm animal caretakers 4350 (SOC 39-2021)	Percent	100.0%	6.4%	4.1%	82.0%	3.7%	0.4%	1.3%	0.0%	0.3%	0.9%	0.4%	0.1%	(X)	(X)	(X)	0.4%
Nonfarm animal caretakers 4350 (SOC 39-2021)	Male																
Nonfarm animal caretakers 4350 (SOC 39-2021)	Number	52 845	5 620	4 040	37 785	3 540	235	650	15	85	485	180	15	(X)	(X)	(X)	195
Nonfarm animal caretakers 4350 (SOC 39-2021)	Percent	28.9%	3.1%	2.2%	20.6%	1.9%	0.1%	0.4%	0.0%	0.0%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Nonfarm animal caretakers 4350 (SOC 39-2021)	Female																
Nonfarm animal caretakers 4350 (SOC 39-2021)	Number	130 210	6 065	3 510	112 365	3 230	545	1 675	60	545	1 080	500	115	(X)	(X)	(X)	520
Nonfarm animal caretakers 4350 (SOC 39-2021)	Percent	71.1%	3.3%	1.9%	61.4%	1.8%	0.3%	0.9%	0.0%	0.3%	0.6%	0.3%	0.1%	(X)	(X)	(X)	0.3%
Gaming services workers 4400 (SOC 39-3010)	Total, both sexes																
Gaming services workers 4400 (SOC 39-3010)	Number	112 340	7 225	4 630	58 450	10 610	3 745	25 015	280	140	710	620	95	(X)	(X)	(X)	820
Gaming services workers 4400 (SOC 39-3010)	Percent	100.0%	6.4%	4.1%	52.0%	9.4%	3.3%	22.3%	0.2%	0.1%	0.6%	0.6%	0.1%	(X)	(X)	(X)	0.7%
Gaming services workers 4400 (SOC 39-3010)	Male																
Gaming services workers 4400 (SOC 39-3010)	Number	58 110	4 150	2 145	33 180	4 590	1 740	11 260	115	20	245	280	55	(X)	(X)	(X)	340
Gaming services workers 4400 (SOC 39-3010)	Percent	51.7%	3.7%	1.9%	29.5%	4.1%	1.5%	10.0%	0.1%	0.0%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Gaming services workers 4400 (SOC 39-3010)	Female																
Gaming services workers 4400 (SOC 39-3010)	Number	54 230	3 075	2 485	25 275	6 020	2 005	13 755	165	120	465	340	40	(X)	(X)	(X)	480
Gaming services workers 4400 (SOC 39-3010)	Percent	48.3%	2.7%	2.2%	22.5%	5.4%	1.8%	12.2%	0.1%	0.1%	0.4%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Motion picture projectionists 4410 (SOC 39-3021)	Total both sexes																
Motion picture projectionists 4410 (SOC 39-3021)	Number	9 260	500	300	7 380	530	35	325	0	30	35	75	10	(X)	(X)	(X)	40

Motion picture projectionists 4410 (SOC 39-3021)	Percent	100.0%	5.4%	3.2%	79.7%	5.7%	0.4%	3.5%	0.0%	0.3%	0.4%	0.8%	0.1%	(X)	(X)	(X)	0.4%
Motion picture projectionists 4410 (SOC 39-3021)	Male																
Motion picture projectionists 4410 (SOC 39-3021)	Number	7 700	455	265	6 165	410	20	240	0	0	25	70	10	(X)	(X)	(X)	40
Motion picture projectionists 4410 (SOC 39-3021)	Percent	83.2%	4.9%	2.9%	66.6%	4.4%	0.2%	2.6%	0.0%	0.0%	0.3%	0.8%	0.1%	(X)	(X)	(X)	0.4%
Motion picture projectionists 4410 (SOC 39-3021)	Female																
Motion picture projectionists 4410 (SOC 39-3021)	Number	1 555	45	35	1 215	120	15	85	0	30	10	4	0	(X)	(X)	(X)	0
Motion picture projectionists 4410 (SOC 39-3021)	Percent	16.8%	0.5%	0.4%	13.1%	1.3%	0.2%	0.9%	0.0%	0.3%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Ushers lobby attendants and ticket takers 4420 (SOC 39-	Total both sexes																
Ushers lobby attendants and ticket takers 4420 (SOC 39-	Number	51 950	4 070	3 005	32 885	9 140	245	1 385	45	240	425	175	40	(X)	(X)	(X)	300
Ushers lobby attendants and ticket takers 4420 (SOC 39-	Percent	100.0%	7.8%	5.8%	63.3%	17.6%	0.5%	2.7%	0.1%	0.5%	0.8%	0.3%	0.1%	(X)	(X)	(X)	0.6%
Ushers lobby attendants and ticket takers 4420 (SOC 39-	Male																
Ushers lobby attendants and ticket takers 4420 (SOC 39-	Number	29 340	2 530	1 770	18 945	4 460	120	785	35	165	265	100	20	(X)	(X)	(X)	150
Ushers lobby attendants and ticket takers 4420 (SOC 39-	Percent	56.5%	4.9%	3.4%	36.5%	8.6%	0.2%	1.5%	0.1%	0.3%	0.5%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Ushers lobby attendants and ticket takers 4420 (SOC 39-	Female																
Ushers lobby attendants and ticket takers 4420 (SOC 39-	Number	22 610	1 540	1 235	13 940	4 680	130	600	10	75	160	75	20	(X)	(X)	(X)	150
Ushers lobby attendants and ticket takers 4420 (SOC 39-	Percent	43.5%	3.0%	2.4%	26.8%	9.0%	0.3%	1.2%	0.0%	0.1%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Miscellaneous entertainment attendants and related	Total both sexes																
Miscellaneous entertainment attendants and related	Number	196 765	14 310	9 710	136 775	21 605	2 190	6 990	455	1 045	965	785	165	(X)	(X)	(X)	1 775
Miscellaneous entertainment attendants and related	Percent	100.0%	7.3%	4.9%	69.5%	11.0%	1.1%	3.6%	0.2%	0.5%	0.5%	0.4%	0.1%	(X)	(X)	(X)	0.9%
Miscellaneous entertainment attendants and related	Male																
Miscellaneous entertainment attendants and related	Number	115 745	7 900	5 045	84 120	11 100	960	3 840	255	455	545	460	65	(X)	(X)	(X)	1 000
Miscellaneous entertainment attendants and related	Percent	58.8%	4.0%	2.6%	42.8%	5.6%	0.5%	2.0%	0.1%	0.2%	0.3%	0.2%	0.0%	(X)	(X)	(X)	0.5%
Miscellaneous entertainment attendants and related	Female																
Miscellaneous entertainment attendants and related	Number	81 020	6 410	4 665	52 655	10 500	1 230	3 150	200	590	415	325	100	(X)	(X)	(X)	775
Miscellaneous entertainment attendants and related	Percent	41.2%	3.3%	2.4%	26.8%	5.3%	0.6%	1.6%	0.1%	0.3%	0.2%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Embalmers and funeral attendants 4460 (SOC 39-40XX)	Total, both sexes																
Embalmers and funeral attendants 4460 (SOC 39-40XX)	Number	15 315	820	285	12 325	1 595	0	155	0	15	35	25	15	(X)	(X)	(X)	45
Embalmers and funeral attendants 4460 (SOC 39-40XX)	Percent	100.0%	5.4%	1.9%	80.5%	10.4%	0.0%	1.0%	0.0%	0.1%	0.2%	0.2%	0.1%	(X)	(X)	(X)	0.3%
Embalmers and funeral attendants 4460 (SOC 39-40XX)	Male																
Embalmers and funeral attendants 4460 (SOC 39-40XX)	Number	11 605	525	220	9 385	1 320	0	100	0	15	20	15	0	(X)	(X)	(X)	4
Embalmers and funeral attendants 4460 (SOC 39-40XX)	Percent	75.8%	3.4%	1.4%	61.3%	8.6%	0.0%	0.7%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.0%
Embalmers and funeral attendants 4460 (SOC 39-40XX)	Female																
Embalmers and funeral attendants 4460 (SOC 39-40XX)	Number	3 710	295	60	2 940	275	0	55	0	0	15	10	15	(X)	(X)	(X)	45
Embalmers and funeral attendants 4460 (SOC 39-40XX)	Percent	24.2%	1.9%	0.4%	19.2%	1.8%	0.0%	0.4%	0.0%	0.0%	0.1%	0.1%	0.1%	(X)	(X)	(X)	0.3%
Morticians undertakers and funeral directors 4465 (SOC	Total both sexes																
Morticians undertakers and funeral directors 4465 (SOC	Number	40 280	1 515	430	33 245	4 550	95	195	15	10	120	0	35	(X)	(X)	(X)	70
Morticians undertakers and funeral directors 4465 (SOC	Percent	100.0%	3.8%	1.1%	82.5%	11.3%	0.2%	0.5%	0.0%	0.0%	0.3%	0.0%	0.1%	(X)	(X)	(X)	0.2%
Morticians undertakers and funeral directors 4465 (SOC	Male																
Morticians undertakers and funeral directors 4465 (SOC	Number	31 185	1 060	290	26 250	3 240	70	145	4	10	60	0	25	(X)	(X)	(X)	25
Morticians undertakers and funeral directors 4465 (SOC	Percent	77.4%	2.6%	0.7%	65.2%	8.0%	0.2%	0.4%	0.0%	0.0%	0.1%	0.0%	0.1%	(X)	(X)	(X)	0.1%
Morticians undertakers and funeral directors 4465 (SOC	Female																
Morticians undertakers and funeral directors 4465 (SOC	Number	9 095	455	140	6 995	1 310	25	50	10	0	55	0	4	(X)	(X)	(X)	45
Morticians undertakers and funeral directors 4465 (SOC	Percent	22.6%	1.1%	0.3%	17.4%	3.3%	0.1%	0.1%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Barbers 4500 (SOC 39-5011)	Total both sexes																
Barbers 4500 (SOC 39-5011)	Number	94 910	8 280	7 045	45 905	27 835	370	4 045	40	205	340	125	205	(X)	(X)	(X)	515
Barbers 4500 (SOC 39-5011)	Percent	100.0%	8.7%	7.4%	48.4%	29.3%	0.4%	4.3%	0.0%	0.2%	0.4%	0.1%	0.2%	(X)	(X)	(X)	0.5%
Barbers 4500 (SOC 39-5011)	Male																
Barbers 4500 (SOC 39-5011)	Number	72 475	6 115	5 585	31 925	25 750	250	1 845	4	190	195	10	205	(X)	(X)	(X)	405
Barbers 4500 (SOC 39-5011)	Percent	76.4%	6.4%	5.9%	33.6%	27.1%	0.3%	1.9%	0.0%	0.2%	0.2%	0.0%	0.2%	(X)	(X)	(X)	0.4%
Barbers 4500 (SOC 39-5011)	Female																
Barbers 4500 (SOC 39-5011)	Number	22,435	2,165	1,455	13,980	2,085	125	2,205	40	15	145	115	4	(X)	(X)	(X)	110
Barbers 4500 (SOC 39-5011)	Percent	23.6%	2.3%	1.5%	14.7%	2.2%	0.1%	2.3%	0.0%	0.0%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Hairdressers hairstylists and cosmetologists 4510 (SOC	Total both sexes																
Hairdressers, hairstylists, and cosmetologists 4510 (SOC	Number	779,220	61,065	43,015	535,000	86,685	2,965	39,365	390	1,475	3,435	2,235	415	(X)	(X)	(X)	3,170
Hairdressers hairstylists and cosmetologists 4510 (SOC	Percent	100.0%	7.8%	5.5%	68.7%	11.1%	0.4%	5.1%	0.1%	0.2%	0.4%	0.3%	0.1%	(X)	(X)	(X)	0.4%
Hairdressers hairstylists and cosmetologists 4510 (SOC	Male																
Hairdressers hairstylists and cosmetologists 4510 (SOC	Number	64 580	6 360	4 635	40 560	6 860	260	4 675	45	160	435	245	90	(X)	(X)	(X)	250
Hairdressers hairstylists and cosmetologists 4510 (SOC	Percent	8.3%	0.8%	0.6%	5.2%	0.9%	0.0%	0.6%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Hairdressers hairstylists and cosmetologists 4510 (SOC	Female																
Hairdressers hairstylists and cosmetologists 4510 (SOC	Number	714 640	54 705	38 380	494 440	79 830	2 705	34 685	340	1 320	3 000	1 985	325	(X)	(X)	(X)	2 920
Hairdressers hairstylists and cosmetologists 4510 (SOC	Percent	91.7%	7.0%	4.9%	63.5%	10.2%	0.3%	4.5%	0.0%	0.2%	0.4%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Miscellaneous personal appearance workers 4520 (SOC	Total both sexes																
Miscellaneous personal appearance workers 4520 (SOC	Number	242 260	14 915	8 440	86 660	9 775	345	118 460	135	400	505	1 380	225	(X)	(X)	(X)	1 020
Miscellaneous personal appearance workers 4520 (SOC	Percent	100.0%	6.2%	3.5%	35.8%	4.0%	0.1%	48.9%	0.1%	0.2%	0.2%	0.6%	0.1%	(X)	(X)	(X)	0.4%
Miscellaneous personal appearance workers 4520 (SOC	Male																
Miscellaneous personal appearance workers 4520 (SOC	Number	32 210	1 005	610	2 855	525	50	26 830	40	0	30	260	0	(X)	(X)	(X)	10
Miscellaneous personal appearance workers 4520 (SOC	Percent	13.3%	0.4%	0.3%	1.2%	0.2%	0.0%	11.1%	0.0%	0.0%	0.0%	0.1%	0.0%	(X)	(X)	(X)	0.0%
Miscellaneous personal appearance workers 4520 (SOC	Female																
Miscellaneous personal appearance workers 4520 (SOC	Number	210 050	13 910	7 830	83 810	9 250	300	91 630	95	400	475	1 120	225	(X)	(X)	(X)	1 010
Miscellaneous personal appearance workers 4520 (SOC	Percent	86.7%	5.7%	3.2%	34.6%	3.8%	0.1%	37.8%	0.0%	0.2%	0.2%	0.5%	0.1%	(X)	(X)	(X)	0.4%
Baggage porters bellhops and concierges 4530 (SOC 39-	Total both sexes																
Baggage porters bellhops and concierges 4530 (SOC 39-	Number	79 655	10 375	9 080	32 580	18 750	475	5 900	540	215	145	355	135	(X)	(X)	(X)	1 105
Baggage porters bellhops and concierges 4530 (SOC 39-	Percent	100.0%	13.0%	11.4%	40.9%	23.5%	0.6%	7.4%	0.7%	0.3%	0.2%	0.4%	0.2%	(X)	(X)	(X)	1.4%
Baggage porters bellhops and concierges 4530 (SOC 39-	Male																
Baggage porters bellhops and concierges 4530 (SOC 39-	Number	63 505	8 630	7 830	24 510	15 455	315	4 860	465	155	115	235	115	(X)	(X)	(X)	820
Baggage porters, bellhops, and concierges 4530 (SOC 39-	Percent	79.7%	10.8%	9.8%	30.8%	19.4%	0.4%	6.1%	0.6%	0.2%	0.1%	0.3%	0.1%	(X)	(X)	(X)	1.0%
Baggage porters bellhops and concierges 4530 (SOC 39-	Female																
Baggage porters bellhops and concierges 4530 (SOC 39-	Number	16 150	1 745	1 250	8 065	3 295	165	1 040	75	55	30	120	20	(X)	(X)	(X)	290
Baggage porters, bellhops, and concierges 4530 (SOC 39-	Percent	20.3%	2.2%	1.6%	10.1%	4.1%	0.2%	1.3%	0.1%	0.1%	0.0%	0.2%	0.0%	(X)	(X)	(X)	0.4%
Tour and travel guides 4540 (SOC 39-7010)	Total both sexes																
Tour and travel guides 4540 (SOC 39-7010)	Number	49 330	1 955	1 215	38 230	3 150	505	2 705	210	180	280	280	0	(X)	(X)	(X)	620
Tour and travel guides 4540 (SOC 39-7010)	Percent	100.0%	4.0%	2.5%	77.5%	6.4%	1.0%	5.5%	0.4%	0.4%	0.6%	0.6%	0.0%	(X)	(X)	(X)	1.3%
Tour and travel guides 4540 (SOC 39-7010)	Male																
Tour and travel guides 4540 (SOC 39-7010)	Number	25 535	1 165	380	19 955	1 295	375	1 670	140	4	125	160	0	(X)	(X)	(X)	255
Tour and travel guides 4540 (SOC 39-7010)	Percent	51.8%	2.4%	0.8%	40.5%	2.6%	0.8%	3.4%	0.3%	0.0%	0.3%	0.3%	0.0%	(X)	(X)	(X)	0.5%
Tour and travel guides 4540 (SOC 39-7010)	Female																
Tour and travel guides 4540 (SOC 39-7010)	Number	23 795	790	830	18 275	1 860	130	1 035	65	170	150	120	0	(X)	(X)	(X)	365
Tour and travel guides 4540 (SOC 39-7010)	Percent	48.2%	1.6%	1.7%	37.0%	3.8%	0.3%	2.1%	0.1%	0.3%	0.3%	0.2%	0.0%	(X)	(X)	(X)	0.7%
Childcare workers 4600 (SOC 39-9011)	Total both sexes																
Childcare workers 4600 (SOC 39-9011)	Number	1 462 075	154 430	127 940	857 555	241 290	10 250	42 750	2 010	4 845	6 270	3 335	1 700	(X)	(X)	(X)	9 690
Childcare workers 4600 (SOC 39-9011)	Percent	100.0%	10.6%	8.8%	58.7%	16.5%	0.7%	2.9%	0.1%	0.3%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.7%
Childcare workers 4600 (SOC 39-9011)	Male																
Childcare workers 4600 (SOC 39-9011)	Number	86 280	7 450	6 250	46 495	19 595	965	3 385	200	425	390	420	25	(X)	(X)	(X)	685
Childcare workers 4600 (SOC 39-9011)	Percent	5.9%	0.5%	0.4%	3.2%	1.3%	0.1%	0.2%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Childcare workers 4600 (SOC 39-9011)	Female																
Childcare workers 4600 (SOC 39-9011)	Number	1 375 795	146 980	121 695	811 060	221 695	9 290	39 365	1 810	4 420	5 880	2 915	1 675	(X)	(X)	(X)	9 005
Childcare workers 4600 (SOC 39-9011)	Percent	94.1%	10.1%	8.3%	55.5%	15.2%	0.6%	2.7%	0.1%	0.3%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.6%
Personal care aides 4610 (SOC 39-9021)	Total both sexes																
Personal care aides 4610 (SOC 39-9021)	Number	927 270	97 240	71 035	447 245	217 370	10 680	62 100	4 190	2 505	5 925	1 520	1 595	(X)	(X)	(X)	5 865
Personal care aides 4610 (SOC 39-9021)	Percent	100.0%	10.5%	7.7%	48.2%	23.4%	1.2%	6.7%	0.5%	0.3%	0.6%	0.2%	0.2%	(X)	(X)	(X)	0.6%
Personal care aides 4610 (SOC 39-9021)	Male																
Personal care aides 4610 (SOC 39-9021)	Number	133 510	11 205	7 410	66 215	31 570	1 615	12 145	530	500	905	270	240	(X)	(X)	(X)	905
Personal care aides 4610 (SOC 39-9021)	Percent	14.4%	1.2%	0.8%	7.1%	3.4%	0.2%	1.3%	0.1%	0.1%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Personal care aides 4610 (SOC 39-9021)	Female																
Personal care aides 4610 (SOC 39-9021)	Number	793 765	86 035	63 625	381 025	185 805	9 065	49 955	3 660	2 010	5 020	1 250	1 355	(X)	(X)	(X)	4 960
Personal care aides 4610 (SOC 39-9021)	Percent	85.6%	9.3%	6.9%	41.1%	20.0%	1.0%	5.4%	0.4%	0.2%	0.5%	0.1%	0.1%	(X)	(X)	(X)	0.5%
Recreation and fitness workers 4620 (SOC 39-9030)	Total both sexes																
Recreation and fitness workers 4620 (SOC 39-9030)	Number	400 220	21 930	14 695	295 895	44 765	3 025	10 790	710	1 825	1 545	1 935	510	(X)	(X)	(X)	2 590
Recreation and fitness workers 4620 (SOC 39-9030)	Percent	100.0%	5.5%	3.7%	73.9%	11.2%	0.8%	2.7%	0.2%	0.5%	0.4%	0.5%	0.1%	(X)	(X)	(X)	0.6%
Recreation and fitness workers 4620 (SOC 39-9030)	Male																
Recreation and fitness workers 4620 (SOC 39-9030)	Number	143 280	9 495	6 770	96 425	20 690	1 295	4 815	280	685	570	815	200	(X)	(X)	(X)	1 240
Recreation and fitness workers 4620 (SOC 39-9030)	Percent	35.8%	2.4%	1.7%	24.1%	5.2%	0.3%	1.2%	0.1%	0.2%	0.1%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Recreation and fitness workers 4620 (SOC 39-9030)	Female																
Recreation and fitness workers 4620 (SOC 39-9030)	Number	256 940	12 440	7 930	199 470	24 075	1 730	5 975	425	1 140	975	1 125	310	(X)	(X)	(X)	1 350
Recreation and fitness workers 4620 (SOC 39-9030)	Percent	64.2%	3.1%	2.0%	49.8%	6.0%	0.4%	1.5%	0.1%	0.3%	0.2%	0.3%	0.1%	(X)	(X)	(X)	0.3%
Residential advisors 4640 (SOC 39-9041)	Total both sexes																
Residential advisors 4640 (SOC 39-9041)	Number	73 260	2 155	2 220	44 950	18 385	1 110	2 390	75	550	340	405	170	(X)	(X)	(X)	505
Residential advisors 4640 (SOC 39-9041)	Percent	100.0%	2.9%	3.0%	61.4%	25.1%	1.5%	3.3%	0.1%	0.8%	0.5%	0.6%	0.2%	(X)	(X)	(X)	0.7%
Residential advisors 4640 (SOC 39-9041)	Male																
Residential advisors 4640 (SOC 39-9041)	Number	26 780	1 000	775	17 070	5 960	380	900	20	140	100	110	90	(X)	(X)	(X)	240
Residential advisors 4640 (SOC 39-9041)	Percent	36.6%	1.4%	1.1%	23.3%	8.1%	0.5%	1.2%	0.0%	0.2%	0.1%	0.2%	0.1%	(X)	(X)	(X)	0.3%
Residential advisors 4640 (SOC 39-9041)	Female																
Residential advisors 4640 (SOC 39-9041)	Number	46 475	1 155	1 445	27 880	12 425	730	1 495	55	410	240	295	80	(X)	(X)	(X)	265
Residential advisors 4640 (SOC 39-9041)	Percent	63.4%	1.6%	2.0%	38.1%	17.0%	1.0%	2.0%	0.1%	0.6%	0.3%	0.4%	0.1%	(X)	(X)	(X)	0.4%
Personal care and service workers all other 4650 (SOC	Total both sexes																
Personal care and service workers, all other 4650 (SOC	Number	95,890	8,595	5,885	63,905	10,115	760	3,965	385	280	670	490	195	(X)	(X)	(X)	650
Personal care and service workers all other 4650 (SOC	Percent	100.0%	9.0%	6.1%	66.6%	10.5%	0.8%	4.1%	0.4%	0.3%	0.7%	0.5%	0.2%	(X)	(X)	(X)	0.7%
Personal care and service workers all other 4650 (SOC	Male																
Personal care and service workers, all other 4650 (SOC	Number	49,830	5,655	3,545	31,695	4,975	455	2,060	310	95	295	235	155	(X)	(X)	(X)	355
Personal care and service workers all other 4650 (SOC	Percent	52.0%	5.9%	3.7%	33.1%	5.2%	0.5%	2.1%	0.3%	0.1%	0.3%	0.2%	0.2%	(X)	(X)	(X)	0.4%
Personal care and service workers all other 4650 (SOC	Female																
Personal care and service workers all other 4650 (SOC	Number	46 065	2 940	2 340	32 210	5 135	305	1 905	75	185	375	255	35	(X)	(X)	(X)	295
Personal care and service workers all other 4650 (SOC	Percent	48.0%	3.1%	2.4%	33.6%	5.4%	0.3%	2.0%	0.1%	0.2%	0.4%	0.3%	0.0%	(X)	(X)	(X)	0.3%
First-line supervisors of reta l sales workers 4700 (SOC 41-	Total both sexes																
First-line supervisors of reta l sales workers 4700 (SOC 41-	Number	3 182 300	214 965	137 125	2 350 140	248 755	13 955	165 210	3 815	6 360	13 405	9 505	1 875	(X)	(X)	(X)	17 190
First-line supervisors of reta l sales workers 4700 (SOC 41-	Percent	100.0%	6.8%	4.3%	73.9%	7.8%	0.4%	5.2%	0.1%	0.2%	0.4%	0.3%	0.1%	(X)	(X)	(X)	0.5%
First-line supervisors of reta l sales workers 4700 (SOC 41-	Male																
First-line supervisors of reta l sales workers 4700 (SOC 41-	Number	1 765 580	117 740	74 815	1 318 455	116 110	6 625	104 625	1 760	3 240	6 440	5 215	800	(X)	(X)	(X)	9 760

First-line supervisors of retail sales workers 4700 (SOC 41-	Percent	55.5%	3.7%	2.4%	41.4%	3.6%	0.2%	3.3%	0.1%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.3%
First-line supervisors of retail sales workers 4700 (SOC 41-	Female																
First-line supervisors of retail sales workers 4700 (SOC 41-	Number	1 416 725	97 225	62 315	1 031 690	132 645	7 335	60 585	2 055	3 120	6 965	4 290	1 075	(X)	(X)	(X)	7 430
First-line supervisors of retail sales workers 4700 (SOC 41-	Percent	44.5%	3.1%	2.0%	32.4%	4.2%	0.2%	1.9%	0.1%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.2%
First-line supervisors of non-retail sales workers 4710	Total, both sexes																
First-line supervisors of non-retail sales workers 4710	Number	1 267 795	84 980	47 595	967 525	79 360	4 045	68 395	1 495	1 695	4 255	2 590	460	(X)	(X)	(X)	5 395
First-line supervisors of non-retail sales workers 4710	Percent	100.0%	6.7%	3.8%	76.3%	6.3%	0.3%	5.4%	0.1%	0.1%	0.3%	0.2%	0.0%	(X)	(X)	(X)	0.4%
First-line supervisors of non-retail sales workers 4710	Male																
First-line supervisors of non-retail sales workers 4710	Number	896 935	59 085	32 750	698 410	46 570	2 720	47 365	890	1 105	2 870	1 525	245	(X)	(X)	(X)	3 410
First-line supervisors of non-retail sales workers 4710	Percent	70.7%	4.7%	2.6%	55.1%	3.7%	0.2%	3.7%	0.1%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.3%
First-line supervisors of non-retail sales workers 4710	Female																
First-line supervisors of non-retail sales workers 4710	Number	370 855	25 900	14 845	269 115	32 795	1 325	21 035	605	595	1 385	1 060	215	(X)	(X)	(X)	1 985
First-line supervisors of non-retail sales workers 4710	Percent	29.3%	2.0%	1.2%	21.2%	2.6%	0.1%	1.7%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Cashiers 4720 (SOC 41-2010)	Total, both sexes																
Cashiers 4720 (SOC 41-2010)	Number	3 703 420	379 480	289 245	2 050 995	652 615	30 745	212 035	8 700	19 005	18 705	12 445	3 490	(X)	(X)	(X)	25 950
Cashiers 4720 (SOC 41-2010)	Percent	100.0%	10.2%	7.8%	55.4%	17.6%	0.8%	5.7%	0.2%	0.5%	0.5%	0.3%	0.1%	(X)	(X)	(X)	0.7%
Cashiers 4720 (SOC 41-2010)	Male																
Cashiers 4720 (SOC 41-2010)	Number	936 865	101 995	76 195	512 610	133 870	6 980	81 195	1 630	5 450	4 175	4 440	840	(X)	(X)	(X)	7 490
Cashiers 4720 (SOC 41-2010)	Percent	25.3%	2.8%	2.1%	13.8%	3.6%	0.2%	2.2%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Cashiers 4720 (SOC 41-2010)	Female																
Cashiers 4720 (SOC 41-2010)	Number	2 766 555	277 480	213 055	1 538 390	518 745	23 765	130 840	7 070	13 555	14 535	8 005	2 650	(X)	(X)	(X)	18 465
Cashiers 4720 (SOC 41-2010)	Percent	74.7%	7.5%	5.8%	41.5%	14.0%	0.6%	3.5%	0.2%	0.4%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.5%
Counter and rental clerks 4740 (SOC 41-2021)	Total, both sexes																
Counter and rental clerks 4740 (SOC 41-2021)	Number	139 590	11 850	8 705	91 790	15 935	1 025	7 325	335	320	985	535	65	(X)	(X)	(X)	715
Counter and rental clerks 4740 (SOC 41-2021)	Percent	100.0%	8.5%	6.2%	65.8%	11.4%	0.7%	5.2%	0.2%	0.2%	0.7%	0.4%	0.0%	(X)	(X)	(X)	0.5%
Counter and rental clerks 4740 (SOC 41-2021)	Male																
Counter and rental clerks 4740 (SOC 41-2021)	Number	61 515	4 955	3 310	42 315	6 640	355	2 705	55	115	395	360	10	(X)	(X)	(X)	295
Counter and rental clerks 4740 (SOC 41-2021)	Percent	44.1%	3.5%	2.4%	30.3%	4.8%	0.3%	1.9%	0.0%	0.1%	0.3%	0.3%	0.0%	(X)	(X)	(X)	0.2%
Counter and rental clerks 4740 (SOC 41-2021)	Female																
Counter and rental clerks 4740 (SOC 41-2021)	Number	78 075	6 895	5 395	49 475	9 295	670	4 620	285	200	590	175	55	(X)	(X)	(X)	420
Counter and rental clerks 4740 (SOC 41-2021)	Percent	55.9%	4.9%	3.9%	35.4%	6.7%	0.5%	3.3%	0.2%	0.1%	0.4%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Parts salespersons 4750 (SOC 41-2022)	Total, both sexes																
Parts salespersons 4750 (SOC 41-2022)	Number	118 355	9 635	6 755	92 805	4 870	545	2 420	40	180	400	225	95	(X)	(X)	(X)	380
Parts salespersons 4750 (SOC 41-2022)	Percent	100.0%	8.1%	5.7%	78.4%	4.1%	0.5%	2.0%	0.0%	0.2%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.3%
Parts salespersons 4750 (SOC 41-2022)	Male																
Parts salespersons 4750 (SOC 41-2022)	Number	104 540	8 535	6 005	82 130	3 950	460	2 275	40	130	370	225	85	(X)	(X)	(X)	335
Parts salespersons 4750 (SOC 41-2022)	Percent	88.3%	7.2%	5.1%	69.4%	3.3%	0.4%	1.9%	0.0%	0.1%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.3%
Parts salespersons 4750 (SOC 41-2022)	Female																
Parts salespersons 4750 (SOC 41-2022)	Number	13 820	1 100	750	10 675	920	90	150	0	50	30	0	10	(X)	(X)	(X)	45
Parts salespersons 4750 (SOC 41-2022)	Percent	11.7%	0.9%	0.6%	9.0%	0.8%	0.1%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Retail salespersons 4760 (SOC 41-2031)	Total, both sexes																
Retail salespersons 4760 (SOC 41-2031)	Number	3 747 080	299 385	198 290	2 580 665	411 275	16 770	167 415	4 265	13 205	15 175	15 330	3 175	(X)	(X)	(X)	22 135
Retail salespersons 4760 (SOC 41-2031)	Percent	100.0%	8.0%	5.3%	68.9%	11.0%	0.4%	4.5%	0.1%	0.4%	0.4%	0.4%	0.1%	(X)	(X)	(X)	0.6%
Retail salespersons 4760 (SOC 41-2031)	Male																
Retail salespersons 4760 (SOC 41-2031)	Number	1 821 005	140 570	91 035	1 291 145	182 020	6 210	77 485	1 770	5 980	7 050	6 885	1 190	(X)	(X)	(X)	9 665
Retail salespersons 4760 (SOC 41-2031)	Percent	48.6%	3.8%	2.4%	34.5%	4.9%	0.2%	2.1%	0.0%	0.2%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Retail salespersons 4760 (SOC 41-2031)	Female																
Retail salespersons 4760 (SOC 41-2031)	Number	1 926 075	158 810	107 255	1 289 520	229 255	10 565	89 925	2 495	7 230	8 125	8 445	1 985	(X)	(X)	(X)	12 470
Retail salespersons 4760 (SOC 41-2031)	Percent	51.4%	4.2%	2.9%	34.4%	6.1%	0.3%	2.4%	0.1%	0.2%	0.2%	0.2%	0.1%	(X)	(X)	(X)	0.3%
Advertising sales agents 4800 (SOC 41-3011)	Total, both sexes																
Advertising sales agents 4800 (SOC 41-3011)	Number	242,985	12,940	7,605	194,355	17,615	595	6,650	270	435	715	715	275	(X)	(X)	(X)	810
Advertising sales agents 4800 (SOC 41-3011)	Percent	100.0%	5.3%	3.1%	80.0%	7.2%	0.2%	2.7%	0.1%	0.2%	0.3%	0.3%	0.1%	(X)	(X)	(X)	0.3%
Advertising sales agents 4800 (SOC 41-3011)	Male																
Advertising sales agents 4800 (SOC 41-3011)	Number	115,555	6,165	3,585	92,370	8,770	200	2,800	195	230	315	325	135	(X)	(X)	(X)	455
Advertising sales agents 4800 (SOC 41-3011)	Percent	47.6%	2.5%	1.5%	38.0%	3.6%	0.1%	1.2%	0.1%	0.1%	0.1%	0.1%	0.1%	(X)	(X)	(X)	0.2%
Advertising sales agents 4800 (SOC 41-3011)	Female																
Advertising sales agents 4800 (SOC 41-3011)	Number	127 430	6 775	4 020	101 985	8 845	395	3 850	70	205	400	390	140	(X)	(X)	(X)	355
Advertising sales agents 4800 (SOC 41-3011)	Percent	52.4%	2.8%	1.7%	42.0%	3.6%	0.2%	1.6%	0.0%	0.1%	0.2%	0.2%	0.1%	(X)	(X)	(X)	0.1%
Insurance sales agents 4810 (SOC 41-3021)	Total, both sexes																
Insurance sales agents 4810 (SOC 41-3021)	Number	561 510	32 365	15 955	448 765	40 020	1 440	16 890	300	740	1 540	1 265	275	(X)	(X)	(X)	1 955
Insurance sales agents 4810 (SOC 41-3021)	Percent	100.0%	5.8%	2.8%	79.9%	7.1%	0.3%	3.0%	0.1%	0.1%	0.3%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Insurance sales agents 4810 (SOC 41-3021)	Male																
Insurance sales agents 4810 (SOC 41-3021)	Number	305 270	13 330	6 735	254 480	18 380	560	8 915	95	405	795	590	180	(X)	(X)	(X)	810
Insurance sales agents 4810 (SOC 41-3021)	Percent	54.4%	2.4%	1.2%	45.3%	3.3%	0.1%	1.6%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Insurance sales agents 4810 (SOC 41-3021)	Female																
Insurance sales agents 4810 (SOC 41-3021)	Number	256 240	19 035	9 220	194 285	21 640	880	7 975	205	335	745	675	90	(X)	(X)	(X)	1 150
Insurance sales agents 4810 (SOC 41-3021)	Percent	45.6%	3.4%	1.6%	34.6%	3.9%	0.2%	1.4%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Securities commodities and financial services sales	Total both sexes																
Securities commodities and financial services sales	Number	375 110	19 545	10 055	293 530	23 450	525	23 095	245	525	735	1 405	145	(X)	(X)	(X)	1 860
Securities commodities and financial services sales	Percent	100.0%	5.2%	2.7%	78.3%	6.3%	0.1%	6.2%	0.1%	0.1%	0.2%	0.4%	0.0%	(X)	(X)	(X)	0.5%
Securities commodities and financial services sales	Male																
Securities commodities and financial services sales	Number	258 140	11 990	5 495	209 005	12 900	370	15 165	150	415	485	1 045	75	(X)	(X)	(X)	1 035
Securities commodities and financial services sales	Percent	68.8%	3.2%	1.5%	55.7%	3.4%	0.1%	4.0%	0.0%	0.1%	0.1%	0.3%	0.0%	(X)	(X)	(X)	0.3%
Securities commodities and financial services sales	Female																
Securities commodities and financial services sales	Number	116 970	7 550	4 560	84 525	10 550	150	7 930	95	110	245	360	70	(X)	(X)	(X)	825
Securities, commodities, and financial services sales	Percent	31.2%	2.0%	1.2%	22.5%	2.8%	0.0%	2.1%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Travel agents 4830 (SOC 41-3041)	Total, both sexes																
Travel agents 4830 (SOC 41-3041)	Number	86 860	4 950	3 005	64 635	5 670	300	6 910	145	25	260	225	0	(X)	(X)	(X)	730
Travel agents 4830 (SOC 41-3041)	Percent	100.0%	5.7%	3.5%	74.4%	6.5%	0.3%	8.0%	0.2%	0.0%	0.3%	0.3%	0.0%	(X)	(X)	(X)	0.8%
Travel agents 4830 (SOC 41-3041)	Male																
Travel agents 4830 (SOC 41-3041)	Number	17 155	1 220	715	10 955	1 450	75	2 390	15	0	55	55	0	(X)	(X)	(X)	225
Travel agents 4830 (SOC 41-3041)	Percent	19.8%	1.4%	0.8%	12.6%	1.7%	0.1%	2.8%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Travel agents 4830 (SOC 41-3041)	Female																
Travel agents 4830 (SOC 41-3041)	Number	69 705	3 730	2 290	53 680	4 220	225	4 520	130	25	205	175	0	(X)	(X)	(X)	505
Travel agents 4830 (SOC 41-3041)	Percent	80.2%	4.3%	2.6%	61.8%	4.9%	0.3%	5.2%	0.1%	0.0%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.6%
Sales representatives services all other 4840 (SOC 41-	Total both sexes																
Sales representatives services all other 4840 (SOC 41-	Number	672 815	39 390	21 190	529 150	49 545	2 125	22 455	580	1 180	2 215	1 895	395	(X)	(X)	(X)	2 695
Sales representatives services all other 4840 (SOC 41-	Percent	100.0%	5.9%	3.1%	78.6%	7.4%	0.3%	3.3%	0.1%	0.2%	0.3%	0.3%	0.1%	(X)	(X)	(X)	0.4%
Sales representatives services all other 4840 (SOC 41-	Male																
Sales representatives services all other 4840 (SOC 41-	Number	444 230	24 305	12 665	359 990	26 815	1 365	13 845	400	570	1 085	1 225	205	(X)	(X)	(X)	1 765
Sales representatives services all other 4840 (SOC 41-	Percent	66.0%	3.6%	1.9%	53.5%	4.0%	0.2%	2.1%	0.1%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Sales representatives services all other 4840 (SOC 41-	Female																
Sales representatives services all other 4840 (SOC 41-	Number	228 580	15 085	8 525	169 160	22 730	765	8 610	175	615	1 130	675	190	(X)	(X)	(X)	930
Sales representatives services all other 4840 (SOC 41-	Percent	34.0%	2.2%	1.3%	25.1%	3.4%	0.1%	1.3%	0.0%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Sales representatives wholesale and manufacturing 4850	Total both sexes																
Sales representatives wholesale and manufacturing 4850	Number	1 541 725	83 135	46 015	1 283 585	56 185	3 475	52 175	1 400	1 450	4 815	4 070	545	(X)	(X)	(X)	4 865
Sales representatives wholesale and manufacturing 4850	Percent	100.0%	5.4%	3.0%	83.3%	3.6%	0.2%	3.4%	0.1%	0.1%	0.3%	0.3%	0.0%	(X)	(X)	(X)	0.3%
Sales representatives wholesale and manufacturing 4850	Male																
Sales representatives wholesale and manufacturing 4850	Number	1 121 975	56 950	30 570	951 490	36 325	2 130	33 135	960	810	3 400	2 655	450	(X)	(X)	(X)	3 100
Sales representatives wholesale and manufacturing 4850	Percent	72.8%	3.7%	2.0%	61.7%	2.4%	0.1%	2.1%	0.1%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Sales representatives, wholesale and manufacturing 4850	Female																
Sales representatives wholesale and manufacturing 4850	Number	419 745	26 185	15 440	332 095	19 860	1 345	19 040	445	635	1 415	1 420	95	(X)	(X)	(X)	1 765
Sales representatives wholesale and manufacturing 4850	Percent	27.2%	1.7%	1.0%	21.5%	1.3%	0.1%	1.2%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Models, demonstrators, and product promoters 4900 (SOC	Total, both sexes																
Models demonstrators and product promoters 4900 (SOC	Number	70 935	5 320	3 755	49 760	7 445	365	2 575	135	355	370	455	45	(X)	(X)	(X)	355
Models demonstrators and product promoters 4900 (SOC	Percent	100.0%	7.5%	5.3%	70.1%	10.5%	0.5%	3.6%	0.2%	0.5%	0.5%	0.6%	0.1%	(X)	(X)	(X)	0.5%
Models demonstrators and product promoters 4900 (SOC	Male																
Models demonstrators and product promoters 4900 (SOC	Number	17 715	1 215	1 125	11 545	2 530	135	670	25	125	115	140	10	(X)	(X)	(X)	75
Models demonstrators and product promoters 4900 (SOC	Percent	25.0%	1.7%	1.6%	16.3%	3.6%	0.2%	0.9%	0.0%	0.2%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.1%
Models demonstrators and product promoters 4900 (SOC	Female																
Models demonstrators and product promoters 4900 (SOC	Number	53 220	4 105	2 630	38 210	4 910	230	1 905	105	230	255	315	40	(X)	(X)	(X)	285
Models demonstrators and product promoters 4900 (SOC	Percent	75.0%	5.8%	3.7%	53.9%	6.9%	0.3%	2.7%	0.1%	0.3%	0.4%	0.4%	0.1%	(X)	(X)	(X)	0.4%
Real estate brokers and sales agents 4920 (SOC 41-	Total both sexes																
Real estate brokers and sales agents 4920 (SOC 41-	Number	899 480	52 850	25 200	717 600	51 120	2 145	39 160	670	1 080	2 990	2 235	520	(X)	(X)	(X)	3 905
Real estate brokers and sales agents 4920 (SOC 41-	Percent	100.0%	5.9%	2.8%	79.8%	5.7%	0.2%	4.4%	0.1%	0.1%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Real estate brokers and sales agents 4920 (SOC 41-	Male																
Real estate brokers and sales agents 4920 (SOC 41-	Number	402 545	24 065	11 080	321 015	21 680	900	18 835	265	560	1 305	925	255	(X)	(X)	(X)	1 655
Real estate brokers and sales agents 4920 (SOC 41-	Percent	44.8%	2.7%	1.2%	35.7%	2.4%	0.1%	2.1%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Real estate brokers and sales agents 4920 (SOC 41-	Female																
Real estate brokers and sales agents 4920 (SOC 41-	Number	496 935	28 785	14 120	396 580	29 435	1 245	20 325	405	525	1 685	1 315	265	(X)	(X)	(X)	2 255
Real estate brokers and sales agents 4920 (SOC 41-	Percent	55.2%	3.2%	1.6%	44.1%	3.3%	0.1%	2.3%	0.0%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Sales engineers 4930 (SOC 41-9031)	Total, both sexes																
Sales engineers 4930 (SOC 41-9031)	Number	32 345	1 185	620	27 450	735	105	2 030	0	4	100	35	10	(X)	(X)	(X)	75
Sales engineers 4930 (SOC 41-9031)	Percent	100.0%	3.7%	1.9%	84.9%	2.3%	0.3%	6.3%	0.0%	0.0%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Sales engineers 4930 (SOC 41-9031)	Male																
Sales engineers 4930 (SOC 41-9031)	Number	30,205	1,135	575	25,815	635	100	1,760	0	4	100	20	0	(X)	(X)	(X)	65
Sales engineers 4930 (SOC 41-9031)	Percent	93.4%	3.5%	1.8%	79.8%	2.0%	0.3%	5.4%	0.0%	0.0%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Sales engineers 4930 (SOC 41-9031)	Female																
Sales engineers 4930 (SOC 41-9031)	Number	2,135	50	45	1,635	100	4	270	0	0	0	10	10	(X)	(X)	(X)	10
Sales engineers 4930 (SOC 41-9031)	Percent	6.6%	0.2%	0.1%	5.1%	0.3%	0.0%	0.8%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Telemarketers 4940 (SOC 41-9041)	Total, both sexes																
Telemarketers 4940 (SOC 41-9041)	Number	183 185	16 320	8 645	107 075	42 050	1 100	3 190	455	1 135	1 110	570	250	(X)	(X)	(X)	1 290
Telemarketers 4940 (SOC 41-9041)	Percent	100.0%	8.9%	4.7%	58.5%	23.0%	0.6%	1.7%	0.2%	0.6%	0.6%	0.3%	0.1%	(X)	(X)	(X)	0.7%
Telemarketers 4940 (SOC 41-9041)	Male																
Telemarketers 4940 (SOC 41-9041)	Number	68 750	5 815	3 625	41 600	14 215	320	1 450	90	575	500	120	50	(X)	(X)	(X)	385
Telemarketers 4940 (SOC 41-9041)	Percent	37.5%	3.2%	2.0%	22.7%	7.8%	0.2%	0.8%	0.0%	0.3%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Telemarketers 4940 (SOC 41-9041)	Female																
Telemarketers 4940 (SOC 41-9041)	Number	114 435	10 505	5 020	65 475	27 835	780	1 740	365	555	610	450	200	(X)	(X)	(X)	905

Telemarketers 4940 (SOC 41-9041)	Percent	62.5%	5.7%	2.7%	35.7%	15.2%	0.4%	0.9%	0.2%	0.3%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.5%
Door-to-door sales workers news and street vendors and	Total both sexes																
Door-to-door sales workers news and street vendors and	Number	211 790	21 670	14 780	145 205	19 790	1 115	5 075	305	485	1 400	680	160	(X)	(X)	(X)	1 120
Door-to-door sales workers, news and street vendors, and	Percent	100.0%	10.2%	7.0%	68.6%	9.3%	0.5%	2.4%	0.1%	0.2%	0.7%	0.3%	0.1%	(X)	(X)	(X)	0.5%
Door-to-door sales workers news and street vendors and	Male																
Door-to-door sales workers news and street vendors and	Number	90 210	9 240	6 385	58 895	10 725	380	2 915	65	245	480	420	45	(X)	(X)	(X)	410
Door-to-door sales workers news and street vendors and	Percent	42.6%	4.4%	3.0%	27.8%	5.1%	0.2%	1.4%	0.0%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Door-to-door sales workers news and street vendors and	Female																
Door-to-door sales workers news and street vendors and	Number	121 580	12 430	8 395	86 310	9 065	735	2 160	240	240	915	260	115	(X)	(X)	(X)	710
Door-to-door sales workers news and street vendors and	Percent	57.4%	5.9%	4.0%	40.8%	4.3%	0.3%	1.0%	0.1%	0.1%	0.4%	0.1%	0.1%	(X)	(X)	(X)	0.3%
Sales and related workers all other 4965 (SOC 41-9099)	Total both sexes																
Sales and related workers all other 4965 (SOC 41-9099)	Number	251 580	13 775	7 675	196 395	20 895	1 030	8 570	300	535	915	645	70	(X)	(X)	(X)	785
Sales and related workers all other 4965 (SOC 41-9099)	Percent	100.0%	5.5%	3.1%	78.1%	8.3%	0.4%	3.4%	0.1%	0.2%	0.4%	0.3%	0.0%	(X)	(X)	(X)	0.3%
Sales and related workers all other 4965 (SOC 41-9099)	Male																
Sales and related workers all other 4965 (SOC 41-9099)	Number	124 920	6 180	4 080	100 590	8 250	390	4 115	140	225	375	270	0	(X)	(X)	(X)	305
Sales and related workers all other 4965 (SOC 41-9099)	Percent	49.7%	2.5%	1.6%	40.0%	3.3%	0.2%	1.6%	0.1%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Sales and related workers all other 4965 (SOC 41-9099)	Female																
Sales and related workers all other 4965 (SOC 41-9099)	Number	126 660	7 595	3 595	95 800	12 645	640	4 455	160	310	540	375	70	(X)	(X)	(X)	475
Sales and related workers all other 4965 (SOC 41-9099)	Percent	50.3%	3.0%	1.4%	38.1%	5.0%	0.3%	1.8%	0.1%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.2%
First-line supervisors of office and administrative support	Total both sexes																
First-line supervisors of office and administrative support	Number	1 615 235	110 135	68 155	1 171 120	175 185	7 675	57 895	2 815	2 975	5 945	4 025	985	(X)	(X)	(X)	8 325
First-line supervisors of office and administrative support	Percent	100.0%	6.8%	4.2%	72.5%	10.8%	0.5%	3.6%	0.2%	0.2%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.5%
First-line supervisors of office and administrative support	Male																
First-line supervisors of office and administrative support	Number	558 590	41 470	27 370	392 390	62 460	2 410	24 105	975	700	1 885	1 345	390	(X)	(X)	(X)	3 085
First-line supervisors of office and administrative support	Percent	34.6%	2.6%	1.7%	24.3%	3.9%	0.1%	1.5%	0.1%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
First-line supervisors of office and administrative support	Female																
First-line supervisors of office and administrative support	Number	1 056 645	68 665	40 785	778 730	112 720	5 265	33 795	1 840	2 270	4 055	2 680	600	(X)	(X)	(X)	5 240
First-line supervisors of office and administrative support	Percent	65.4%	4.3%	2.5%	48.2%	7.0%	0.3%	2.1%	0.1%	0.1%	0.3%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Switchboard operators, including answering service 5010	Total, both sexes																
Switchboard operators including answering service 5010	Number	47 655	2 860	2 210	31 655	8 565	405	1 240	130	75	160	135	25	(X)	(X)	(X)	195
Switchboard operators including answering service 5010	Percent	100.0%	6.0%	4.6%	66.4%	18.0%	0.8%	2.6%	0.3%	0.2%	0.3%	0.3%	0.1%	(X)	(X)	(X)	0.4%
Switchboard operators including answering service 5010	Male																
Switchboard operators including answering service 5010	Number	7 450	615	435	4 315	1 515	80	360	30	0	10	25	20	(X)	(X)	(X)	45
Switchboard operators including answering service 5010	Percent	15.6%	1.3%	0.9%	9.1%	3.2%	0.2%	0.8%	0.1%	0.0%	0.0%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Switchboard operators including answering service 5010	Female																
Switchboard operators including answering service 5010	Number	40 205	2 245	1 775	27 335	7 055	325	880	100	75	150	110	4	(X)	(X)	(X)	150
Switchboard operators including answering service 5010	Percent	84.4%	4.7%	3.7%	57.4%	14.8%	0.7%	1.8%	0.2%	0.2%	0.3%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Telephone operators 5020 (SOC 43-2021)	Total both sexes																
Telephone operators 5020 (SOC 43-2021)	Number	56 475	4 770	4 050	30 960	13 470	390	1 590	75	200	250	170	185	(X)	(X)	(X)	360
Telephone operators 5020 (SOC 43-2021)	Percent	100.0%	8.4%	7.2%	54.8%	23.9%	0.7%	2.8%	0.1%	0.4%	0.4%	0.3%	0.3%	(X)	(X)	(X)	0.6%
Telephone operators 5020 (SOC 43-2021)	Male																
Telephone operators 5020 (SOC 43-2021)	Number	11 530	1 320	1 030	6 010	2 430	40	470	0	35	60	45	20	(X)	(X)	(X)	75
Telephone operators 5020 (SOC 43-2021)	Percent	20.4%	2.3%	1.8%	10.6%	4.3%	0.1%	0.8%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Telephone operators 5020 (SOC 43-2021)	Female																
Telephone operators 5020 (SOC 43-2021)	Number	44 945	3 450	3 020	24 950	11 040	355	1 120	75	170	190	125	165	(X)	(X)	(X)	280
Telephone operators 5020 (SOC 43-2021)	Percent	79.6%	6.1%	5.3%	44.2%	19.5%	0.6%	2.0%	0.1%	0.3%	0.3%	0.2%	0.3%	(X)	(X)	(X)	0.5%
Communications equipment operators all other 5030	Total both sexes																
Communications equipment operators all other 5030	Number	11 220	705	510	7 725	1 665	55	400	30	15	20	50	0	(X)	(X)	(X)	45
Communications equipment operators all other 5030	Percent	100.0%	6.3%	4.5%	68.9%	14.8%	0.5%	3.6%	0.3%	0.1%	0.2%	0.4%	0.0%	(X)	(X)	(X)	0.4%
Communications equipment operators all other 5030	Male																
Communications equipment operators, all other 5030	Number	4,990	320	235	3,500	775	4	130	0	0	0	0	0	(X)	(X)	(X)	25
Communications equipment operators all other 5030	Percent	44.5%	2.9%	2.1%	31.2%	6.9%	0.0%	1.2%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.2%
Communications equipment operators all other 5030	Female																
Communications equipment operators, all other 5030	Number	6,230	385	275	4,225	895	50	270	30	15	20	50	0	(X)	(X)	(X)	20
Communications equipment operators all other 5030	Percent	55.5%	3.4%	2.5%	37.7%	8.0%	0.4%	2.4%	0.3%	0.1%	0.2%	0.4%	0.0%	(X)	(X)	(X)	0.2%
Bill and account collectors 5100 (SOC 43-3011)	Total both sexes																
Bill and account collectors 5100 (SOC 43-3011)	Number	245 240	22 440	14 845	145 640	51 225	1 095	5 580	450	1 020	955	500	360	(X)	(X)	(X)	1 130
Bill and account collectors 5100 (SOC 43-3011)	Percent	100.0%	9.2%	6.1%	59.4%	20.9%	0.4%	2.3%	0.2%	0.4%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.5%
Bill and account collectors 5100 (SOC 43-3011)	Male																
Bill and account collectors 5100 (SOC 43-3011)	Number	72 845	7 225	4 005	44 210	14 115	415	1 730	50	325	135	125	35	(X)	(X)	(X)	470
Bill and account collectors 5100 (SOC 43-3011)	Percent	29.7%	2.9%	1.6%	18.0%	5.8%	0.2%	0.7%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Bill and account collectors 5100 (SOC 43-3011)	Female																
Bill and account collectors 5100 (SOC 43-3011)	Number	172 395	15 215	10 840	101 430	37 110	680	3 850	400	695	820	370	325	(X)	(X)	(X)	660
Bill and account collectors 5100 (SOC 43-3011)	Percent	70.3%	6.2%	4.4%	41.4%	15.1%	0.3%	1.6%	0.2%	0.3%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.3%
Billing and posting clerks 5110 (SOC 43-3021)	Total both sexes																
Billing and posting clerks 5110 (SOC 43-3021)	Number	497 360	38 020	24 690	343 295	58 965	2 890	21 300	1 000	1 160	2 025	1 150	225	(X)	(X)	(X)	2 635
Billing and posting clerks 5110 (SOC 43-3021)	Percent	100.0%	7.6%	5.0%	69.0%	11.9%	0.6%	4.3%	0.2%	0.2%	0.4%	0.2%	0.0%	(X)	(X)	(X)	0.5%
Billing and posting clerks 5110 (SOC 43-3021)	Male																
Billing and posting clerks 5110 (SOC 43-3021)	Number	52 835	4 600	2 995	32 900	6 730	235	4 090	215	245	245	250	25	(X)	(X)	(X)	300
Billing and posting clerks 5110 (SOC 43-3021)	Percent	10.6%	0.9%	0.6%	6.6%	1.4%	0.0%	0.8%	0.0%	0.0%	0.0%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Billing and posting clerks 5110 (SOC 43-3021)	Female																
Billing and posting clerks 5110 (SOC 43-3021)	Number	444 525	33 415	21 690	310 395	52 235	2 655	17 210	785	915	1 780	895	205	(X)	(X)	(X)	2 335
Billing and posting clerks 5110 (SOC 43-3021)	Percent	89.4%	6.7%	4.4%	62.4%	10.5%	0.5%	3.5%	0.2%	0.2%	0.4%	0.2%	0.0%	(X)	(X)	(X)	0.5%
Bookkeeping accounting and auditing clerks 5120 (SOC	Total both sexes																
Bookkeeping accounting and auditing clerks 5120 (SOC	Number	1 548 285	91 560	51 925	1 188 730	119 985	8 860	65 750	2 150	2 055	5 690	3 710	850	(X)	(X)	(X)	7 020
Bookkeeping, accounting, and auditing clerks 5120 (SOC	Percent	100.0%	5.9%	3.4%	76.8%	7.7%	0.6%	4.2%	0.1%	0.1%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.5%
Bookkeeping accounting and auditing clerks 5120 (SOC	Male																
Bookkeeping accounting and auditing clerks 5120 (SOC	Number	176 925	13 710	8 345	118 415	19 045	885	13 605	370	375	405	530	125	(X)	(X)	(X)	1 115
Bookkeeping, accounting, and auditing clerks 5120 (SOC	Percent	11.4%	0.9%	0.5%	7.6%	1.2%	0.1%	0.9%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Bookkeeping accounting and auditing clerks 5120 (SOC	Female																
Bookkeeping accounting and auditing clerks 5120 (SOC	Number	1 371 360	77 850	43 580	1 070 315	100 935	7 975	52 145	1 780	1 680	5 285	3 180	725	(X)	(X)	(X)	5 910
Bookkeeping accounting and auditing clerks 5120 (SOC	Percent	88.6%	5.0%	2.8%	69.1%	6.5%	0.5%	3.4%	0.1%	0.1%	0.3%	0.2%	0.0%	(X)	(X)	(X)	0.4%
Gaming cage workers 5130 (SOC 43-3041)	Total both sexes																
Gaming cage workers 5130 (SOC 43-3041)	Number	13 970	1 060	1 010	6 920	1 915	1 080	1 450	30	85	255	15	75	(X)	(X)	(X)	80
Gaming cage workers 5130 (SOC 43-3041)	Percent	100.0%	7.6%	7.2%	49.5%	13.7%	7.7%	10.4%	0.2%	0.6%	1.8%	0.1%	0.5%	(X)	(X)	(X)	0.6%
Gaming cage workers 5130 (SOC 43-3041)	Male																
Gaming cage workers 5130 (SOC 43-3041)	Number	3 715	530	220	1 845	265	265	460	15	0	75	15	15	(X)	(X)	(X)	4
Gaming cage workers 5130 (SOC 43-3041)	Percent	26.6%	3.8%	1.6%	13.2%	1.9%	1.9%	3.3%	0.1%	0.0%	0.5%	0.1%	0.1%	(X)	(X)	(X)	0.0%
Gaming cage workers 5130 (SOC 43-3041)	Female																
Gaming cage workers 5130 (SOC 43-3041)	Number	10 260	530	790	5 075	1 650	815	985	15	85	180	0	60	(X)	(X)	(X)	75
Gaming cage workers 5130 (SOC 43-3041)	Percent	73.4%	3.8%	5.7%	36.3%	11.8%	5.8%	7.1%	0.1%	0.6%	1.3%	0.0%	0.4%	(X)	(X)	(X)	0.5%
Payroll and timekeeping clerks 5140 (SOC 43-3051)	Total both sexes																
Payroll and timekeeping clerks 5140 (SOC 43-3051)	Number	185 035	12 525	7 850	133 720	20 675	1 035	6 420	195	270	750	400	205	(X)	(X)	(X)	985
Payroll and timekeeping clerks 5140 (SOC 43-3051)	Percent	100.0%	6.8%	4.2%	72.3%	11.2%	0.6%	3.5%	0.1%	0.1%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.5%
Payroll and timekeeping clerks 5140 (SOC 43-3051)	Male																
Payroll and timekeeping clerks 5140 (SOC 43-3051)	Number	18 690	1 810	1 000	11 585	2 560	55	1 195	25	30	65	95	50	(X)	(X)	(X)	215
Payroll and timekeeping clerks 5140 (SOC 43-3051)	Percent	10.1%	1.0%	0.5%	6.3%	1.4%	0.0%	0.6%	0.0%	0.0%	0.0%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Payroll and timekeeping clerks 5140 (SOC 43-3051)	Female																
Payroll and timekeeping clerks 5140 (SOC 43-3051)	Number	166 345	10 715	6 850	122 135	18 120	980	5 220	170	245	685	300	155	(X)	(X)	(X)	770
Payroll and timekeeping clerks 5140 (SOC 43-3051)	Percent	89.9%	5.8%	3.7%	66.0%	9.8%	0.5%	2.8%	0.1%	0.1%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Procurement clerks 5150 (SOC 43-3061)	Total, both sexes																
Procurement clerks 5150 (SOC 43-3061)	Number	31 070	1 725	765	22 565	3 805	275	1 360	10	25	110	70	25	(X)	(X)	(X)	335
Procurement clerks 5150 (SOC 43-3061)	Percent	100.0%	5.6%	2.5%	72.6%	12.2%	0.9%	4.4%	0.0%	0.1%	0.4%	0.2%	0.1%	(X)	(X)	(X)	1.1%
Procurement clerks 5150 (SOC 43-3061)	Male																
Procurement clerks 5150 (SOC 43-3061)	Number	11 650	775	260	8 640	1 060	4	690	0	25	40	40	15	(X)	(X)	(X)	110
Procurement clerks 5150 (SOC 43-3061)	Percent	37.5%	2.5%	0.8%	27.8%	3.4%	0.0%	2.2%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.4%
Procurement clerks 5150 (SOC 43-3061)	Female																
Procurement clerks 5150 (SOC 43-3061)	Number	19 415	950	505	13 920	2 750	275	670	10	0	70	30	10	(X)	(X)	(X)	225
Procurement clerks 5150 (SOC 43-3061)	Percent	62.5%	3.1%	1.6%	44.8%	8.9%	0.9%	2.2%	0.0%	0.0%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.7%
Tellers 5160 (SOC 43-3071)	Total both sexes																
Tellers 5160 (SOC 43-3071)	Number	450 300	41 955	27 705	294 740	49 060	1 710	26 675	940	1 175	1 370	1 470	225	(X)	(X)	(X)	3 280
Tellers 5160 (SOC 43-3071)	Percent	100.0%	9.3%	6.2%	65.5%	10.9%	0.4%	5.9%	0.2%	0.3%	0.3%	0.3%	0.0%	(X)	(X)	(X)	0.7%
Tellers 5160 (SOC 43-3071)	Male																
Tellers 5160 (SOC 43-3071)	Number	63 885	8 770	5 560	34 240	6 955	100	6 785	200	280	200	290	15	(X)	(X)	(X)	485
Tellers 5160 (SOC 43-3071)	Percent	14.2%	1.9%	1.2%	7.6%	1.5%	0.0%	1.5%	0.0%	0.1%	0.0%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Tellers 5160 (SOC 43-3071)	Female																
Tellers 5160 (SOC 43-3071)	Number	386 415	33 185	22 145	260 500	42 105	1 615	19 885	740	895	1 170	1 175	210	(X)	(X)	(X)	2 795
Tellers 5160 (SOC 43-3071)	Percent	85.8%	7.4%	4.9%	57.9%	9.4%	0.4%	4.4%	0.2%	0.2%	0.3%	0.3%	0.0%	(X)	(X)	(X)	0.6%
Financial clerks all other 5165 (SOC 43-3099)	Total both sexes																
Financial clerks all other 5165 (SOC 43-3099)	Number	69 330	4 590	2 735	46 295	8 445	310	5 695	75	120	125	240	150	(X)	(X)	(X)	550
Financial clerks all other 5165 (SOC 43-3099)	Percent	100.0%	6.6%	3.9%	66.8%	12.2%	0.4%	8.2%	0.1%	0.2%	0.2%	0.3%	0.2%	(X)	(X)	(X)	0.8%
Financial clerks all other 5165 (SOC 43-3099)	Male																
Financial clerks all other 5165 (SOC 43-3099)	Number	23 300	1 565	900	15 590	2 100	90	2 620	25	55	25	140	15	(X)	(X)	(X)	185
Financial clerks all other 5165 (SOC 43-3099)	Percent	33.6%	2.3%	1.3%	22.5%	3.0%	0.1%	3.8%	0.0%	0.1%	0.0%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Financial clerks all other 5165 (SOC 43-3099)	Female																
Financial clerks, all other 5165 (SOC 43-3099)	Number	46,030	3,025	1,835	30,705	6,345	220	3,075	50	65	105	100	140	(X)	(X)	(X)	365
Financial clerks all other 5165 (SOC 43-3099)	Percent	66.4%	4.4%	2.6%	44.3%	9.2%	0.3%	4.4%	0.1%	0.1%	0.2%	0.1%	0.2%	(X)	(X)	(X)	0.5%
Brokerage clerks 5200 (SOC 43-4011)	Total both sexes																
Brokerage clerks 5200 (SOC 43-4011)	Number	10,460	580	440	7,860	970	30	485	25	0	0	40	0	(X)	(X)	(X)	30
Brokerage clerks 5200 (SOC 43-4011)	Percent	100.0%	5.5%	4.2%	75.1%	9.3%	0.3%	4.6%	0.2%	0.0%	0.0%	0.4%	0.0%	(X)	(X)	(X)	0.3%
Brokerage clerks 5200 (SOC 43-4011)	Male																
Brokerage clerks 5200 (SOC 43-4011)	Number	3 435	180	20	2 805	285	0	95	4	0	0	20	0	(X)	(X)	(X)	20
Brokerage clerks 5200 (SOC 43-4011)	Percent	32.8%	1.7%	0.2%	26.8%	2.7%	0.0%	0.9%	0.0%	0.0%	0.0%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Brokerage clerks 5200 (SOC 43-4011)	Female																
Brokerage clerks 5200 (SOC 43-4011)	Number	7 025	400	415	5 055	685	30	395	25	0	0	20	0	(X)	(X)	(X)	4
Brokerage clerks 5200 (SOC 43-4011)	Percent	67.2%	3.8%	4.0%	48.3%	6.5%	0.3%	3.8%	0.2%	0.0%	0.0%	0.2%	0.0%	(X)	(X)	(X)	0.0%
Court municipal and icense clerks 5220 (SOC 43-4031)	Total both sexes																
Court municipal and icense clerks 5220 (SOC 43-4031)	Number	95 185	7 340	3 780	66 085	13 380	965	2 465	135	55	325	150	115	(X)	(X)	(X)	385

Court, municipal, and icense clerks 5220 (SOC 43-4031)	Percent	100.0%	7.7%	4.0%	69.4%	14.1%	1.0%	2.6%	0.1%	0.1%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Court municipal and icense clerks 5220 (SOC 43-4031)	Male																
Court, municipal, and icense clerks 5220 (SOC 43-4031)	Number	19 580	1 425	840	13 430	2 635	180	880	30	0	50	40	0	(X)	(X)	(X)	75
Court, municipal, and icense clerks 5220 (SOC 43-4031)	Percent	20.6%	1.5%	0.9%	14.1%	2.8%	0.2%	0.9%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Court municipal and icense clerks 5220 (SOC 43-4031)	Female																
Court, municipal, and icense clerks 5220 (SOC 43-4031)	Number	75 600	5 910	2 935	52 655	10 745	785	1 590	105	55	275	110	115	(X)	(X)	(X)	315
Court municipal and icense clerks 5220 (SOC 43-4031)	Percent	79.4%	6.2%	3.1%	55.3%	11.3%	0.8%	1.7%	0.1%	0.1%	0.3%	0.1%	0.1%	(X)	(X)	(X)	0.3%
Credit authorizers checkers and clerks 5230 (SOC 43-	Total both sexes																
Credit authorizers checkers and clerks 5230 (SOC 43-	Number	58 065	4 950	2 320	38 670	8 325	260	2 410	180	125	255	205	35	(X)	(X)	(X)	330
Credit authorizers checkers and clerks 5230 (SOC 43-	Percent	100.0%	8.5%	4.0%	66.6%	14.3%	0.4%	4.2%	0.3%	0.2%	0.4%	0.4%	0.1%	(X)	(X)	(X)	0.6%
Credit authorizers checkers and clerks 5230 (SOC 43-	Male																
Credit authorizers checkers and clerks 5230 (SOC 43-	Number	14 930	1 265	495	9 880	1 815	65	1 040	120	30	55	85	0	(X)	(X)	(X)	75
Credit authorizers checkers and clerks 5230 (SOC 43-	Percent	25.7%	2.2%	0.9%	17.0%	3.1%	0.1%	1.8%	0.2%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Credit authorizers checkers and clerks 5230 (SOC 43-	Female																
Credit authorizers checkers and clerks 5230 (SOC 43-	Number	43 135	3 685	1 825	28 790	6 510	195	1 365	60	95	200	120	35	(X)	(X)	(X)	255
Credit authorizers checkers and clerks 5230 (SOC 43-	Percent	74.3%	6.3%	3.1%	49.6%	11.2%	0.3%	2.4%	0.1%	0.2%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Customer service representatives 5240 (SOC 43-4051)	Total both sexes																
Customer service representatives 5240 (SOC 43-4051)	Number	2 415 235	214 280	149 160	1 487 060	412 615	11 935	90 125	4 855	9 495	9 335	8 320	2 985	(X)	(X)	(X)	15 075
Customer service representatives 5240 (SOC 43-4051)	Percent	100.0%	8.9%	6.2%	61.6%	17.1%	0.5%	3.7%	0.2%	0.4%	0.4%	0.3%	0.1%	(X)	(X)	(X)	0.6%
Customer service representatives 5240 (SOC 43-4051)	Male																
Customer service representatives 5240 (SOC 43-4051)	Number	774 270	74 010	50 785	485 515	110 205	3 310	33 915	1 655	3 055	2 790	2 895	815	(X)	(X)	(X)	5 320
Customer service representatives 5240 (SOC 43-4051)	Percent	32.1%	3.1%	2.1%	20.1%	4.6%	0.1%	1.4%	0.1%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Customer service representatives 5240 (SOC 43-4051)	Female																
Customer service representatives 5240 (SOC 43-4051)	Number	1 640 965	140 270	98 375	1 001 545	302 405	8 625	56 210	3 200	6 440	6 545	5 425	2 170	(X)	(X)	(X)	9 755
Customer service representatives 5240 (SOC 43-4051)	Percent	67.9%	5.8%	4.1%	41.5%	12.5%	0.4%	2.3%	0.1%	0.3%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Eligib lity interviewers, government programs 5250 (SOC	Total, both sexes																
Eligib lity interviewers government programs 5250 (SOC	Number	70 355	7 965	6 080	35 910	15 040	805	3 455	75	100	365	215	70	(X)	(X)	(X)	275
Eligib lity interviewers government programs 5250 (SOC	Percent	100.0%	11.3%	8.6%	51.0%	21.4%	1.1%	4.9%	0.1%	0.1%	0.5%	0.3%	0.1%	(X)	(X)	(X)	0.4%
Eligib lity interviewers, government programs 5250 (SOC	Male																
Eligib lity interviewers government programs 5250 (SOC	Number	12 790	1 455	1 075	6 495	2 430	65	1 020	0	0	75	105	0	(X)	(X)	(X)	75
Eligib lity interviewers government programs 5250 (SOC	Percent	18.2%	2.1%	1.5%	9.2%	3.5%	0.1%	1.4%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Eligib lity interviewers government programs 5250 (SOC	Female																
Eligib lity interviewers government programs 5250 (SOC	Number	57 565	6 510	5 005	29 415	12 615	740	2 435	75	100	290	110	70	(X)	(X)	(X)	200
Eligib lity interviewers government programs 5250 (SOC	Percent	81.8%	9.3%	7.1%	41.8%	17.9%	1.1%	3.5%	0.1%	0.1%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.3%
File clerks 5260 (SOC 43-4071)	Total both sexes																
File clerks 5260 (SOC 43-4071)	Number	415 360	32 820	19 955	266 770	61 570	3 330	22 545	800	1 270	1 495	2 050	415	(X)	(X)	(X)	2 345
File clerks 5260 (SOC 43-4071)	Percent	100.0%	7.9%	4.8%	64.2%	14.8%	0.8%	5.4%	0.2%	0.3%	0.4%	0.5%	0.1%	(X)	(X)	(X)	0.6%
File clerks 5260 (SOC 43-4071)	Male																
File clerks 5260 (SOC 43-4071)	Number	92 150	8 045	5 185	54 385	14 725	470	7 085	305	305	275	500	95	(X)	(X)	(X)	775
File clerks 5260 (SOC 43-4071)	Percent	22.2%	1.9%	1.2%	13.1%	3.5%	0.1%	1.7%	0.1%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
File clerks 5260 (SOC 43-4071)	Female																
File clerks 5260 (SOC 43-4071)	Number	323 210	24 775	14 770	212 380	46 840	2 860	15 460	500	970	1 220	1 550	315	(X)	(X)	(X)	1 575
File clerks 5260 (SOC 43-4071)	Percent	77.8%	6.0%	3.6%	51.1%	11.3%	0.7%	3.7%	0.1%	0.2%	0.3%	0.4%	0.1%	(X)	(X)	(X)	0.4%
Hotel motel and resort desk clerks 5300 (SOC 43-4081)	Total both sexes																
Hotel motel and resort desk clerks 5300 (SOC 43-4081)	Number	150 670	12 685	9 615	89 965	21 860	1 620	10 270	780	950	1 020	500	185	(X)	(X)	(X)	1 215
Hotel motel and resort desk clerks 5300 (SOC 43-4081)	Percent	100.0%	8.4%	6.4%	59.7%	14.5%	1.1%	6.8%	0.5%	0.6%	0.7%	0.3%	0.1%	(X)	(X)	(X)	0.8%
Hotel motel and resort desk clerks 5300 (SOC 43-4081)	Male																
Hotel motel and resort desk clerks 5300 (SOC 43-4081)	Number	48 295	4 760	3 300	27 675	6 070	345	4 785	240	205	170	215	55	(X)	(X)	(X)	480
Hotel motel and resort desk clerks 5300 (SOC 43-4081)	Percent	32.1%	3.2%	2.2%	18.4%	4.0%	0.2%	3.2%	0.2%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Hotel motel and resort desk clerks 5300 (SOC 43-4081)	Female																
Hotel, motel, and resort desk clerks 5300 (SOC 43-4081)	Number	102,375	7,925	6,320	62,290	15,790	1,275	5,490	540	750	845	285	130	(X)	(X)	(X)	740
Hotel motel and resort desk clerks 5300 (SOC 43-4081)	Percent	67.9%	5.3%	4.2%	41.3%	10.5%	0.8%	3.6%	0.4%	0.5%	0.6%	0.2%	0.1%	(X)	(X)	(X)	0.5%
Interviewers except eligib lity and loan 5310 (SOC 43-	Total both sexes																
Interviewers, except eligib lity and loan 5310 (SOC 43-	Number	171,645	14,540	8,915	106,260	31,215	1,790	5,385	315	625	975	375	270	(X)	(X)	(X)	975
Interviewers except eligib lity and loan 5310 (SOC 43-	Percent	100.0%	8.5%	5.2%	61.9%	18.2%	1.0%	3.1%	0.2%	0.4%	0.6%	0.2%	0.2%	(X)	(X)	(X)	0.6%
Interviewers except eligib lity and loan 5310 (SOC 43-	Male																
Interviewers except eligib lity and loan 5310 (SOC 43-	Number	42 530	3 445	2 100	26 890	6 750	415	1 850	95	230	285	85	10	(X)	(X)	(X)	380
Interviewers except eligib lity and loan 5310 (SOC 43-	Percent	24.8%	2.0%	1.2%	15.7%	3.9%	0.2%	1.1%	0.1%	0.1%	0.2%	0.0%	0.0%	(X)	(X)	(X)	0.2%
Interviewers except eligib lity and loan 5310 (SOC 43-	Female																
Interviewers except eligib lity and loan 5310 (SOC 43-	Number	129 115	11 095	6 820	79 370	24 465	1 375	3 535	225	395	690	290	260	(X)	(X)	(X)	600
Interviewers except eligib lity and loan 5310 (SOC 43-	Percent	75.2%	6.5%	4.0%	46.2%	14.3%	0.8%	2.1%	0.1%	0.2%	0.4%	0.2%	0.2%	(X)	(X)	(X)	0.3%
Library assistants clerical 5320 (SOC 43-4121)	Total both sexes																
Library assistants clerical 5320 (SOC 43-4121)	Number	129 145	6 365	4 205	94 860	12 710	620	7 860	65	390	570	485	100	(X)	(X)	(X)	920
Library assistants clerical 5320 (SOC 43-4121)	Percent	100.0%	4.9%	3.3%	73.5%	9.8%	0.5%	6.1%	0.1%	0.3%	0.4%	0.4%	0.1%	(X)	(X)	(X)	0.7%
Library assistants clerical 5320 (SOC 43-4121)	Male																
Library assistants clerical 5320 (SOC 43-4121)	Number	24 130	1 685	900	15 515	2 930	75	2 290	15	125	155	180	0	(X)	(X)	(X)	255
Library assistants clerical 5320 (SOC 43-4121)	Percent	18.7%	1.3%	0.7%	12.0%	2.3%	0.1%	1.8%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Library assistants clerical 5320 (SOC 43-4121)	Female																
Library assistants clerical 5320 (SOC 43-4121)	Number	105 015	4 680	3 310	79 345	9 780	540	5 570	50	260	415	305	100	(X)	(X)	(X)	665
Library assistants clerical 5320 (SOC 43-4121)	Percent	81.3%	3.6%	2.6%	61.4%	7.6%	0.4%	4.3%	0.0%	0.2%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.5%
Loan interviewers and clerks 5330 (SOC 43-4131)	Total both sexes																
Loan interviewers and clerks 5330 (SOC 43-4131)	Number	154 570	13 500	7 830	103 250	18 670	690	7 715	385	405	605	465	30	(X)	(X)	(X)	1 035
Loan interviewers and clerks 5330 (SOC 43-4131)	Percent	100.0%	8.7%	5.1%	66.8%	12.1%	0.4%	5.0%	0.2%	0.3%	0.4%	0.3%	0.0%	(X)	(X)	(X)	0.7%
Loan interviewers and clerks 5330 (SOC 43-4131)	Male																
Loan interviewers and clerks 5330 (SOC 43-4131)	Number	30 055	2 905	1 810	18 390	3 945	165	2 270	30	80	50	135	0	(X)	(X)	(X)	280
Loan interviewers and clerks 5330 (SOC 43-4131)	Percent	19.4%	1.9%	1.2%	11.9%	2.6%	0.1%	1.5%	0.0%	0.1%	0.0%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Loan interviewers and clerks 5330 (SOC 43-4131)	Female																
Loan interviewers and clerks 5330 (SOC 43-4131)	Number	124 515	10 595	6 020	84 860	14 725	525	5 445	355	325	555	330	30	(X)	(X)	(X)	750
Loan interviewers and clerks 5330 (SOC 43-4131)	Percent	80.6%	6.9%	3.9%	54.9%	9.5%	0.3%	3.5%	0.2%	0.2%	0.4%	0.2%	0.0%	(X)	(X)	(X)	0.5%
New accounts clerks 5340 (SOC 43-4141)	Total both sexes																
New accounts clerks 5340 (SOC 43-4141)	Number	24 860	2 625	1 300	16 165	2 715	40	1 570	30	90	105	40	10	(X)	(X)	(X)	175
New accounts clerks 5340 (SOC 43-4141)	Percent	100.0%	10.6%	5.2%	65.0%	10.9%	0.2%	6.3%	0.1%	0.4%	0.4%	0.2%	0.0%	(X)	(X)	(X)	0.7%
New accounts clerks 5340 (SOC 43-4141)	Male																
New accounts clerks 5340 (SOC 43-4141)	Number	5 075	720	235	3 070	390	10	465	20	45	0	0	0	(X)	(X)	(X)	120
New accounts clerks 5340 (SOC 43-4141)	Percent	20.4%	2.9%	0.9%	12.3%	1.6%	0.0%	1.9%	0.1%	0.2%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.5%
New accounts clerks 5340 (SOC 43-4141)	Female																
New accounts clerks 5340 (SOC 43-4141)	Number	19 785	1 905	1 065	13 095	2 330	30	1 105	10	40	105	40	10	(X)	(X)	(X)	50
New accounts clerks 5340 (SOC 43-4141)	Percent	79.6%	7.7%	4.3%	52.7%	9.4%	0.1%	4.4%	0.0%	0.2%	0.4%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Correspondence clerks and order clerks 5350 (SOC 43-	Total both sexes																
Correspondence clerks and order clerks 5350 (SOC 43-	Number	164 135	15 385	11 465	106 700	20 340	895	6 860	270	320	600	450	115	(X)	(X)	(X)	735
Correspondence clerks and order clerks 5350 (SOC 43-	Percent	100.0%	9.4%	7.0%	65.0%	12.4%	0.5%	4.2%	0.2%	0.2%	0.4%	0.3%	0.1%	(X)	(X)	(X)	0.4%
Correspondence clerks and order clerks 5350 (SOC 43-	Male																
Correspondence clerks and order clerks 5350 (SOC 43-	Number	61 185	6 335	5 575	37 010	8 120	330	2 785	60	160	240	220	80	(X)	(X)	(X)	275
Correspondence clerks and order clerks 5350 (SOC 43-	Percent	37.3%	3.9%	3.4%	22.5%	4.9%	0.2%	1.7%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Correspondence clerks and order clerks 5350 (SOC 43-	Female																
Correspondence clerks and order clerks 5350 (SOC 43-	Number	102 945	9 050	5 890	69 690	12 215	565	4 075	210	160	360	230	40	(X)	(X)	(X)	455
Correspondence clerks and order clerks 5350 (SOC 43-	Percent	62.7%	5.5%	3.6%	42.5%	7.4%	0.3%	2.5%	0.1%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Human resources assistants except payroll and	Total both sexes																
Human resources assistants except payroll and	Number	55 440	4 565	3 185	34 145	9 925	595	2 055	45	230	150	230	105	(X)	(X)	(X)	210
Human resources assistants except payroll and	Percent	100.0%	8.2%	5.7%	61.6%	17.9%	1.1%	3.7%	0.1%	0.4%	0.3%	0.4%	0.2%	(X)	(X)	(X)	0.4%
Human resources assistants, except payroll and	Male																
Human resources assistants except payroll and	Number	9 545	830	375	5 640	1 940	160	405	0	30	60	55	10	(X)	(X)	(X)	40
Human resources assistants except payroll and	Percent	17.2%	1.5%	0.7%	10.2%	3.5%	0.3%	0.7%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Human resources assistants, except payroll and	Female																
Human resources assistants except payroll and	Number	45 895	3 740	2 810	28 505	7 985	435	1 650	45	200	90	175	95	(X)	(X)	(X)	170
Human resources assistants except payroll and	Percent	82.8%	6.7%	5.1%	51.4%	14.4%	0.8%	3.0%	0.1%	0.4%	0.2%	0.3%	0.2%	(X)	(X)	(X)	0.3%
Receptionists and information clerks 5400 (SOC 43-4171)	Total both sexes																
Receptionists and information clerks 5400 (SOC 43-4171)	Number	1 318 740	124 535	89 705	875 920	153 180	8 365	42 140	2 095	4 350	5 390	4 085	1 260	(X)	(X)	(X)	7 720
Receptionists and information clerks 5400 (SOC 43-4171)	Percent	100.0%	9.4%	6.8%	66.4%	11.6%	0.6%	3.2%	0.2%	0.3%	0.4%	0.3%	0.1%	(X)	(X)	(X)	0.6%
Receptionists and information clerks 5400 (SOC 43-4171)	Male																
Receptionists and information clerks 5400 (SOC 43-4171)	Number	122 115	11 115	8 945	74 680	17 205	745	6 570	195	705	375	570	155	(X)	(X)	(X)	855
Receptionists and information clerks 5400 (SOC 43-4171)	Percent	9.3%	0.8%	0.7%	5.7%	1.3%	0.1%	0.5%	0.0%	0.1%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Receptionists and information clerks 5400 (SOC 43-4171)	Female																
Receptionists and information clerks 5400 (SOC 43-4171)	Number	1 196 625	113 420	80 755	801 240	135 975	7 620	35 570	1 900	3 645	5 015	3 520	1 105	(X)	(X)	(X)	6 860
Receptionists and information clerks 5400 (SOC 43-4171)	Percent	90.7%	8.6%	6.1%	60.8%	10.3%	0.6%	2.7%	0.1%	0.3%	0.4%	0.3%	0.1%	(X)	(X)	(X)	0.5%
Reservation and transportation ticket agents and travel	Total both sexes																
Reservation and transportation ticket agents and travel	Number	151 640	13 670	8 160	90 625	24 505	825	8 830	1 655	370	520	570	165	(X)	(X)	(X)	1 750
Reservation and transportation ticket agents and travel	Percent	100.0%	9.0%	5.4%	59.8%	16.2%	0.5%	5.8%	1.1%	0.2%	0.3%	0.4%	0.1%	(X)	(X)	(X)	1.2%
Reservation and transportation ticket agents and travel	Male																
Reservation and transportation ticket agents and travel	Number	57 265	5 715	3 255	32 460	9 855	235	3 695	860	65	210	190	60	(X)	(X)	(X)	660
Reservation and transportation ticket agents and travel	Percent	37.8%	3.8%	2.1%	21.4%	6.5%	0.2%	2.4%	0.6%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.4%
Reservation and transportation ticket agents and travel	Female																
Reservation and transportation ticket agents and travel	Number	94 375	7 955	4 905	58 165	14 650	590	5 130	795	305	310	375	105	(X)	(X)	(X)	1 090
Reservation and transportation ticket agents and travel	Percent	62.2%	5.2%	3.2%	38.4%	9.7%	0.4%	3.4%	0.5%	0.2%	0.2%	0.2%	0.1%	(X)	(X)	(X)	0.7%
Information and record clerks all other 5420 (SOC 43-	Total both sexes																
Information and record clerks, all other 5420 (SOC 43-	Number	102,660	7,775	4,285	68,380	14,835	1,150	4,315	295	235	570	245	220	(X)	(X)	(X)	350
Information and record clerks all other 5420 (SOC 43-	Percent	100.0%	7.6%	4.2%	66.6%	14.5%	1.1%	4.2%	0.3%	0.2%	0.6%	0.2%	0.2%	(X)	(X)	(X)	0.3%
Information and record clerks all other 5420 (SOC 43-	Male																
Information and record clerks, all other 5420 (SOC 43-	Number	16,230	1,540	770	9,615	2,380	195	1,385	80	95	45	100	10	(X)	(X)	(X)	15
Information and record clerks all other 5420 (SOC 43-	Percent	15.8%	1.5%	0.8%	9.4%	2.3%	0.2%	1.3%	0.1%	0.1%	0.0%	0.1%	0.0%	(X)	(X)	(X)	0.0%
Information and record clerks all other 5420 (SOC 43-	Female																
Information and record clerks, all other 5420 (SOC 43-	Number	86 425	6 235	3 520	58 765	12 455	955	2 930	215	135	525	145	210	(X)	(X)	(X)	335
Information and record clerks all other 5420 (SOC 43-	Percent	84.2%	6.1%	3.4%	57.2%	12.1%	0.9%	2.9%	0.2%	0.1%	0.5%	0.1%	0.2%	(X)	(X)	(X)	0.3%
Cargo and freight agents 5500 (SOC 43-5011)	Total both sexes																
Cargo and freight agents 5500 (SOC 43-5011)	Number	20 465	2 545	1 175	11 975	2 520	55	1 705	225	70	35	25	0	(X)	(X)	(X)	135
Cargo and freight agents 5500 (SOC 43-5011)	Percent	100.0%	12.4%	5.7%	58.5%	12.3%	0.3%	8.3%	1.1%	0.3%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.7%
Cargo and freight agents 5500 (SOC 43-5011)	Male																
Cargo and freight agents 5500 (SOC 43-5011)	Number	13 885	1 780	875	7 665	1 830	50	1 325	205	55	20	15	0	(X)	(X)	(X)	65

Cargo and freight agents 5500 (SOC 43-5011)	Percent	67.8%	8.7%	4.3%	37.5%	8.9%	0.2%	6.5%	1.0%	0.3%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Cargo and freight agents 5500 (SOC 43-5011)	Female																
Cargo and freight agents 5500 (SOC 43-5011)	Number	6 580	770	300	4 310	695	4	380	20	15	10	10	0	(X)	(X)	(X)	70
Cargo and freight agents 5500 (SOC 43-5011)	Percent	32.2%	3.8%	1.5%	21.1%	3.4%	0.0%	1.9%	0.1%	0.1%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.3%
Couriers and messengers 5510 (SOC 43-5021)	Total, both sexes																
Couriers and messengers 5510 (SOC 43-5021)	Number	323 105	28 455	20 680	204 650	51 750	1 355	10 820	575	590	1 335	765	425	(X)	(X)	(X)	1 710
Couriers and messengers 5510 (SOC 43-5021)	Percent	100.0%	8.8%	6.4%	63.3%	16.0%	0.4%	3.3%	0.2%	0.2%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.5%
Couriers and messengers 5510 (SOC 43-5021)	Male																
Couriers and messengers 5510 (SOC 43-5021)	Number	267 500	23 895	17 720	167 315	44 115	915	9 310	340	520	950	700	325	(X)	(X)	(X)	1 400
Couriers and messengers 5510 (SOC 43-5021)	Percent	82.8%	7.4%	5.5%	51.8%	13.7%	0.3%	2.9%	0.1%	0.2%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Couriers and messengers 5510 (SOC 43-5021)	Female																
Couriers and messengers 5510 (SOC 43-5021)	Number	55 605	4 560	2 965	37 335	7 635	440	1 510	235	70	385	65	100	(X)	(X)	(X)	310
Couriers and messengers 5510 (SOC 43-5021)	Percent	17.2%	1.4%	0.9%	11.6%	2.4%	0.1%	0.5%	0.1%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Dispatchers 5520 (SOC 43-5030)	Total, both sexes																
Dispatchers 5520 (SOC 43-5030)	Number	290 115	20 555	14 550	207 900	35 575	2 205	4 335	460	630	1 565	695	265	(X)	(X)	(X)	1 380
Dispatchers 5520 (SOC 43-5030)	Percent	100.0%	7.1%	5.0%	71.7%	12.3%	0.8%	1.5%	0.2%	0.2%	0.5%	0.2%	0.1%	(X)	(X)	(X)	0.5%
Dispatchers 5520 (SOC 43-5030)	Male																
Dispatchers 5520 (SOC 43-5030)	Number	126 355	9 735	6 775	93 595	11 185	720	2 425	115	260	490	365	85	(X)	(X)	(X)	610
Dispatchers 5520 (SOC 43-5030)	Percent	43.6%	3.4%	2.3%	32.3%	3.9%	0.2%	0.8%	0.0%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Dispatchers 5520 (SOC 43-5030)	Female																
Dispatchers 5520 (SOC 43-5030)	Number	163 760	10 820	7 775	114 305	24 390	1 485	1 910	345	370	1 075	330	180	(X)	(X)	(X)	770
Dispatchers 5520 (SOC 43-5030)	Percent	56.4%	3.7%	2.7%	39.4%	8.4%	0.5%	0.7%	0.1%	0.1%	0.4%	0.1%	0.1%	(X)	(X)	(X)	0.3%
Meter readers, utilities 5530 (SOC 43-5041)	Total, both sexes																
Meter readers, utilities 5530 (SOC 43-5041)	Number	39 485	2 790	2 125	26 475	6 410	335	635	80	45	220	130	20	(X)	(X)	(X)	215
Meter readers, utilities 5530 (SOC 43-5041)	Percent	100.0%	7.1%	5.4%	67.1%	16.2%	0.8%	1.6%	0.2%	0.1%	0.6%	0.3%	0.1%	(X)	(X)	(X)	0.5%
Meter readers, utilities 5530 (SOC 43-5041)	Male																
Meter readers, utilities 5530 (SOC 43-5041)	Number	33 395	2 740	1 855	21 815	5 555	295	535	80	45	145	125	20	(X)	(X)	(X)	190
Meter readers, utilities 5530 (SOC 43-5041)	Percent	84.6%	6.9%	4.7%	55.2%	14.1%	0.7%	1.4%	0.2%	0.1%	0.4%	0.3%	0.1%	(X)	(X)	(X)	0.5%
Meter readers, utilities 5530 (SOC 43-5041)	Female																
Meter readers, utilities 5530 (SOC 43-5041)	Number	6 090	50	265	4 660	855	40	105	4	0	75	4	0	(X)	(X)	(X)	25
Meter readers, utilities 5530 (SOC 43-5041)	Percent	15.4%	0.1%	0.7%	11.8%	2.2%	0.1%	0.3%	0.0%	0.0%	0.2%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Postal service clerks 5540 (SOC 43-5051)	Total, both sexes																
Postal service clerks 5540 (SOC 43-5051)	Number	150 885	6 935	5 590	77 810	40 955	855	16 500	265	100	570	345	215	(X)	(X)	(X)	750
Postal service clerks 5540 (SOC 43-5051)	Percent	100.0%	4.6%	3.7%	51.6%	27.1%	0.6%	10.9%	0.2%	0.1%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.5%
Postal service clerks 5540 (SOC 43-5051)	Male																
Postal service clerks 5540 (SOC 43-5051)	Number	74 540	3 825	3 140	40 275	17 570	380	8 305	155	70	270	180	100	(X)	(X)	(X)	265
Postal service clerks 5540 (SOC 43-5051)	Percent	49.4%	2.5%	2.1%	26.7%	11.6%	0.3%	5.5%	0.1%	0.0%	0.2%	0.1%	0.1%	(X)	(X)	(X)	0.2%
Postal service clerks 5540 (SOC 43-5051)	Female																
Postal service clerks 5540 (SOC 43-5051)	Number	76 345	3 110	2 450	37 530	23 385	475	8 195	110	30	300	165	115	(X)	(X)	(X)	480
Postal service clerks 5540 (SOC 43-5051)	Percent	50.6%	2.1%	1.6%	24.9%	15.5%	0.3%	5.4%	0.1%	0.0%	0.2%	0.1%	0.1%	(X)	(X)	(X)	0.3%
Postal service mail carriers 5550 (SOC 43-5052)	Total, both sexes																
Postal service mail carriers 5550 (SOC 43-5052)	Number	341 080	18 970	12 650	232 995	48 910	1 250	21 475	695	575	1 220	615	255	(X)	(X)	(X)	1 465
Postal service mail carriers 5550 (SOC 43-5052)	Percent	100.0%	5.6%	3.7%	68.3%	14.3%	0.4%	6.3%	0.2%	0.2%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Postal service mail carriers 5550 (SOC 43-5052)	Male																
Postal service mail carriers 5550 (SOC 43-5052)	Number	212 935	12 960	8 200	141 425	28 910	620	18 030	340	390	720	410	115	(X)	(X)	(X)	815
Postal service mail carriers 5550 (SOC 43-5052)	Percent	62.4%	3.8%	2.4%	41.5%	8.5%	0.2%	5.3%	0.1%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Postal service mail carriers 5550 (SOC 43-5052)	Female																
Postal service mail carriers 5550 (SOC 43-5052)	Number	128 145	6 015	4 450	91 575	20 000	625	3 445	355	185	500	205	135	(X)	(X)	(X)	650
Postal service mail carriers 5550 (SOC 43-5052)	Percent	37.6%	1.8%	1.3%	26.8%	5.9%	0.2%	1.0%	0.1%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Postal service mail sorters, processors, and processing	Total, both sexes																
Postal service mail sorters, processors, and processing	Number	97,050	5,445	3,730	45,850	29,115	345	11,180	210	220	210	205	55	(X)	(X)	(X)	480
Postal service mail sorters, processors, and processing	Percent	100.0%	5.6%	3.8%	47.2%	30.0%	0.4%	11.5%	0.2%	0.2%	0.2%	0.2%	0.1%	(X)	(X)	(X)	0.5%
Postal service mail sorters, processors, and processing	Male																
Postal service mail sorters, processors, and processing	Number	49,265	2,780	1,990	25,460	12,375	175	5,740	75	130	130	155	0	(X)	(X)	(X)	255
Postal service mail sorters, processors, and processing	Percent	50.8%	2.9%	2.1%	26.2%	12.8%	0.2%	5.9%	0.1%	0.1%	0.1%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Postal service mail sorters, processors, and processing	Female																
Postal service mail sorters, processors, and processing	Number	47 780	2 665	1 735	20 395	16 740	170	5 440	135	90	80	50	55	(X)	(X)	(X)	225
Postal service mail sorters, processors, and processing	Percent	49.2%	2.7%	1.8%	21.0%	17.2%	0.2%	5.6%	0.1%	0.1%	0.1%	0.1%	0.1%	(X)	(X)	(X)	0.2%
Production, planning, and expediting clerks 5600 (SOC 43-	Total, both sexes																
Production, planning, and expediting clerks 5600 (SOC 43-	Number	297 550	17 160	11 585	224 985	25 895	1 215	11 240	480	810	1 255	1 305	65	(X)	(X)	(X)	1 550
Production, planning, and expediting clerks 5600 (SOC 43-	Percent	100.0%	5.8%	3.9%	75.6%	8.7%	0.4%	3.8%	0.2%	0.3%	0.4%	0.4%	0.0%	(X)	(X)	(X)	0.5%
Production, planning, and expediting clerks 5600 (SOC 43-	Male																
Production, planning, and expediting clerks 5600 (SOC 43-	Number	129 690	6 530	4 565	100 805	9 780	530	5 065	190	370	525	465	65	(X)	(X)	(X)	795
Production, planning, and expediting clerks 5600 (SOC 43-	Percent	43.6%	2.2%	1.5%	33.9%	3.3%	0.2%	1.7%	0.1%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Production, planning, and expediting clerks 5600 (SOC 43-	Female																
Production, planning, and expediting clerks 5600 (SOC 43-	Number	167 860	10 630	7 020	124 185	16 120	680	6 170	295	440	730	840	0	(X)	(X)	(X)	750
Production, planning, and expediting clerks 5600 (SOC 43-	Percent	56.4%	3.6%	2.4%	41.7%	5.4%	0.2%	2.1%	0.1%	0.1%	0.2%	0.3%	0.0%	(X)	(X)	(X)	0.3%
Shipping, receiving, and traffic clerks 5610 (SOC 43-5071)	Total, both sexes																
Shipping, receiving, and traffic clerks 5610 (SOC 43-5071)	Number	631 960	74 410	64 305	365 705	93 595	2 195	21 415	1 710	1 315	2 155	1 395	280	(X)	(X)	(X)	3 485
Shipping, receiving, and traffic clerks 5610 (SOC 43-5071)	Percent	100.0%	11.8%	10.2%	57.9%	14.8%	0.3%	3.4%	0.3%	0.2%	0.3%	0.2%	0.0%	(X)	(X)	(X)	0.6%
Shipping, receiving, and traffic clerks 5610 (SOC 43-5071)	Male																
Shipping, receiving, and traffic clerks 5610 (SOC 43-5071)	Number	439 185	55 870	48 280	243 395	66 775	1 290	15 990	1 265	980	1 460	1 050	205	(X)	(X)	(X)	2 620
Shipping, receiving, and traffic clerks 5610 (SOC 43-5071)	Percent	69.5%	8.8%	7.6%	38.5%	10.6%	0.2%	2.5%	0.2%	0.2%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.4%
Shipping, receiving, and traffic clerks 5610 (SOC 43-5071)	Female																
Shipping, receiving, and traffic clerks 5610 (SOC 43-5071)	Number	192 775	18 535	16 025	122 310	26 820	900	5 425	445	335	695	345	75	(X)	(X)	(X)	860
Shipping, receiving, and traffic clerks 5610 (SOC 43-5071)	Percent	30.5%	2.9%	2.5%	19.4%	4.2%	0.1%	0.9%	0.1%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Stock clerks and order fillers 5620 (SOC 43-5081)	Total, both sexes																
Stock clerks and order fillers 5620 (SOC 43-5081)	Number	1 690 045	167 465	131 850	994 180	286 170	12 410	62 005	4 665	6 105	7 045	5 195	1 775	(X)	(X)	(X)	11 175
Stock clerks and order fillers 5620 (SOC 43-5081)	Percent	100.0%	9.9%	7.8%	58.8%	16.9%	0.7%	3.7%	0.3%	0.4%	0.4%	0.3%	0.1%	(X)	(X)	(X)	0.7%
Stock clerks and order fillers 5620 (SOC 43-5081)	Male																
Stock clerks and order fillers 5620 (SOC 43-5081)	Number	1 075 835	106 260	83 150	622 520	193 740	7 670	39 135	2 820	4 375	4 200	3 545	1 095	(X)	(X)	(X)	7 325
Stock clerks and order fillers 5620 (SOC 43-5081)	Percent	63.7%	6.3%	4.9%	36.8%	11.5%	0.5%	2.3%	0.2%	0.3%	0.2%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Stock clerks and order fillers 5620 (SOC 43-5081)	Female																
Stock clerks and order fillers 5620 (SOC 43-5081)	Number	614 210	61 205	48 700	371 660	92 435	4 740	22 870	1 845	1 735	2 845	1 655	680	(X)	(X)	(X)	3 850
Stock clerks and order fillers 5620 (SOC 43-5081)	Percent	36.3%	3.6%	2.9%	22.0%	5.5%	0.3%	1.4%	0.1%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Weighers, measurers, checkers and samplers	Total, both sexes																
Weighers, measurers, checkers and samplers	Number	80 515	9 025	6 565	50 045	9 960	485	3 175	85	170	410	220	35	(X)	(X)	(X)	340
Weighers, measurers, checkers and samplers	Percent	100.0%	11.2%	8.2%	62.2%	12.4%	0.6%	3.9%	0.1%	0.2%	0.5%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Weighers, measurers, checkers and samplers	Male																
Weighers, measurers, checkers and samplers	Number	41 280	4 700	3 310	26 075	4 890	175	1 565	0	85	170	170	0	(X)	(X)	(X)	145
Weighers, measurers, checkers and samplers	Percent	51.3%	5.8%	4.1%	32.4%	6.1%	0.2%	1.9%	0.0%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Weighers, measurers, checkers and samplers	Female																
Weighers, measurers, checkers and samplers	Number	39 235	4 325	3 260	23 970	5 070	310	1 610	85	85	235	55	35	(X)	(X)	(X)	195
Weighers, measurers, checkers and samplers	Percent	48.7%	5.4%	4.0%	29.8%	6.3%	0.4%	2.0%	0.1%	0.1%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Secretaries and administrative assistants 5700 (SOC 43-	Total, both sexes																
Secretaries and administrative assistants 5700 (SOC 43-	Number	3 991 485	249 315	150 300	3 049 700	360 895	22 915	101 205	5 000	6 705	14 315	10 460	2 710	(X)	(X)	(X)	17 970
Secretaries and administrative assistants 5700 (SOC 43-	Percent	100.0%	6.2%	3.8%	76.4%	9.0%	0.6%	2.5%	0.1%	0.2%	0.4%	0.3%	0.1%	(X)	(X)	(X)	0.5%
Secretaries and administrative assistants 5700 (SOC 43-	Male																
Secretaries and administrative assistants 5700 (SOC 43-	Number	163 195	12 275	7 510	110 490	19 445	1 105	9 335	90	660	490	575	195	(X)	(X)	(X)	1 025
Secretaries and administrative assistants 5700 (SOC 43-	Percent	4.1%	0.3%	0.2%	2.8%	0.5%	0.0%	0.2%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Secretaries and administrative assistants 5700 (SOC 43-	Female																
Secretaries and administrative assistants 5700 (SOC 43-	Number	3 828 290	237 040	142 790	2 939 210	341 455	21 815	91 870	4 905	6 045	13 825	9 885	2 515	(X)	(X)	(X)	16 945
Secretaries and administrative assistants 5700 (SOC 43-	Percent	95.9%	5.9%	3.6%	73.6%	8.6%	0.5%	2.3%	0.1%	0.2%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Computer operators 5800 (SOC 43-9011)	Total, both sexes																
Computer operators 5800 (SOC 43-9011)	Number	151 215	9 715	6 530	102 845	20 440	975	8 800	170	70	430	370	210	(X)	(X)	(X)	660
Computer operators 5800 (SOC 43-9011)	Percent	100.0%	6.4%	4.3%	68.0%	13.5%	0.6%	5.8%	0.1%	0.0%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Computer operators 5800 (SOC 43-9011)	Male																
Computer operators 5800 (SOC 43-9011)	Number	76 705	5 355	3 510	52 665	8 290	405	5 675	40	70	145	175	80	(X)	(X)	(X)	295
Computer operators 5800 (SOC 43-9011)	Percent	50.7%	3.5%	2.3%	34.8%	5.5%	0.3%	3.8%	0.0%	0.0%	0.1%	0.1%	0.1%	(X)	(X)	(X)	0.2%
Computer operators 5800 (SOC 43-9011)	Female																
Computer operators 5800 (SOC 43-9011)	Number	74 510	4 360	3 020	50 180	12 150	570	3 125	130	0	285	190	135	(X)	(X)	(X)	365
Computer operators 5800 (SOC 43-9011)	Percent	49.3%	2.9%	2.0%	33.2%	8.0%	0.4%	2.1%	0.1%	0.0%	0.2%	0.1%	0.1%	(X)	(X)	(X)	0.2%
Data entry keyers 5810 (SOC 43-9021)	Total, both sexes																
Data entry keyers 5810 (SOC 43-9021)	Number	493 815	36 860	27 980	313 030	76 765	2 765	27 180	1 080	1 170	1 965	1 865	460	(X)	(X)	(X)	2 700
Data entry keyers 5810 (SOC 43-9021)	Percent	100.0%	7.5%	5.7%	63.4%	15.5%	0.6%	5.5%	0.2%	0.2%	0.4%	0.4%	0.1%	(X)	(X)	(X)	0.5%
Data entry keyers 5810 (SOC 43-9021)	Male																
Data entry keyers 5810 (SOC 43-9021)	Number	102 610	8 235	6 490	63 150	13 335	580	8 715	155	340	360	575	25	(X)	(X)	(X)	650
Data entry keyers 5810 (SOC 43-9021)	Percent	20.8%	1.7%	1.3%	12.8%	2.7%	0.1%	1.8%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Data entry keyers 5810 (SOC 43-9021)	Female																
Data entry keyers 5810 (SOC 43-9021)	Number	391 205	28 625	21 490	249 880	63 430	2 185	18 465	925	830	1 610	1 295	430	(X)	(X)	(X)	2 050
Data entry keyers 5810 (SOC 43-9021)	Percent	79.2%	5.8%	4.4%	50.6%	12.8%	0.4%	3.7%	0.2%	0.2%	0.3%	0.3%	0.1%	(X)	(X)	(X)	0.4%
Word processors and typists 5820 (SOC 43-9022)	Total, both sexes																
Word processors and typists 5820 (SOC 43-9022)	Number	352 460	23 755	15 655	237 665	50 645	1 345	17 725	575	885	980	1 060	185	(X)	(X)	(X)	1 980
Word processors and typists 5820 (SOC 43-9022)	Percent	100.0%	6.7%	4.4%	67.4%	14.4%	0.4%	5.0%	0.2%	0.3%	0.3%	0.3%	0.1%	(X)	(X)	(X)	0.6%
Word processors and typists 5820 (SOC 43-9022)	Male																
Word processors and typists 5820 (SOC 43-9022)	Number	39,835	3,500	2,320	23,440	5,550	170	3,970	125	160	95	240	0	(X)	(X)	(X)	270
Word processors and typists 5820 (SOC 43-9022)	Percent	11.3%	1.0%	0.7%	6.7%	1.6%	0.0%	1.1%	0.0%	0.0%	0.0%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Word processors and typists 5820 (SOC 43-9022)	Female																
Word processors and typists 5820 (SOC 43-9022)	Number	312,620	20,255	13,335	214,225	45,095	1,175	13,755	450	725	885	820	185	(X)	(X)	(X)	1,710
Word processors and typists 5820 (SOC 43-9022)	Percent	88.7%	5.7%	3.8%	60.8%	12.8%	0.3%	3.9%	0.1%	0.2%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.5%
Insurance claims and policy processing clerks 5840 (SOC	Total, both sexes																
Insurance claims and policy processing clerks 5840 (SOC	Number	325 030	22 405	14 410	221 365	52 280	970	8 460	455	815	1 225	675	465	(X)	(X)	(X)	1 510
Insurance claims and policy processing clerks 5840 (SOC	Percent	100.0%	6.9%	4.4%	68.1%	16.1%	0.3%	2.6%	0.1%	0.3%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.5%
Insurance claims and policy processing clerks 5840 (SOC	Male																
Insurance claims and policy processing clerks 5840 (SOC	Number	52 505	3 955	2 630	34 775	7 970	80	2 085	25	100	300	160	85	(X)	(X)	(X)	340
Insurance claims and policy processing clerks 5840 (SOC	Percent	16.2%	1.2%	0.8%	10.7%	2.5%	0.0%	0.6%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Insurance claims and policy processing clerks 5840 (SOC	Female																
Insurance claims and policy processing clerks 5840 (SOC	Number	272 530	18 450	11 780	186 585	44 315	890	6 380	425	710	925	515	380	(X)	(X)	(X)	1 170

Insurance claims and policy processing clerks 5840 (SOC	Percent	83.8%	5.7%	3.6%	57.4%	13.6%	0.3%	2.0%	0.1%	0.2%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Mail clerks and mail machine operators except postal	Total, both sexes																
Mail clerks and mail machine operators except postal	Number	131 890	9 420	9 165	71 845	30 860	870	7 575	260	350	400	395	90	(X)	(X)	(X)	650
Mail clerks and mail machine operators, except postal	Percent	100.0%	7.1%	6.9%	54.5%	23.4%	0.7%	5.7%	0.2%	0.3%	0.3%	0.3%	0.1%	(X)	(X)	(X)	0.5%
Mail clerks and mail machine operators except postal	Male																
Mail clerks and mail machine operators except postal	Number	64 355	4 700	4 500	32 935	16 410	235	4 250	65	280	170	355	35	(X)	(X)	(X)	410
Mail clerks and mail machine operators except postal	Percent	48.8%	3.6%	3.4%	25.0%	12.4%	0.2%	3.2%	0.0%	0.2%	0.1%	0.3%	0.0%	(X)	(X)	(X)	0.3%
Mail clerks and mail machine operators except postal	Female																
Mail clerks and mail machine operators except postal	Number	67 535	4 720	4 665	38 910	14 450	635	3 325	195	70	230	40	55	(X)	(X)	(X)	240
Mail clerks and mail machine operators except postal	Percent	51.2%	3.6%	3.5%	29.5%	11.0%	0.5%	2.5%	0.1%	0.1%	0.2%	0.0%	0.0%	(X)	(X)	(X)	0.2%
Office clerks general 5860 (SOC 43-9061)	Total both sexes																
Office clerks general 5860 (SOC 43-9061)	Number	1 282 130	108 865	72 675	827 975	172 955	7 680	67 605	3 190	3 225	4 130	4 070	1 465	(X)	(X)	(X)	8 295
Office clerks general 5860 (SOC 43-9061)	Percent	100.0%	8.5%	5.7%	64.6%	13.5%	0.6%	5.3%	0.2%	0.3%	0.3%	0.3%	0.1%	(X)	(X)	(X)	0.6%
Office clerks general 5860 (SOC 43-9061)	Male																
Office clerks general 5860 (SOC 43-9061)	Number	230 885	22 130	15 190	136 760	30 550	1 195	19 750	325	855	915	1 015	275	(X)	(X)	(X)	1 920
Office clerks general 5860 (SOC 43-9061)	Percent	18.0%	1.7%	1.2%	10.7%	2.4%	0.1%	1.5%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Office clerks general 5860 (SOC 43-9061)	Female																
Office clerks general 5860 (SOC 43-9061)	Number	1 051 245	86 735	57 485	691 215	142 405	6 485	47 850	2 865	2 370	3 215	3 055	1 190	(X)	(X)	(X)	6 375
Office clerks general 5860 (SOC 43-9061)	Percent	82.0%	6.8%	4.5%	53.9%	11.1%	0.5%	3.7%	0.2%	0.2%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.5%
Office machine operators except computer 5900 (SOC 43-	Total both sexes																
Office machine operators except computer 5900 (SOC 43-	Number	55 825	4 315	3 470	31 420	9 890	335	4 865	65	295	265	220	140	(X)	(X)	(X)	540
Office machine operators except computer 5900 (SOC 43-	Percent	100.0%	7.7%	6.2%	56.3%	17.7%	0.6%	8.7%	0.1%	0.5%	0.5%	0.4%	0.3%	(X)	(X)	(X)	1.0%
Office machine operators except computer 5900 (SOC 43-	Male																
Office machine operators except computer 5900 (SOC 43-	Number	23 125	2 030	1 710	12 110	4 115	80	2 440	20	105	115	40	65	(X)	(X)	(X)	290
Office machine operators except computer 5900 (SOC 43-	Percent	41.4%	3.6%	3.1%	21.7%	7.4%	0.1%	4.4%	0.0%	0.2%	0.2%	0.1%	0.1%	(X)	(X)	(X)	0.5%
Office machine operators, except computer 5900 (SOC 43-	Female																
Office machine operators except computer 5900 (SOC 43-	Number	32 700	2 285	1 760	19 315	5 775	255	2 425	40	195	150	180	70	(X)	(X)	(X)	250
Office machine operators except computer 5900 (SOC 43-	Percent	58.6%	4.1%	3.2%	34.6%	10.3%	0.5%	4.3%	0.1%	0.3%	0.3%	0.3%	0.1%	(X)	(X)	(X)	0.4%
Proofreaders and copy markers 5910 (SOC 43-9081)	Total, both sexes																
Proofreaders and copy markers 5910 (SOC 43-9081)	Number	16 395	515	300	13 455	1 215	35	550	25	30	55	65	10	(X)	(X)	(X)	135
Proofreaders and copy markers 5910 (SOC 43-9081)	Percent	100.0%	3.1%	1.8%	82.1%	7.4%	0.2%	3.4%	0.2%	0.2%	0.3%	0.4%	0.1%	(X)	(X)	(X)	0.8%
Proofreaders and copy markers 5910 (SOC 43-9081)	Male																
Proofreaders and copy markers 5910 (SOC 43-9081)	Number	4 655	200	130	3 620	415	0	165	25	0	15	30	10	(X)	(X)	(X)	40
Proofreaders and copy markers 5910 (SOC 43-9081)	Percent	28.4%	1.2%	0.8%	22.1%	2.5%	0.0%	1.0%	0.2%	0.0%	0.1%	0.2%	0.1%	(X)	(X)	(X)	0.2%
Proofreaders and copy markers 5910 (SOC 43-9081)	Female																
Proofreaders and copy markers 5910 (SOC 43-9081)	Number	11 740	310	170	9 835	800	35	385	0	30	40	35	0	(X)	(X)	(X)	100
Proofreaders and copy markers 5910 (SOC 43-9081)	Percent	71.6%	1.9%	1.0%	60.0%	4.9%	0.2%	2.3%	0.0%	0.2%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.6%
Statistical assistants 5920 (SOC 43-9111)	Total both sexes																
Statistical assistants 5920 (SOC 43-9111)	Number	27 600	1 475	855	19 450	3 315	215	1 650	25	105	120	145	55	(X)	(X)	(X)	200
Statistical assistants 5920 (SOC 43-9111)	Percent	100.0%	5.3%	3.1%	70.5%	12.0%	0.8%	6.0%	0.1%	0.4%	0.4%	0.5%	0.2%	(X)	(X)	(X)	0.7%
Statistical assistants 5920 (SOC 43-9111)	Male																
Statistical assistants 5920 (SOC 43-9111)	Number	10 165	475	155	7 410	1 035	75	755	0	0	50	80	4	(X)	(X)	(X)	125
Statistical assistants 5920 (SOC 43-9111)	Percent	36.8%	1.7%	0.6%	26.8%	3.8%	0.3%	2.7%	0.0%	0.0%	0.2%	0.3%	0.0%	(X)	(X)	(X)	0.5%
Statistical assistants 5920 (SOC 43-9111)	Female																
Statistical assistants 5920 (SOC 43-9111)	Number	17 435	1 000	700	12 040	2 275	135	895	25	105	70	65	50	(X)	(X)	(X)	70
Statistical assistants 5920 (SOC 43-9111)	Percent	63.2%	3.6%	2.5%	43.6%	8.2%	0.5%	3.2%	0.1%	0.4%	0.3%	0.2%	0.2%	(X)	(X)	(X)	0.3%
Miscellaneous office and administrative support workers	Total both sexes																
Miscellaneous office and administrative support workers	Number	552 105	37 605	25 050	376 090	76 765	3 880	22 205	1 260	1 565	2 560	2 015	710	(X)	(X)	(X)	2 395
Miscellaneous office and administrative support workers	Percent	100.0%	6.8%	4.5%	68.1%	13.9%	0.7%	4.0%	0.2%	0.3%	0.5%	0.4%	0.1%	(X)	(X)	(X)	0.4%
Miscellaneous office and administrative support workers	Male																
Miscellaneous office and administrative support workers,	Number	138,085	10,925	6,525	91,360	17,575	1,025	7,600	410	550	675	545	80	(X)	(X)	(X)	815
Miscellaneous office and administrative support workers	Percent	25.0%	2.0%	1.2%	16.5%	3.2%	0.2%	1.4%	0.1%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Miscellaneous office and administrative support workers	Female																
Miscellaneous office and administrative support workers,	Number	414,015	26,680	18,530	284,735	59,190	2,855	14,605	850	1,015	1,885	1,475	625	(X)	(X)	(X)	1,580
Miscellaneous office and administrative support workers	Percent	75.0%	4.8%	3.4%	51.6%	10.7%	0.5%	2.6%	0.2%	0.2%	0.3%	0.3%	0.1%	(X)	(X)	(X)	0.3%
First-line supervisors of farming fishing and forestry	Total both sexes																
First-line supervisors of farming fishing and forestry	Number	61 480	12 445	9 065	35 745	2 175	560	825	15	70	335	20	15	(X)	(X)	(X)	205
First-line supervisors of farming fishing and forestry	Percent	100.0%	20.2%	14.7%	58.1%	3.5%	0.9%	1.3%	0.0%	0.1%	0.5%	0.0%	0.0%	(X)	(X)	(X)	0.3%
First-line supervisors of farming fishing and forestry	Male																
First-line supervisors of farming fishing and forestry	Number	52 345	11 035	7 790	29 975	1 900	500	575	15	50	285	20	15	(X)	(X)	(X)	195
First-line supervisors of farming fishing and forestry	Percent	85.1%	17.9%	12.7%	48.8%	3.1%	0.8%	0.9%	0.0%	0.1%	0.5%	0.0%	0.0%	(X)	(X)	(X)	0.3%
First-line supervisors of farming fishing and forestry	Female																
First-line supervisors of farming fishing and forestry	Number	9 130	1 415	1 280	5 770	275	60	250	0	25	50	0	0	(X)	(X)	(X)	10
First-line supervisors of farming fishing and forestry	Percent	14.9%	2.3%	2.1%	9.4%	0.4%	0.1%	0.4%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Agricultural inspectors 6010 (SOC 45-2011)	Total both sexes																
Agricultural inspectors 6010 (SOC 45-2011)	Number	17 815	1 640	1 120	11 105	2 700	230	740	55	15	80	40	0	(X)	(X)	(X)	90
Agricultural inspectors 6010 (SOC 45-2011)	Percent	100.0%	9.2%	6.3%	62.3%	15.2%	1.3%	4.2%	0.3%	0.1%	0.4%	0.2%	0.0%	(X)	(X)	(X)	0.5%
Agricultural inspectors 6010 (SOC 45-2011)	Male																
Agricultural inspectors 6010 (SOC 45-2011)	Number	10 250	945	440	6 995	1 200	85	430	45	0	35	30	0	(X)	(X)	(X)	45
Agricultural inspectors 6010 (SOC 45-2011)	Percent	57.5%	5.3%	2.5%	39.3%	6.7%	0.5%	2.4%	0.3%	0.0%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Agricultural inspectors 6010 (SOC 45-2011)	Female																
Agricultural inspectors 6010 (SOC 45-2011)	Number	7 560	695	680	4 110	1 500	145	310	10	15	45	10	0	(X)	(X)	(X)	45
Agricultural inspectors 6010 (SOC 45-2011)	Percent	42.4%	3.9%	3.8%	23.1%	8.4%	0.8%	1.7%	0.1%	0.1%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Graders and sorters agricultural products 6040 (SOC 45-	Total both sexes																
Graders and sorters agricultural products 6040 (SOC 45-	Number	56 665	21 750	14 885	11 655	5 345	380	2 140	125	0	130	50	15	(X)	(X)	(X)	190
Graders and sorters, agricultural products 6040 (SOC 45-	Percent	100.0%	38.4%	26.3%	20.6%	9.4%	0.7%	3.8%	0.2%	0.0%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Graders and sorters agricultural products 6040 (SOC 45-	Male																
Graders and sorters agricultural products 6040 (SOC 45-	Number	18 070	5 685	4 175	5 680	1 670	210	430	50	0	75	40	10	(X)	(X)	(X)	45
Graders and sorters, agricultural products 6040 (SOC 45-	Percent	31.9%	10.0%	7.4%	10.0%	2.9%	0.4%	0.8%	0.1%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Graders and sorters, agricultural products 6040 (SOC 45-	Female																
Graders and sorters agricultural products 6040 (SOC 45-	Number	38 595	16 065	10 710	5 975	3 675	175	1 710	75	0	55	10	4	(X)	(X)	(X)	145
Graders and sorters agricultural products 6040 (SOC 45-	Percent	68.1%	28.4%	18.9%	10.5%	6.5%	0.3%	3.0%	0.1%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.3%
Miscellaneous agricultural workers including animal	Total both sexes																
Miscellaneous agricultural workers including animal	Number	871 090	294 720	188 575	333 180	32 830	4 370	9 265	1 055	570	3 015	375	145	(X)	(X)	(X)	2 995
Miscellaneous agricultural workers including animal	Percent	100.0%	33.8%	21.6%	38.2%	3.8%	0.5%	1.1%	0.1%	0.1%	0.3%	0.0%	0.0%	(X)	(X)	(X)	0.3%
Miscellaneous agricultural workers including animal	Male																
Miscellaneous agricultural workers including animal	Number	682 060	228 085	149 145	261 895	27 565	3 570	5 365	785	365	2 405	275	100	(X)	(X)	(X)	2 510
Miscellaneous agricultural workers including animal	Percent	78.3%	26.2%	17.1%	30.1%	3.2%	0.4%	0.6%	0.1%	0.0%	0.3%	0.0%	0.0%	(X)	(X)	(X)	0.3%
Miscellaneous agricultural workers including animal	Female																
Miscellaneous agricultural workers including animal	Number	189 030	66 635	39 430	71 290	5 265	800	3 900	270	205	610	100	45	(X)	(X)	(X)	485
Miscellaneous agricultural workers including animal	Percent	21.7%	7.6%	4.5%	8.2%	0.6%	0.1%	0.4%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Fishing and hunting workers 6100 (SOC 45-3000)	Total both sexes																
Fishing and hunting workers 6100 (SOC 45-3000)	Number	42 200	2 320	910	32 705	1 085	1 610	2 530	145	55	570	60	4	(X)	(X)	(X)	205
Fishing and hunting workers 6100 (SOC 45-3000)	Percent	100.0%	5.5%	2.2%	77.5%	2.6%	3.8%	6.0%	0.3%	0.1%	1.4%	0.1%	0.0%	(X)	(X)	(X)	0.5%
Fishing and hunting workers 6100 (SOC 45-3000)	Male																
Fishing and hunting workers 6100 (SOC 45-3000)	Number	40 070	2 235	845	30 970	1 085	1 525	2 405	145	55	545	60	4	(X)	(X)	(X)	205
Fishing and hunting workers 6100 (SOC 45-3000)	Percent	95.0%	5.3%	2.0%	73.4%	2.6%	3.6%	5.7%	0.3%	0.1%	1.3%	0.1%	0.0%	(X)	(X)	(X)	0.5%
Fishing and hunting workers 6100 (SOC 45-3000)	Female																
Fishing and hunting workers 6100 (SOC 45-3000)	Number	2 130	85	65	1 740	0	85	130	0	0	25	0	0	(X)	(X)	(X)	0
Fishing and hunting workers 6100 (SOC 45-3000)	Percent	5.0%	0.2%	0.2%	4.1%	0.0%	0.2%	0.3%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Forest and conservation workers 6120 (SOC 45-4011)	Total, both sexes																
Forest and conservation workers 6120 (SOC 45-4011)	Number	16 935	1 700	1 775	11 695	1 095	310	125	20	50	105	30	4	(X)	(X)	(X)	30
Forest and conservation workers 6120 (SOC 45-4011)	Percent	100.0%	10.0%	10.5%	69.1%	6.5%	1.8%	0.7%	0.1%	0.3%	0.6%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Forest and conservation workers 6120 (SOC 45-4011)	Male																
Forest and conservation workers 6120 (SOC 45-4011)	Number	14 110	1 595	1 620	9 460	935	225	110	15	20	85	30	4	(X)	(X)	(X)	4
Forest and conservation workers 6120 (SOC 45-4011)	Percent	83.3%	9.4%	9.6%	55.9%	5.5%	1.3%	0.6%	0.1%	0.1%	0.5%	0.2%	0.0%	(X)	(X)	(X)	0.0%
Forest and conservation workers 6120 (SOC 45-4011)	Female																
Forest and conservation workers 6120 (SOC 45-4011)	Number	2 825	105	160	2 235	160	80	10	4	30	20	0	0	(X)	(X)	(X)	25
Forest and conservation workers 6120 (SOC 45-4011)	Percent	16.7%	0.6%	0.9%	13.2%	0.9%	0.5%	0.1%	0.0%	0.2%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Logging workers 6130 (SOC 45-4020)	Total both sexes																
Logging workers 6130 (SOC 45-4020)	Number	85 905	4 240	3 260	66 225	9 095	1 850	215	85	65	690	45	0	(X)	(X)	(X)	140
Logging workers 6130 (SOC 45-4020)	Percent	100.0%	4.9%	3.8%	77.1%	10.6%	2.2%	0.3%	0.1%	0.1%	0.8%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Logging workers 6130 (SOC 45-4020)	Male																
Logging workers 6130 (SOC 45-4020)	Number	83 750	4 100	3 190	64 540	8 955	1 775	205	85	50	685	45	0	(X)	(X)	(X)	120
Logging workers 6130 (SOC 45-4020)	Percent	97.5%	4.8%	3.7%	75.1%	10.4%	2.1%	0.2%	0.1%	0.1%	0.8%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Logging workers 6130 (SOC 45-4020)	Female																
Logging workers 6130 (SOC 45-4020)	Number	2 155	135	65	1 685	140	75	10	0	15	10	0	0	(X)	(X)	(X)	20
Logging workers 6130 (SOC 45-4020)	Percent	2.5%	0.2%	0.1%	2.0%	0.2%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
First-line supervisors of construction trades and extraction	Total both sexes																
First-line supervisors of construction trades and extraction	Number	1 033 845	86 050	61 380	815 140	41 445	7 400	10 080	1 395	990	5 230	1 200	390	(X)	(X)	(X)	3 150
First-line supervisors of construction trades and extraction	Percent	100.0%	8.3%	5.9%	78.8%	4.0%	0.7%	1.0%	0.1%	0.1%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.3%
First-line supervisors of construction trades and extraction	Male																
First-line supervisors of construction trades and extraction	Number	1 003 545	83 315	59 875	792 630	39 260	7 175	9 595	1 325	990	4 985	1 160	315	(X)	(X)	(X)	2 915
First-line supervisors of construction trades and extraction	Percent	97.1%	8.1%	5.8%	76.7%	3.8%	0.7%	0.9%	0.1%	0.1%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.3%
First-line supervisors of construction trades and extraction	Female																
First-line supervisors of construction trades and extraction	Number	30,300	2,735	1,505	22,510	2,180	225	485	70	0	245	40	75	(X)	(X)	(X)	230
First-line supervisors of construction trades and extraction	Percent	2.9%	0.3%	0.1%	2.2%	0.2%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Boilermakers 6210 (SOC 47-2011)	Total both sexes																
Boilermakers 6210 (SOC 47-2011)	Number	22,165	1,450	1,235	17,260	1,415	345	155	35	0	125	40	25	(X)	(X)	(X)	80
Boilermakers 6210 (SOC 47-2011)	Percent	100.0%	6.5%	5.6%	77.9%	6.4%	1.6%	0.7%	0.2%	0.0%	0.6%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Boilermakers 6210 (SOC 47-2011)	Male																
Boilermakers 6210 (SOC 47-2011)	Number	21 655	1 435	1 165	16 975	1 320	310	140	35	0	125	40	25	(X)	(X)	(X)	80
Boilermakers 6210 (SOC 47-2011)	Percent	97.7%	6.5%	5.3%	76.6%	6.0%	1.4%	0.6%	0.2%	0.0%	0.6%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Boilermakers 6210 (SOC 47-2011)	Female																
Boilermakers 6210 (SOC 47-2011)	Number	510	15	75	280	95	35	10	0	0	0	0	0	(X)	(X)	(X)	0
Boilermakers 6210 (SOC 47-2011)	Percent	2.3%	0.1%	0.3%	1.3%	0.4%	0.2%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Brickmasons blockmasons and stonemasons 6220 (SOC	Total both sexes																
Brickmasons blockmasons and stonemasons 6220 (SOC	Number	225 620	42 005	34 750	120 710	21 510	2 005	1 470	635	215	725	215	75	(X)	(X)	(X)	1 310

Brickmasons, blockmasons, and stonemasons 6220 (SOC	Percent	100.0%	18.6%	15.4%	53.5%	9.5%	0.9%	0.7%	0.3%	0.1%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.6%
Brickmasons, blockmasons, and stonemasons 6220 (SOC	Male																
Brickmasons, blockmasons, and stonemasons 6220 (SOC	Number	223 455	41 810	34 540	119 320	21 300	1 910	1 415	635	205	725	215	75	(X)	(X)	(X)	1 310
Brickmasons, blockmasons, and stonemasons 6220 (SOC	Percent	99.0%	18.5%	15.3%	52.9%	9.4%	0.8%	0.6%	0.3%	0.1%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.6%
Brickmasons, blockmasons, and stonemasons 6220 (SOC	Female																
Brickmasons, blockmasons, and stonemasons 6220 (SOC	Number	2 165	195	210	1 390	205	95	55	0	15	0	0	0	(X)	(X)	(X)	0
Brickmasons, blockmasons, and stonemasons 6220 (SOC	Percent	1.0%	0.1%	0.1%	0.6%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Carpenters 6230 (SOC 47-2031)	Total, both sexes																
Carpenters 6230 (SOC 47-2031)	Number	1 619 895	238 595	176 945	1 066 245	77 795	14 730	20 420	2 965	1 570	8 260	2 080	440	(X)	(X)	(X)	9 845
Carpenters 6230 (SOC 47-2031)	Percent	100.0%	14.7%	10.9%	65.8%	4.8%	0.9%	1.3%	0.2%	0.1%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.6%
Carpenters 6230 (SOC 47-2031)	Male																
Carpenters 6230 (SOC 47-2031)	Number	1 590 715	235 665	174 775	1 045 920	75 720	14 200	19 810	2 865	1 560	8 075	2 020	405	(X)	(X)	(X)	9 705
Carpenters 6230 (SOC 47-2031)	Percent	98.2%	14.5%	10.8%	64.6%	4.7%	0.9%	1.2%	0.2%	0.1%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.6%
Carpenters 6230 (SOC 47-2031)	Female																
Carpenters 6230 (SOC 47-2031)	Number	29 180	2 930	2 170	20 330	2 075	535	610	100	10	190	60	35	(X)	(X)	(X)	140
Carpenters 6230 (SOC 47-2031)	Percent	1.8%	0.2%	0.1%	1.3%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Carpet floor and tile installers and finishers 6240 (SOC	Total, both sexes																
Carpet floor and tile installers and finishers 6240 (SOC	Number	235 185	53 345	38 700	125 130	10 535	1 110	2 790	245	220	1 045	300	45	(X)	(X)	(X)	1 710
Carpet floor and tile installers and finishers 6240 (SOC	Percent	100.0%	22.7%	16.5%	53.2%	4.5%	0.5%	1.2%	0.1%	0.1%	0.4%	0.1%	0.0%	(X)	(X)	(X)	0.7%
Carpet floor and tile installers and finishers 6240 (SOC	Male																
Carpet floor and tile installers and finishers 6240 (SOC	Number	229 835	52 280	38 290	121 900	10 320	1 040	2 640	245	220	990	295	45	(X)	(X)	(X)	1 565
Carpet floor and tile installers and finishers 6240 (SOC	Percent	97.7%	22.2%	16.3%	51.8%	4.4%	0.4%	1.1%	0.1%	0.1%	0.4%	0.1%	0.0%	(X)	(X)	(X)	0.7%
Carpet floor and tile installers and finishers 6240 (SOC	Female																
Carpet floor and tile installers and finishers 6240 (SOC	Number	5 350	1 065	415	3 230	220	65	150	0	0	55	4	0	(X)	(X)	(X)	145
Carpet floor and tile installers and finishers 6240 (SOC	Percent	2.3%	0.5%	0.2%	1.4%	0.1%	0.0%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Cement masons, concrete finishers, and terrazzo workers	Total, both sexes																
Cement masons concrete finishers and terrazzo workers	Number	95 685	24 555	16 475	40 855	11 155	970	245	295	120	475	40	135	(X)	(X)	(X)	365
Cement masons concrete finishers and terrazzo workers	Percent	100.0%	25.7%	17.2%	42.7%	11.7%	1.0%	0.3%	0.3%	0.1%	0.5%	0.0%	0.1%	(X)	(X)	(X)	0.4%
Cement masons, concrete finishers, and terrazzo workers	Male																
Cement masons concrete finishers and terrazzo workers	Number	94 535	24 440	16 295	40 155	11 025	960	245	295	120	460	40	135	(X)	(X)	(X)	365
Cement masons concrete finishers and terrazzo workers	Percent	98.8%	25.5%	17.0%	42.0%	11.5%	1.0%	0.3%	0.3%	0.1%	0.5%	0.0%	0.1%	(X)	(X)	(X)	0.4%
Cement masons concrete finishers and terrazzo workers	Female																
Cement masons concrete finishers and terrazzo workers	Number	1 150	115	180	700	130	15	0	0	0	15	0	0	(X)	(X)	(X)	0
Cement masons concrete finishers and terrazzo workers	Percent	1.2%	0.1%	0.2%	0.7%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Construction laborers 6260 (SOC 47-2061)	Total, both sexes																
Construction laborers 6260 (SOC 47-2061)	Number	1 932 325	409 000	312 920	982 095	154 495	16 410	26 855	3 855	2 895	9 610	2 085	785	(X)	(X)	(X)	11 325
Construction laborers 6260 (SOC 47-2061)	Percent	100.0%	21.2%	16.2%	50.8%	8.0%	0.8%	1.4%	0.2%	0.1%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.6%
Construction laborers 6260 (SOC 47-2061)	Male																
Construction laborers 6260 (SOC 47-2061)	Number	1 872 555	401 950	305 755	945 955	148 560	15 550	25 685	3 675	2 860	9 170	1 980	715	(X)	(X)	(X)	10 695
Construction laborers 6260 (SOC 47-2061)	Percent	96.9%	20.8%	15.8%	49.0%	7.7%	0.8%	1.3%	0.2%	0.1%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.6%
Construction laborers 6260 (SOC 47-2061)	Female																
Construction laborers 6260 (SOC 47-2061)	Number	59 770	7 045	7 160	36 145	5 935	860	1 170	175	35	440	105	65	(X)	(X)	(X)	630
Construction laborers 6260 (SOC 47-2061)	Percent	3.1%	0.4%	0.4%	1.9%	0.3%	0.0%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Paving surfacing and tamping equipment operators 6300	Total, both sexes																
Paving surfacing and tamping equipment operators 6300	Number	21 530	2 170	2 375	14 570	2 015	110	30	20	40	185	10	0	(X)	(X)	(X)	4
Paving surfacing and tamping equipment operators 6300	Percent	100.0%	10.1%	11.0%	67.7%	9.4%	0.5%	0.1%	0.1%	0.2%	0.9%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Paving surfacing and tamping equipment operators 6300	Male																
Paving surfacing and tamping equipment operators 6300	Number	20 865	2 170	2 355	13 975	1 985	110	30	10	40	180	10	0	(X)	(X)	(X)	4
Paving surfacing and tamping equipment operators 6300	Percent	96.9%	10.1%	10.9%	64.9%	9.2%	0.5%	0.1%	0.0%	0.2%	0.8%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Paving surfacing and tamping equipment operators 6300	Female																
Paving, surfacing, and tamping equipment operators 6300	Number	660	0	20	595	30	0	0	10	0	4	0	0	(X)	(X)	(X)	0
Paving surfacing and tamping equipment operators 6300	Percent	3.1%	0.0%	0.1%	2.8%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Construction equipment operators except paving	Total, both sexes																
Construction equipment operators except paving,	Number	417,390	33,965	21,425	321,700	25,785	5,880	1,565	915	305	3,455	310	225	(X)	(X)	(X)	1,855
Construction equipment operators except paving	Percent	100.0%	8.1%	5.1%	77.1%	6.2%	1.4%	0.4%	0.2%	0.1%	0.8%	0.1%	0.1%	(X)	(X)	(X)	0.4%
Construction equipment operators except paving	Male																
Construction equipment operators except paving	Number	407 660	33 340	21 010	314 455	24 915	5 705	1 485	865	290	3 330	300	215	(X)	(X)	(X)	1 750
Construction equipment operators except paving	Percent	97.7%	8.0%	5.0%	75.3%	6.0%	1.4%	0.4%	0.2%	0.1%	0.8%	0.1%	0.1%	(X)	(X)	(X)	0.4%
Construction equipment operators except paving	Female																
Construction equipment operators except paving	Number	9 730	630	415	7 250	865	175	80	50	15	125	10	15	(X)	(X)	(X)	105
Construction equipment operators except paving	Percent	2.3%	0.2%	0.1%	1.7%	0.2%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Drywall installers ceiling tile installers and tapers 6330	Total, both sexes																
Drywall installers ceiling tile installers and tapers 6330	Number	213 410	62 890	50 050	83 925	10 135	2 475	1 245	210	285	825	245	90	(X)	(X)	(X)	1 035
Drywall installers ceiling tile installers and tapers 6330	Percent	100.0%	29.5%	23.5%	39.3%	4.7%	1.2%	0.6%	0.1%	0.1%	0.4%	0.1%	0.0%	(X)	(X)	(X)	0.5%
Drywall installers ceiling tile installers and tapers 6330	Male																
Drywall installers ceiling tile installers and tapers 6330	Number	208 520	61 915	49 255	81 370	9 775	2 355	1 245	210	285	745	245	90	(X)	(X)	(X)	1 025
Drywall installers ceiling tile installers and tapers 6330	Percent	97.7%	29.0%	23.1%	38.1%	4.6%	1.1%	0.6%	0.1%	0.1%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.5%
Drywall installers ceiling tile installers and tapers 6330	Female																
Drywall installers ceiling tile installers and tapers 6330	Number	4 895	975	795	2 555	365	115	0	0	0	75	0	0	(X)	(X)	(X)	10
Drywall installers ceiling tile installers and tapers 6330	Percent	2.3%	0.5%	0.4%	1.2%	0.2%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Electricians 6355 (SOC 47-2111)	Total, both sexes																
Electricians 6355 (SOC 47-2111)	Number	830 730	72 495	46 845	620 675	58 190	5 640	15 210	1 425	785	4 135	1 610	270	(X)	(X)	(X)	3 445
Electricians 6355 (SOC 47-2111)	Percent	100.0%	8.7%	5.6%	74.7%	7.0%	0.7%	1.8%	0.2%	0.1%	0.5%	0.2%	0.0%	(X)	(X)	(X)	0.4%
Electricians 6355 (SOC 47-2111)	Male																
Electricians 6355 (SOC 47-2111)	Number	813 400	71 240	46 030	608 190	56 365	5 430	14 845	1 355	755	3 975	1 580	245	(X)	(X)	(X)	3 385
Electricians 6355 (SOC 47-2111)	Percent	97.9%	8.6%	5.5%	73.2%	6.8%	0.7%	1.8%	0.2%	0.1%	0.5%	0.2%	0.0%	(X)	(X)	(X)	0.4%
Electricians 6355 (SOC 47-2111)	Female																
Electricians 6355 (SOC 47-2111)	Number	17 330	1 255	815	12 490	1 825	210	365	70	30	160	35	25	(X)	(X)	(X)	60
Electricians 6355 (SOC 47-2111)	Percent	2.1%	0.2%	0.1%	1.5%	0.2%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Glaziers 6360 (SOC 47-2121)	Total, both sexes																
Glaziers 6360 (SOC 47-2121)	Number	47 900	5 185	4 150	34 500	2 100	410	710	115	75	285	85	0	(X)	(X)	(X)	285
Glaziers 6360 (SOC 47-2121)	Percent	100.0%	10.8%	8.7%	72.0%	4.4%	0.9%	1.5%	0.2%	0.2%	0.6%	0.2%	0.0%	(X)	(X)	(X)	0.6%
Glaziers 6360 (SOC 47-2121)	Male																
Glaziers 6360 (SOC 47-2121)	Number	47 000	5 105	4 140	33 815	2 010	400	700	115	75	270	85	0	(X)	(X)	(X)	285
Glaziers 6360 (SOC 47-2121)	Percent	98.1%	10.7%	8.6%	70.6%	4.2%	0.8%	1.5%	0.2%	0.2%	0.6%	0.2%	0.0%	(X)	(X)	(X)	0.6%
Glaziers 6360 (SOC 47-2121)	Female																
Glaziers 6360 (SOC 47-2121)	Number	900	75	10	685	90	10	10	0	0	15	0	0	(X)	(X)	(X)	0
Glaziers 6360 (SOC 47-2121)	Percent	1.9%	0.2%	0.0%	1.4%	0.2%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Insulation workers 6400 (SOC 47-2130)	Total, both sexes																
Insulation workers 6400 (SOC 47-2130)	Number	49 660	10 730	7 175	26 640	3 800	360	230	70	35	250	70	0	(X)	(X)	(X)	295
Insulation workers 6400 (SOC 47-2130)	Percent	100.0%	21.6%	14.4%	53.6%	7.7%	0.7%	0.5%	0.1%	0.1%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.6%
Insulation workers 6400 (SOC 47-2130)	Male																
Insulation workers 6400 (SOC 47-2130)	Number	47 695	10 395	6 935	25 750	3 470	325	215	70	35	210	70	0	(X)	(X)	(X)	225
Insulation workers 6400 (SOC 47-2130)	Percent	96.0%	20.9%	14.0%	51.9%	7.0%	0.7%	0.4%	0.1%	0.1%	0.4%	0.1%	0.0%	(X)	(X)	(X)	0.5%
Insulation workers 6400 (SOC 47-2130)	Female																
Insulation workers 6400 (SOC 47-2130)	Number	1 960	340	240	895	330	35	15	0	0	35	0	0	(X)	(X)	(X)	70
Insulation workers 6400 (SOC 47-2130)	Percent	3.9%	0.7%	0.5%	1.8%	0.7%	0.1%	0.0%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Painters construction and maintenance 6420 (SOC 47-	Total, both sexes																
Painters construction and maintenance 6420 (SOC 47-	Number	676 715	138 910	122 050	347 110	44 275	3 505	10 845	880	850	2 580	955	305	(X)	(X)	(X)	4 445
Painters construction and maintenance 6420 (SOC 47-	Percent	100.0%	20.5%	18.0%	51.3%	6.5%	0.5%	1.6%	0.1%	0.1%	0.4%	0.1%	0.0%	(X)	(X)	(X)	0.7%
Painters, construction and maintenance 6420 (SOC 47-	Male																
Painters construction and maintenance 6420 (SOC 47-	Number	629 400	134 545	118 165	312 130	42 170	3 140	10 035	865	760	2 405	880	265	(X)	(X)	(X)	4 045
Painters construction and maintenance 6420 (SOC 47-	Percent	93.0%	19.9%	17.5%	46.1%	6.2%	0.5%	1.5%	0.1%	0.1%	0.4%	0.1%	0.0%	(X)	(X)	(X)	0.6%
Painters, construction and maintenance 6420 (SOC 47-	Female																
Painters construction and maintenance 6420 (SOC 47-	Number	47 315	4 365	3 885	34 980	2 110	365	810	20	90	175	75	40	(X)	(X)	(X)	400
Painters construction and maintenance 6420 (SOC 47-	Percent	7.0%	0.6%	0.6%	5.2%	0.3%	0.1%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Paperhangers 6430 (SOC 47-2142)	Total, both sexes																
Paperhangers 6430 (SOC 47-2142)	Number	8 985	895	415	7 010	270	30	275	0	0	35	25	0	(X)	(X)	(X)	25
Paperhangers 6430 (SOC 47-2142)	Percent	100.0%	10.0%	4.6%	78.0%	3.0%	0.3%	3.1%	0.0%	0.0%	0.4%	0.3%	0.0%	(X)	(X)	(X)	0.3%
Paperhangers 6430 (SOC 47-2142)	Male																
Paperhangers 6430 (SOC 47-2142)	Number	6 880	805	395	5 110	230	20	270	0	0	20	10	0	(X)	(X)	(X)	25
Paperhangers 6430 (SOC 47-2142)	Percent	76.6%	9.0%	4.4%	56.9%	2.6%	0.2%	3.0%	0.0%	0.0%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Paperhangers 6430 (SOC 47-2142)	Female																
Paperhangers 6430 (SOC 47-2142)	Number	2 105	90	25	1 900	40	10	4	0	0	15	15	0	(X)	(X)	(X)	0
Paperhangers 6430 (SOC 47-2142)	Percent	23.4%	1.0%	0.3%	21.1%	0.4%	0.1%	0.0%	0.0%	0.0%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.0%
Pipelayers plumbers pipefitters and steamfitters 6440	Total, both sexes																
Pipelayers plumbers pipefitters and steamfitters 6440	Number	623 165	72 580	48 930	437 930	43 380	5 075	6 520	975	715	3 325	875	185	(X)	(X)	(X)	2 675
Pipelayers plumbers pipefitters and steamfitters 6440	Percent	100.0%	11.6%	7.9%	70.3%	7.0%	0.8%	1.0%	0.2%	0.1%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.4%
Pipelayers plumbers pipefitters and steamfitters 6440	Male																
Pipelayers plumbers pipefitters and steamfitters 6440	Number	614 125	71 750	48 250	431 620	42 695	4 915	6 420	975	715	3 210	850	185	(X)	(X)	(X)	2 530
Pipelayers plumbers pipefitters and steamfitters 6440	Percent	98.5%	11.5%	7.7%	69.3%	6.9%	0.8%	1.0%	0.2%	0.1%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.4%
Pipelayers plumbers pipefitters and steamfitters 6440	Female																
Pipelayers plumbers pipefitters and steamfitters 6440	Number	9 045	830	680	6 310	685	160	100	0	0	110	25	0	(X)	(X)	(X)	145
Pipelayers plumbers pipefitters and steamfitters 6440	Percent	1.5%	0.1%	0.1%	1.0%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Plasterers and stucco masons 6460 (SOC 47-2161)	Total, both sexes																
Plasterers and stucco masons 6460 (SOC 47-2161)	Number	49,780	17,650	11,895	15,325	4,270	160	75	45	4	35	15	15	(X)	(X)	(X)	300
Plasterers and stucco masons 6460 (SOC 47-2161)	Percent	100.0%	35.5%	23.9%	30.8%	8.6%	0.3%	0.2%	0.1%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.6%
Plasterers and stucco masons 6460 (SOC 47-2161)	Male																
Plasterers and stucco masons 6460 (SOC 47-2161)	Number	49,050	17,470	11,745	14,990	4,220	140	75	45	4	35	15	15	(X)	(X)	(X)	300
Plasterers and stucco masons 6460 (SOC 47-2161)	Percent	98.5%	35.1%	23.6%	30.1%	8.5%	0.3%	0.2%	0.1%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.6%
Plasterers and stucco masons 6460 (SOC 47-2161)	Female																
Plasterers and stucco masons 6460 (SOC 47-2161)	Number	735	175	155	340	45	20	0	0	0	0	0	0	(X)	(X)	(X)	0
Plasterers and stucco masons 6460 (SOC 47-2161)	Percent	1.5%	0.4%	0.3%	0.7%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Reinforcing iron and rebar workers 6500 (SOC 47-2171)	Total, both sexes																
Reinforcing iron and rebar workers 6500 (SOC 47-2171)	Number	10 670	2 035	1 525	5 795	785	230	105	30	0	50	60	0	(X)	(X)	(X)	50
Reinforcing iron and rebar workers 6500 (SOC 47-2171)	Percent	100.0%	19.1%	14.3%	54.3%	7.4%	2.2%	1.0%	0.3%	0.0%	0.5%	0.6%	0.0%	(X)	(X)	(X)	0.5%
Reinforcing iron and rebar workers 6500 (SOC 47-2171)	Male																
Reinforcing iron and rebar workers 6500 (SOC 47-2171)	Number	10 525	2 035	1 520	5 660	780	230	105	30	0	50	60	0	(X)	(X)	(X)	50

Reinforcing iron and rebar workers 6500 (SOC 47-2171)	Percent	98.6%	19.1%	14.2%	53.0%	7.3%	2.2%	1.0%	0.3%	0.0%	0.5%	0.6%	0.0%	(X)	(X)	(X)	0.5%
Reinforcing iron and rebar workers 6500 (SOC 47-2171)	Female																
Reinforcing iron and rebar workers 6500 (SOC 47-2171)	Number	145	0	4	140	4	0	0	0	0	0	0	0	(X)	(X)	(X)	0
Reinforcing iron and rebar workers 6500 (SOC 47-2171)	Percent	1.4%	0.0%	0.0%	1.3%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Roofers 6515 (SOC 47-2181)	Total, both sexes																
Roofers 6515 (SOC 47-2181)	Number	255 565	63 160	50 450	119 665	15 315	2 225	1 235	470	635	1 145	285	80	(X)	(X)	(X)	895
Roofers 6515 (SOC 47-2181)	Percent	100.0%	24.7%	19.7%	46.8%	6.0%	0.9%	0.5%	0.2%	0.2%	0.4%	0.1%	0.0%	(X)	(X)	(X)	0.4%
Roofers 6515 (SOC 47-2181)	Male																
Roofers 6515 (SOC 47-2181)	Number	252 500	62 750	50 185	117 575	15 205	2 105	1 215	470	635	1 100	285	80	(X)	(X)	(X)	895
Roofers 6515 (SOC 47-2181)	Percent	98.8%	24.6%	19.6%	46.0%	5.9%	0.8%	0.5%	0.2%	0.2%	0.4%	0.1%	0.0%	(X)	(X)	(X)	0.4%
Roofers 6515 (SOC 47-2181)	Female																
Roofers 6515 (SOC 47-2181)	Number	3 065	410	265	2 090	110	120	20	0	0	45	0	0	(X)	(X)	(X)	0
Roofers 6515 (SOC 47-2181)	Percent	1.2%	0.2%	0.1%	0.8%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Sheet metal workers 6520 (SOC 47-2211)	Total, both sexes																
Sheet metal workers 6520 (SOC 47-2211)	Number	147 415	12 555	8 860	112 220	8 530	720	2 495	205	250	885	185	55	(X)	(X)	(X)	455
Sheet metal workers 6520 (SOC 47-2211)	Percent	100.0%	8.5%	6.0%	76.1%	5.8%	0.5%	1.7%	0.1%	0.2%	0.6%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Sheet metal workers 6520 (SOC 47-2211)	Male																
Sheet metal workers 6520 (SOC 47-2211)	Number	141 580	12 310	8 365	108 120	7 900	670	2 355	190	250	780	165	45	(X)	(X)	(X)	435
Sheet metal workers 6520 (SOC 47-2211)	Percent	96.0%	8.4%	5.7%	73.3%	5.4%	0.5%	1.6%	0.1%	0.2%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Sheet metal workers 6520 (SOC 47-2211)	Female																
Sheet metal workers 6520 (SOC 47-2211)	Number	5 830	245	495	4 100	630	50	140	15	0	105	20	10	(X)	(X)	(X)	20
Sheet metal workers 6520 (SOC 47-2211)	Percent	4.0%	0.2%	0.3%	2.8%	0.4%	0.0%	0.1%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Structural iron and steel workers 6530 (SOC 47-2221)	Total, both sexes																
Structural iron and steel workers 6530 (SOC 47-2221)	Number	75 900	7 470	5 630	53 905	5 555	1 195	850	255	205	415	100	60	(X)	(X)	(X)	265
Structural iron and steel workers 6530 (SOC 47-2221)	Percent	100.0%	9.8%	7.4%	71.0%	7.3%	1.6%	1.1%	0.3%	0.3%	0.5%	0.1%	0.1%	(X)	(X)	(X)	0.3%
Structural iron and steel workers 6530 (SOC 47-2221)	Male																
Structural iron and steel workers 6530 (SOC 47-2221)	Number	74 015	7 320	5 535	52 770	5 220	1 150	805	255	160	395	85	60	(X)	(X)	(X)	265
Structural iron and steel workers 6530 (SOC 47-2221)	Percent	97.5%	9.6%	7.3%	69.5%	6.9%	1.5%	1.1%	0.3%	0.2%	0.5%	0.1%	0.1%	(X)	(X)	(X)	0.3%
Structural iron and steel workers 6530 (SOC 47-2221)	Female																
Structural iron and steel workers 6530 (SOC 47-2221)	Number	1 885	150	95	1 135	335	45	45	0	45	20	15	0	(X)	(X)	(X)	0
Structural iron and steel workers 6530 (SOC 47-2221)	Percent	2.5%	0.2%	0.1%	1.5%	0.4%	0.1%	0.1%	0.0%	0.1%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Helpers construction trades 6600 (SOC 47-3010)	Total, both sexes																
Helpers construction trades 6600 (SOC 47-3010)	Number	98 490	23 430	16 260	46 315	8 965	915	1 185	100	160	515	195	20	(X)	(X)	(X)	430
Helpers construction trades 6600 (SOC 47-3010)	Percent	100.0%	23.8%	16.5%	47.0%	9.1%	0.9%	1.2%	0.1%	0.2%	0.5%	0.2%	0.0%	(X)	(X)	(X)	0.4%
Helpers construction trades 6600 (SOC 47-3010)	Male																
Helpers construction trades 6600 (SOC 47-3010)	Number	94 220	22 780	15 760	43 830	8 620	820	1 005	100	160	510	180	20	(X)	(X)	(X)	430
Helpers construction trades 6600 (SOC 47-3010)	Percent	95.7%	23.1%	16.0%	44.5%	8.8%	0.8%	1.0%	0.1%	0.2%	0.5%	0.2%	0.0%	(X)	(X)	(X)	0.4%
Helpers construction trades 6600 (SOC 47-3010)	Female																
Helpers construction trades 6600 (SOC 47-3010)	Number	4 265	650	500	2 485	345	90	175	0	0	4	15	0	(X)	(X)	(X)	0
Helpers construction trades 6600 (SOC 47-3010)	Percent	4.3%	0.7%	0.5%	2.5%	0.4%	0.1%	0.2%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Construction and bu lding inspectors 6660 (SOC 47-4011)	Total, both sexes																
Construction and bu lding inspectors 6660 (SOC 47-4011)	Number	108 345	6 195	2 875	85 170	9 270	820	2 790	195	105	525	130	40	(X)	(X)	(X)	230
Construction and bu lding inspectors 6660 (SOC 47-4011)	Percent	100.0%	5.7%	2.7%	78.6%	8.6%	0.8%	2.6%	0.2%	0.1%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Construction and bu lding inspectors 6660 (SOC 47-4011)	Male																
Construction and bu lding inspectors 6660 (SOC 47-4011)	Number	96 430	5 475	2 440	76 720	7 410	740	2 565	180	105	475	105	30	(X)	(X)	(X)	190
Construction and bu lding inspectors 6660 (SOC 47-4011)	Percent	89.0%	5.1%	2.3%	70.8%	6.8%	0.7%	2.4%	0.2%	0.1%	0.4%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Construction and bu lding inspectors 6660 (SOC 47-4011)	Female																
Construction and bu lding inspectors 6660 (SOC 47-4011)	Number	11 915	720	435	8 450	1 860	80	225	15	0	55	25	10	(X)	(X)	(X)	45
Construction and bu lding inspectors 6660 (SOC 47-4011)	Percent	11.0%	0.7%	0.4%	7.8%	1.7%	0.1%	0.2%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Elevator installers and repairers 6700 (SOC 47-4021)	Total, both sexes																
Elevator installers and repairers 6700 (SOC 47-4021)	Number	29,510	1,950	1,050	23,935	1,715	45	395	75	10	130	130	0	(X)	(X)	(X)	80
Elevator installers and repairers 6700 (SOC 47-4021)	Percent	100.0%	6.6%	3.6%	81.1%	5.8%	0.2%	1.3%	0.3%	0.0%	0.4%	0.4%	0.0%	(X)	(X)	(X)	0.3%
Elevator installers and repairers 6700 (SOC 47-4021)	Male																
Elevator installers and repairers 6700 (SOC 47-4021)	Number	28,980	1,925	1,010	23,560	1,625	45	395	75	10	125	130	0	(X)	(X)	(X)	80
Elevator installers and repairers 6700 (SOC 47-4021)	Percent	98.2%	6.5%	3.4%	79.8%	5.5%	0.2%	1.3%	0.3%	0.0%	0.4%	0.4%	0.0%	(X)	(X)	(X)	0.3%
Elevator installers and repairers 6700 (SOC 47-4021)	Female																
Elevator installers and repairers 6700 (SOC 47-4021)	Number	535	25	35	375	95	0	0	0	0	4	0	0	(X)	(X)	(X)	0
Elevator installers and repairers 6700 (SOC 47-4021)	Percent	1.8%	0.1%	0.1%	1.3%	0.3%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Fence erectors 6710 (SOC 47-4031)	Total, both sexes																
Fence erectors 6710 (SOC 47-4031)	Number	35 570	7 465	3 700	21 575	1 755	345	150	90	35	305	25	4	(X)	(X)	(X)	125
Fence erectors 6710 (SOC 47-4031)	Percent	100.0%	21.0%	10.4%	60.7%	4.9%	1.0%	0.4%	0.3%	0.1%	0.9%	0.1%	0.0%	(X)	(X)	(X)	0.4%
Fence erectors 6710 (SOC 47-4031)	Male																
Fence erectors 6710 (SOC 47-4031)	Number	35 035	7 375	3 670	21 180	1 735	345	150	90	35	305	25	4	(X)	(X)	(X)	125
Fence erectors 6710 (SOC 47-4031)	Percent	98.5%	20.7%	10.3%	59.5%	4.9%	1.0%	0.4%	0.3%	0.1%	0.9%	0.1%	0.0%	(X)	(X)	(X)	0.4%
Fence erectors 6710 (SOC 47-4031)	Female																
Fence erectors 6710 (SOC 47-4031)	Number	535	90	25	395	20	0	0	0	0	0	0	0	(X)	(X)	(X)	0
Fence erectors 6710 (SOC 47-4031)	Percent	1.5%	0.3%	0.1%	1.1%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Hazardous materials removal workers 6720 (SOC 47-	Total, both sexes																
Hazardous materials removal workers 6720 (SOC 47-	Number	35 395	4 880	4 370	18 535	6 005	425	690	55	45	130	15	60	(X)	(X)	(X)	190
Hazardous materials removal workers 6720 (SOC 47-	Percent	100.0%	13.8%	12.3%	52.4%	17.0%	1.2%	1.9%	0.2%	0.1%	0.4%	0.0%	0.2%	(X)	(X)	(X)	0.5%
Hazardous materials removal workers 6720 (SOC 47-	Male																
Hazardous materials removal workers 6720 (SOC 47-	Number	29 260	4 005	3 715	15 605	4 645	340	485	55	45	130	0	60	(X)	(X)	(X)	170
Hazardous materials removal workers 6720 (SOC 47-	Percent	82.7%	11.3%	10.5%	44.1%	13.1%	1.0%	1.4%	0.2%	0.1%	0.4%	0.0%	0.2%	(X)	(X)	(X)	0.5%
Hazardous materials removal workers 6720 (SOC 47-	Female																
Hazardous materials removal workers 6720 (SOC 47-	Number	6 135	870	655	2 930	1 360	85	205	0	0	0	15	0	(X)	(X)	(X)	15
Hazardous materials removal workers 6720 (SOC 47-	Percent	17.3%	2.5%	1.9%	8.3%	3.8%	0.2%	0.6%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Highway maintenance workers 6730 (SOC 47-4051)	Total, both sexes																
Highway maintenance workers 6730 (SOC 47-4051)	Number	109 780	7 790	5 170	82 245	11 615	1 260	405	90	75	545	65	100	(X)	(X)	(X)	415
Highway maintenance workers 6730 (SOC 47-4051)	Percent	100.0%	7.1%	4.7%	74.9%	10.6%	1.1%	0.4%	0.1%	0.1%	0.5%	0.1%	0.1%	(X)	(X)	(X)	0.4%
Highway maintenance workers 6730 (SOC 47-4051)	Male																
Highway maintenance workers 6730 (SOC 47-4051)	Number	105 875	7 625	5 015	79 180	11 220	1 225	395	90	75	520	65	65	(X)	(X)	(X)	395
Highway maintenance workers 6730 (SOC 47-4051)	Percent	96.4%	6.9%	4.6%	72.1%	10.2%	1.1%	0.4%	0.1%	0.1%	0.5%	0.1%	0.1%	(X)	(X)	(X)	0.4%
Highway maintenance workers 6730 (SOC 47-4051)	Female																
Highway maintenance workers 6730 (SOC 47-4051)	Number	3 905	165	155	3 065	395	35	10	0	0	25	0	35	(X)	(X)	(X)	20
Highway maintenance workers 6730 (SOC 47-4051)	Percent	3.6%	0.2%	0.1%	2.8%	0.4%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Rail-track laying and maintenance equipment operators	Total, both sexes																
Rail-track laying and maintenance equipment operators	Number	12 090	970	600	7 990	2 115	150	160	0	60	30	15	0	(X)	(X)	(X)	0
Rail-track laying and maintenance equipment operators	Percent	100.0%	8.0%	5.0%	66.1%	17.5%	1.2%	1.3%	0.0%	0.5%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.0%
Rail-track laying and maintenance equipment operators	Male																
Rail-track laying and maintenance equipment operators	Number	11 895	940	600	7 880	2 070	150	160	0	60	30	15	0	(X)	(X)	(X)	0
Rail-track laying and maintenance equipment operators	Percent	98.4%	7.8%	5.0%	65.2%	17.1%	1.2%	1.3%	0.0%	0.5%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.0%
Rail-track laying and maintenance equipment operators	Female																
Rail-track laying and maintenance equipment operators	Number	190	35	0	110	50	0	0	0	0	0	0	0	(X)	(X)	(X)	0
Rail-track laying and maintenance equipment operators	Percent	1.6%	0.3%	0.0%	0.9%	0.4%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Miscellaneous construction workers including solar	Total, both sexes																
Miscellaneous construction workers including solar	Number	53 095	7 365	5 150	33 740	4 850	290	640	110	20	350	40	10	(X)	(X)	(X)	525
Miscellaneous construction workers including solar	Percent	100.0%	13.9%	9.7%	63.5%	9.1%	0.5%	1.2%	0.2%	0.0%	0.7%	0.1%	0.0%	(X)	(X)	(X)	1.0%
Miscellaneous construction workers including solar	Male																
Miscellaneous construction workers including solar	Number	51 055	7 075	5 010	32 490	4 565	270	615	110	20	350	15	10	(X)	(X)	(X)	525
Miscellaneous construction workers including solar	Percent	96.2%	13.3%	9.4%	61.2%	8.6%	0.5%	1.2%	0.2%	0.0%	0.7%	0.0%	0.0%	(X)	(X)	(X)	1.0%
Miscellaneous construction workers, including solar	Female																
Miscellaneous construction workers including solar	Number	2 035	290	145	1 250	285	15	20	4	0	0	25	0	(X)	(X)	(X)	0
Miscellaneous construction workers including solar	Percent	3.8%	0.5%	0.3%	2.4%	0.5%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Derrick, rotary drill, and service unit operators, and	Total, both sexes																
Derrick rotary drill and service unit operators and	Number	41 935	6 560	2 790	28 675	2 320	845	55	4	25	540	80	0	(X)	(X)	(X)	45
Derrick rotary drill and service unit operators and	Percent	100.0%	15.6%	6.7%	68.4%	5.5%	2.0%	0.1%	0.0%	0.1%	1.3%	0.2%	0.0%	(X)	(X)	(X)	0.1%
Derrick rotary drill and service unit operators and	Male																
Derrick rotary drill and service unit operators and	Number	41 495	6 510	2 780	28 380	2 290	800	55	4	25	535	65	0	(X)	(X)	(X)	45
Derrick rotary drill and service unit operators and	Percent	99.0%	15.5%	6.6%	67.7%	5.5%	1.9%	0.1%	0.0%	0.1%	1.3%	0.2%	0.0%	(X)	(X)	(X)	0.1%
Derrick rotary drill and service unit operators and	Female																
Derrick rotary drill and service unit operators and	Number	445	50	10	295	25	45	0	0	0	4	15	0	(X)	(X)	(X)	0
Derrick rotary drill and service unit operators and	Percent	1.1%	0.1%	0.0%	0.7%	0.1%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Earth drillers except oil and gas 6820 (SOC 47-5021)	Total, both sexes																
Earth drillers except oil and gas 6820 (SOC 47-5021)	Number	28 535	1 885	1 085	23 845	885	320	115	50	85	195	25	0	(X)	(X)	(X)	40
Earth drillers except oil and gas 6820 (SOC 47-5021)	Percent	100.0%	6.6%	3.8%	83.6%	3.1%	1.1%	0.4%	0.2%	0.3%	0.7%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Earth drillers except oil and gas 6820 (SOC 47-5021)	Male																
Earth drillers except oil and gas 6820 (SOC 47-5021)	Number	28 215	1 830	1 085	23 620	860	310	115	50	85	195	25	0	(X)	(X)	(X)	40
Earth drillers except oil and gas 6820 (SOC 47-5021)	Percent	98.9%	6.4%	3.8%	82.8%	3.0%	1.1%	0.4%	0.2%	0.3%	0.7%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Earth drillers except oil and gas 6820 (SOC 47-5021)	Female																
Earth drillers except oil and gas 6820 (SOC 47-5021)	Number	320	55	0	225	30	10	0	0	0	0	0	0	(X)	(X)	(X)	0
Earth drillers except oil and gas 6820 (SOC 47-5021)	Percent	1.1%	0.2%	0.0%	0.8%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Explosives workers ordnance handling experts and	Total, both sexes																
Explosives workers ordnance handling experts and	Number	11 245	715	485	8 635	1 085	90	65	20	40	35	20	10	(X)	(X)	(X)	45
Explosives workers ordnance handling experts and	Percent	100.0%	6.4%	4.3%	76.8%	9.6%	0.8%	0.6%	0.2%	0.4%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Explosives workers ordnance handling experts and	Male																
Explosives workers, ordnance handling experts, and	Number	10,525	695	470	8,200	910	90	65	20	0	35	20	10	(X)	(X)	(X)	20
Explosives workers ordnance handling experts and	Percent	93.6%	6.2%	4.2%	72.9%	8.1%	0.8%	0.6%	0.2%	0.0%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.2%
Explosives workers ordnance handling experts and	Female																
Explosives workers, ordnance handling experts, and	Number	720	20	20	440	175	0	0	0	40	0	0	0	(X)	(X)	(X)	25
Explosives workers ordnance handling experts and	Percent	6.4%	0.2%	0.2%	3.9%	1.6%	0.0%	0.0%	0.0%	0.4%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.2%
Mining machine operators 6840 (SOC 47-5040)	Total, both sexes																
Mining machine operators 6840 (SOC 47-5040)	Number	60 695	4 730	2 570	49 825	2 215	575	245	30	15	345	35	25	(X)	(X)	(X)	80
Mining machine operators 6840 (SOC 47-5040)	Percent	100.0%	7.8%	4.2%	82.1%	3.6%	0.9%	0.4%	0.0%	0.0%	0.6%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Mining machine operators 6840 (SOC 47-5040)	Male																
Mining machine operators 6840 (SOC 47-5040)	Number	59 280	4 595	2 520	48 885	2 090	535	200	30	15	285	35	25	(X)	(X)	(X)	60
Mining machine operators 6840 (SOC 47-5040)	Percent	97.7%	7.6%	4.2%	80.5%	3.4%	0.9%	0.3%	0.0%	0.0%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Mining machine operators 6840 (SOC 47-5040)	Female																
Mining machine operators 6840 (SOC 47-5040)	Number	1 415	135	50	940	120	45	45	0	0	60	0	0	(X)	(X)	(X)	15

Mining machine operators 6840 (SOC 47-5040)	Percent	2.3%	0.2%	0.1%	1.5%	0.2%	0.1%	0.1%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Miscellaneous extraction workers including roof bolters	Total both sexes																
Miscellaneous extraction workers including roof bolters	Number	68 595	9 275	4 195	49 030	3 800	1 180	305	120	20	435	40	10	(X)	(X)	(X)	185
Miscellaneous extraction workers including roof bolters	Percent	100.0%	13.5%	6.1%	71.5%	5.5%	1.7%	0.4%	0.2%	0.0%	0.6%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Miscellaneous extraction workers including roof bolters	Male																
Miscellaneous extraction workers including roof bolters	Number	67 245	9 105	4 055	48 100	3 735	1 150	305	120	0	435	40	10	(X)	(X)	(X)	185
Miscellaneous extraction workers including roof bolters	Percent	98.0%	13.3%	5.9%	70.1%	5.4%	1.7%	0.4%	0.2%	0.0%	0.6%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Miscellaneous extraction workers including roof bolters	Female																
Miscellaneous extraction workers including roof bolters	Number	1 355	170	135	930	65	30	0	0	20	0	0	0	(X)	(X)	(X)	0
Miscellaneous extraction workers including roof bolters	Percent	2.0%	0.2%	0.2%	1.4%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
First-line supervisors of mechanics instalers and	Total both sexes																
First-line supervisors of mechanics instalers and	Number	314 875	18 925	11 375	248 720	23 825	1 590	6 070	535	375	1 655	430	210	(X)	(X)	(X)	1 160
First-line supervisors of mechanics instalers and	Percent	100.0%	6.0%	3.6%	79.0%	7.6%	0.5%	1.9%	0.2%	0.1%	0.5%	0.1%	0.1%	(X)	(X)	(X)	0.4%
First-line supervisors of mechanics instalers and	Male																
First-line supervisors of mechanics instalers and	Number	292 195	17 205	10 100	233 410	20 255	1 540	5 590	475	350	1 550	420	210	(X)	(X)	(X)	1 090
First-line supervisors of mechanics instalers and	Percent	92.8%	5.5%	3.2%	74.1%	6.4%	0.5%	1.8%	0.2%	0.1%	0.5%	0.1%	0.1%	(X)	(X)	(X)	0.3%
First-line supervisors of mechanics instalers and	Female																
First-line supervisors of mechanics instalers and	Number	22 680	1 720	1 275	15 310	3 575	50	480	60	25	105	10	0	(X)	(X)	(X)	70
First-line supervisors of mechanics instalers and	Percent	7.2%	0.5%	0.4%	4.9%	1.1%	0.0%	0.2%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Computer automated teller and office machine repairers	Total both sexes																
Computer automated teller and office machine repairers	Number	287 155	17 810	11 700	201 145	30 870	1 190	18 825	570	545	990	1 330	355	(X)	(X)	(X)	1 830
Computer automated teller and office machine repairers	Percent	100.0%	6.2%	4.1%	70.0%	10.8%	0.4%	6.6%	0.2%	0.2%	0.3%	0.5%	0.1%	(X)	(X)	(X)	0.6%
Computer automated teller and office machine repairers	Male																
Computer automated teller and office machine repairers	Number	251 305	16 015	9 905	177 845	25 150	970	16 610	545	450	865	1 215	265	(X)	(X)	(X)	1 475
Computer automated teller and office machine repairers	Percent	87.5%	5.6%	3.4%	61.9%	8.8%	0.3%	5.8%	0.2%	0.2%	0.3%	0.4%	0.1%	(X)	(X)	(X)	0.5%
Computer, automated teller, and office machine repairers	Female																
Computer automated teller and office machine repairers	Number	35 850	1 795	1 795	23 300	5 720	220	2 215	25	95	125	115	90	(X)	(X)	(X)	355
Computer automated teller and office machine repairers	Percent	12.5%	0.6%	0.6%	8.1%	2.0%	0.1%	0.8%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Radio and telecommunications equipment installers and	Total, both sexes																
Radio and telecommunications equipment installers and	Number	196 005	13 325	9 335	139 285	24 245	795	6 610	195	205	680	530	95	(X)	(X)	(X)	695
Radio and telecommunications equipment installers and	Percent	100.0%	6.8%	4.8%	71.1%	12.4%	0.4%	3.4%	0.1%	0.1%	0.3%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Radio and telecommunications equipment installers and	Male																
Radio and telecommunications equipment installers and	Number	171 990	11 550	8 320	125 420	18 675	675	5 320	115	185	600	495	95	(X)	(X)	(X)	545
Radio and telecommunications equipment installers and	Percent	87.7%	5.9%	4.2%	64.0%	9.5%	0.3%	2.7%	0.1%	0.1%	0.3%	0.3%	0.0%	(X)	(X)	(X)	0.3%
Radio and telecommunications equipment installers and	Female																
Radio and telecommunications equipment installers and	Number	24 010	1 775	1 020	13 865	5 575	120	1 290	80	20	80	40	0	(X)	(X)	(X)	150
Radio and telecommunications equipment installers and	Percent	12.2%	0.9%	0.5%	7.1%	2.8%	0.1%	0.7%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Avionics technicians 7030 (SOC 49-2091)	Total both sexes																
Avionics technicians 7030 (SOC 49-2091)	Number	17 865	1 840	480	13 165	1 345	95	585	35	25	155	30	0	(X)	(X)	(X)	105
Avionics technicians 7030 (SOC 49-2091)	Percent	100.0%	10.3%	2.7%	73.7%	7.5%	0.5%	3.3%	0.2%	0.1%	0.9%	0.2%	0.0%	(X)	(X)	(X)	0.6%
Avionics technicians 7030 (SOC 49-2091)	Male																
Avionics technicians 7030 (SOC 49-2091)	Number	16 370	1 720	390	12 170	1 235	85	475	35	25	110	30	0	(X)	(X)	(X)	105
Avionics technicians 7030 (SOC 49-2091)	Percent	91.6%	9.6%	2.2%	68.1%	6.9%	0.5%	2.7%	0.2%	0.1%	0.6%	0.2%	0.0%	(X)	(X)	(X)	0.6%
Avionics technicians 7030 (SOC 49-2091)	Female																
Avionics technicians 7030 (SOC 49-2091)	Number	1 495	125	90	1 000	115	10	110	0	0	50	0	0	(X)	(X)	(X)	0
Avionics technicians 7030 (SOC 49-2091)	Percent	8.4%	0.7%	0.5%	5.6%	0.6%	0.1%	0.6%	0.0%	0.0%	0.3%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Electric motor power tool and related repairers 7040	Total both sexes																
Electric motor power tool and related repairers 7040	Number	30 330	2 675	1 945	21 895	2 195	270	1 000	50	15	130	105	0	(X)	(X)	(X)	50
Electric motor power tool and related repairers 7040	Percent	100.0%	8.8%	6.4%	72.2%	7.2%	0.9%	3.3%	0.2%	0.0%	0.4%	0.3%	0.0%	(X)	(X)	(X)	0.2%
Electric motor power tool and related repairers 7040	Male																
Electric motor, power tool, and related repairers 7040	Number	28,865	2,410	1,790	21,085	2,005	270	970	50	15	115	105	0	(X)	(X)	(X)	50
Electric motor power tool and related repairers 7040	Percent	95.2%	7.9%	5.9%	69.5%	6.6%	0.9%	3.2%	0.2%	0.0%	0.4%	0.3%	0.0%	(X)	(X)	(X)	0.2%
Electric motor power tool and related repairers 7040	Female																
Electric motor, power tool, and related repairers 7040	Number	1,465	265	155	810	190	0	30	0	0	15	0	0	(X)	(X)	(X)	0
Electric motor power tool and related repairers 7040	Percent	4.8%	0.9%	0.5%	2.7%	0.6%	0.0%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Electrical and electronics repairers transportation	Total both sexes																
Electrical and electronics repairers transportation	Number	17 310	590	410	14 225	1 295	140	440	15	15	115	4	0	(X)	(X)	(X)	65
Electrical and electronics repairers transportation	Percent	100.0%	3.4%	2.4%	82.2%	7.5%	0.8%	2.5%	0.1%	0.1%	0.7%	0.0%	0.0%	(X)	(X)	(X)	0.4%
Electrical and electronics repairers transportation	Male																
Electrical and electronics repairers transportation	Number	16 715	580	400	13 810	1 265	90	390	15	15	90	4	0	(X)	(X)	(X)	65
Electrical and electronics repairers transportation	Percent	96.6%	3.4%	2.3%	79.8%	7.3%	0.5%	2.3%	0.1%	0.1%	0.5%	0.0%	0.0%	(X)	(X)	(X)	0.4%
Electrical and electronics repairers transportation	Female																
Electrical and electronics repairers transportation	Number	595	10	15	415	30	50	50	0	0	30	0	0	(X)	(X)	(X)	0
Electrical and electronics repairers transportation	Percent	3.4%	0.1%	0.1%	2.4%	0.2%	0.3%	0.3%	0.0%	0.0%	0.2%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Electronic equipment installers and repairers motor	Total both sexes																
Electronic equipment installers and repairers motor	Number	20 215	1 785	1 310	14 350	1 810	120	490	20	60	80	45	25	(X)	(X)	(X)	130
Electronic equipment installers and repairers motor	Percent	100.0%	8.8%	6.5%	71.0%	9.0%	0.6%	2.4%	0.1%	0.3%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.6%
Electronic equipment installers and repairers motor	Male																
Electronic equipment installers and repairers motor	Number	18 880	1 720	1 230	13 570	1 540	115	450	20	60	55	30	0	(X)	(X)	(X)	95
Electronic equipment installers and repairers motor	Percent	93.4%	8.5%	6.1%	67.1%	7.6%	0.6%	2.2%	0.1%	0.3%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.5%
Electronic equipment installers and repairers motor	Female																
Electronic equipment installers and repairers motor	Number	1 335	65	85	775	270	4	40	0	0	25	10	25	(X)	(X)	(X)	35
Electronic equipment installers and repairers motor	Percent	6.6%	0.3%	0.4%	3.8%	1.3%	0.0%	0.2%	0.0%	0.0%	0.1%	0.0%	0.1%	(X)	(X)	(X)	0.2%
Electronic home entertainment equipment installers and	Total both sexes																
Electronic home entertainment equipment installers and	Number	64 255	6 165	4 615	43 540	6 000	320	2 555	80	105	410	170	25	(X)	(X)	(X)	275
Electronic home entertainment equipment installers and	Percent	100.0%	9.6%	7.2%	67.8%	9.3%	0.5%	4.0%	0.1%	0.2%	0.6%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Electronic home entertainment equipment installers and	Male																
Electronic home entertainment equipment installers and	Number	62 115	6 060	4 295	42 310	5 710	250	2 450	80	105	390	170	25	(X)	(X)	(X)	275
Electronic home entertainment equipment installers and	Percent	96.7%	9.4%	6.7%	65.8%	8.9%	0.4%	3.8%	0.1%	0.2%	0.6%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Electronic home entertainment equipment installers and	Female																
Electronic home entertainment equipment installers and	Number	2 140	110	315	1 230	290	70	100	0	0	20	0	0	(X)	(X)	(X)	0
Electronic home entertainment equipment installers and	Percent	3.3%	0.2%	0.5%	1.9%	0.5%	0.1%	0.2%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Security and fire alarm systems installers 7130 (SOC 49-	Total both sexes																
Security and fire alarm systems installers 7130 (SOC 49-	Number	60 470	6 410	3 620	42 325	5 050	315	1 505	165	270	320	190	15	(X)	(X)	(X)	285
Security and fire alarm systems installers 7130 (SOC 49-	Percent	100.0%	10.6%	6.0%	70.0%	8.4%	0.5%	2.5%	0.3%	0.4%	0.5%	0.3%	0.0%	(X)	(X)	(X)	0.5%
Security and fire alarm systems installers 7130 (SOC 49-	Male																
Security and fire alarm systems installers 7130 (SOC 49-	Number	58 815	6 300	3 545	41 180	4 780	300	1 485	165	250	320	190	15	(X)	(X)	(X)	275
Security and fire alarm systems installers 7130 (SOC 49-	Percent	97.3%	10.4%	5.9%	68.1%	7.9%	0.5%	2.5%	0.3%	0.4%	0.5%	0.3%	0.0%	(X)	(X)	(X)	0.5%
Security and fire alarm systems installers 7130 (SOC 49-	Female																
Security and fire alarm systems installers 7130 (SOC 49-	Number	1 660	115	70	1 145	265	15	20	0	20	0	0	0	(X)	(X)	(X)	10
Security and fire alarm systems installers 7130 (SOC 49-	Percent	2.7%	0.2%	0.1%	1.9%	0.4%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Aircraft mechanics and service technicians 7140 (SOC 49-	Total both sexes																
Aircraft mechanics and service technicians 7140 (SOC 49-	Number	156 600	13 515	6 710	112 285	12 630	860	7 070	680	260	995	510	110	(X)	(X)	(X)	980
Aircraft mechanics and service technicians 7140 (SOC 49-	Percent	100.0%	8.6%	4.3%	71.7%	8.1%	0.5%	4.5%	0.4%	0.2%	0.6%	0.3%	0.1%	(X)	(X)	(X)	0.6%
Aircraft mechanics and service technicians 7140 (SOC 49-	Male																
Aircraft mechanics and service technicians 7140 (SOC 49-	Number	149 245	12 905	6 430	107 305	11 855	740	6 615	650	260	915	510	110	(X)	(X)	(X)	945
Aircraft mechanics and service technicians 7140 (SOC 49-	Percent	95.3%	8.2%	4.1%	68.5%	7.6%	0.5%	4.2%	0.4%	0.2%	0.6%	0.3%	0.1%	(X)	(X)	(X)	0.6%
Aircraft mechanics and service technicians 7140 (SOC 49-	Female																
Aircraft mechanics and service technicians 7140 (SOC 49-	Number	7 355	610	280	4 980	770	115	455	30	0	75	0	0	(X)	(X)	(X)	35
Aircraft mechanics and service technicians 7140 (SOC 49-	Percent	4.7%	0.4%	0.2%	3.2%	0.5%	0.1%	0.3%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Automotive body and related repairers 7150 (SOC 49-	Total, both sexes																
Automotive body and related repairers 7150 (SOC 49-	Number	171 190	23 040	15 535	116 030	9 320	1 080	4 125	75	95	880	230	25	(X)	(X)	(X)	760
Automotive body and related repairers 7150 (SOC 49-	Percent	100.0%	13.5%	9.1%	67.8%	5.4%	0.6%	2.4%	0.0%	0.1%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.4%
Automotive body and related repairers 7150 (SOC 49-	Male																
Automotive body and related repairers 7150 (SOC 49-	Number	168 200	22 765	15 300	113 885	9 075	1 060	4 070	75	95	875	230	25	(X)	(X)	(X)	735
Automotive body and related repairers 7150 (SOC 49-	Percent	98.3%	13.3%	8.9%	66.5%	5.3%	0.6%	2.4%	0.0%	0.1%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.4%
Automotive body and related repairers 7150 (SOC 49-	Female																
Automotive body and related repairers 7150 (SOC 49-	Number	2 990	275	230	2 140	240	20	50	0	0	4	0	0	(X)	(X)	(X)	25
Automotive body and related repairers 7150 (SOC 49-	Percent	1.7%	0.2%	0.1%	1.3%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Automotive glass installers and repairers 7160 (SOC 49-	Total both sexes																
Automotive glass installers and repairers 7160 (SOC 49-	Number	20 510	2 680	1 790	14 400	940	75	320	0	40	100	0	0	(X)	(X)	(X)	160
Automotive glass installers and repairers 7160 (SOC 49-	Percent	100.0%	13.1%	8.7%	70.2%	4.6%	0.4%	1.6%	0.0%	0.2%	0.5%	0.0%	0.0%	(X)	(X)	(X)	0.8%
Automotive glass installers and repairers 7160 (SOC 49-	Male																
Automotive glass installers and repairers 7160 (SOC 49-	Number	19 830	2 600	1 740	13 980	895	45	285	0	40	90	0	0	(X)	(X)	(X)	160
Automotive glass installers and repairers 7160 (SOC 49-	Percent	96.7%	12.7%	8.5%	68.2%	4.4%	0.2%	1.4%	0.0%	0.2%	0.4%	0.0%	0.0%	(X)	(X)	(X)	0.8%
Automotive glass installers and repairers 7160 (SOC 49-	Female																
Automotive glass installers and repairers 7160 (SOC 49-	Number	675	85	55	420	45	30	35	0	0	10	0	0	(X)	(X)	(X)	0
Automotive glass installers and repairers 7160 (SOC 49-	Percent	3.3%	0.4%	0.3%	2.0%	0.2%	0.1%	0.2%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Automotive service technicians and mechanics 7200 (SOC	Total both sexes																
Automotive service technicians and mechanics 7200 (SOC	Number	884 675	96 000	72 070	601 520	65 860	5 195	30 175	1 415	1 045	3 970	2 010	340	(X)	(X)	(X)	5 070
Automotive service technicians and mechanics 7200 (SOC	Percent	100.0%	10.9%	8.1%	68.0%	7.4%	0.6%	3.4%	0.2%	0.1%	0.4%	0.2%	0.0%	(X)	(X)	(X)	0.6%
Automotive service technicians and mechanics 7200 (SOC	Male																
Automotive service technicians and mechanics 7200 (SOC	Number	871 350	94 635	71 295	592 700	64 265	5 140	29 670	1 415	1 025	3 910	1 955	340	(X)	(X)	(X)	4 995
Automotive service technicians and mechanics 7200 (SOC	Percent	98.5%	10.7%	8.1%	67.0%	7.3%	0.6%	3.4%	0.2%	0.1%	0.4%	0.2%	0.0%	(X)	(X)	(X)	0.6%
Automotive service technicians and mechanics 7200 (SOC	Female																
Automotive service technicians and mechanics 7200 (SOC	Number	13,325	1,365	775	8,820	1,595	55	505	0	20	60	50	0	(X)	(X)	(X)	75
Automotive service technicians and mechanics 7200 (SOC	Percent	1.5%	0.2%	0.1%	1.0%	0.2%	0.0%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Bus and truck mechanics and diesel engine specialists	Total both sexes																
Bus and truck mechanics and diesel engine specialists	Number	312,055	23,950	15,860	236,955	23,805	1,950	5,155	615	280	1,655	410	60	(X)	(X)	(X)	1,365
Bus and truck mechanics and diesel engine specialists	Percent	100.0%	7.7%	5.1%	75.9%	7.6%	0.6%	1.7%	0.2%	0.1%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.4%
Bus and truck mechanics and diesel engine specialists	Male																
Bus and truck mechanics and diesel engine specialists	Number	308 555	23 590	15 715	234 745	23 245	1 880	5 110	615	280	1 635	410	60	(X)	(X)	(X)	1 275
Bus and truck mechanics and diesel engine specialists	Percent	98.9%	7.6%	5.0%	75.2%	7.4%	0.6%	1.6%	0.2%	0.1%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.4%
Bus and truck mechanics and diesel engine specialists	Female																
Bus and truck mechanics and diesel engine specialists	Number	3 500	360	145	2 210	560	70	45	0	0	25	0	0	(X)	(X)	(X)	90
Bus and truck mechanics and diesel engine specialists	Percent	1.1%	0.1%	0.0%	0.7%	0.2%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Heavy vehicle and mobile equipment service technicians	Total both sexes																
Heavy vehicle and mobile equipment service technicians	Number	220 610	16 955	11 195	175 180	10 675	1 820	2 220	350	115	1 225	250	60	(X)	(X)	(X)	565

Heavy vehicle and mobile equipment service technicians	Percent	100.0%	7.7%	5.1%	79.4%	4.8%	0.8%	1.0%	0.2%	0.1%	0.6%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Heavy vehicle and mobile equipment service technicians	Male																
Heavy vehicle and mobile equipment service technicians	Number	217 940	16 790	11 060	173 215	10 345	1 790	2 175	350	115	1 225	250	60	(X)	(X)	(X)	565
Heavy vehicle and mobile equipment service technicians	Percent	98.8%	7.6%	5.0%	78.5%	4.7%	0.8%	1.0%	0.2%	0.1%	0.6%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Heavy vehicle and mobile equipment service technicians	Female																
Heavy vehicle and mobile equipment service technicians	Number	2 665	165	135	1 965	330	30	45	0	0	0	0	0	(X)	(X)	(X)	0
Heavy vehicle and mobile equipment service technicians	Percent	1.2%	0.1%	0.1%	0.9%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Small engine mechanics 7240 (SOC 49-3050)	Total, both sexes																
Small engine mechanics 7240 (SOC 49-3050)	Number	52 710	2 355	1 885	45 115	1 825	280	540	65	35	315	100	0	(X)	(X)	(X)	200
Small engine mechanics 7240 (SOC 49-3050)	Percent	100.0%	4.5%	3.6%	85.6%	3.5%	0.5%	1.0%	0.1%	0.1%	0.6%	0.2%	0.0%	(X)	(X)	(X)	0.4%
Small engine mechanics 7240 (SOC 49-3050)	Male																
Small engine mechanics 7240 (SOC 49-3050)	Number	51 895	2 295	1 845	44 450	1 805	265	540	65	30	315	100	0	(X)	(X)	(X)	185
Small engine mechanics 7240 (SOC 49-3050)	Percent	98.5%	4.4%	3.5%	84.3%	3.4%	0.5%	1.0%	0.1%	0.1%	0.6%	0.2%	0.0%	(X)	(X)	(X)	0.4%
Small engine mechanics 7240 (SOC 49-3050)	Female																
Small engine mechanics 7240 (SOC 49-3050)	Number	815	60	45	665	15	15	0	0	4	0	0	0	(X)	(X)	(X)	15
Small engine mechanics 7240 (SOC 49-3050)	Percent	1.5%	0.1%	0.1%	1.3%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Miscellaneous vehicle and mobile equipment mechanics	Total, both sexes																
Miscellaneous vehicle and mobile equipment mechanics	Number	88 705	11 820	8 225	56 745	8 630	675	1 200	100	285	425	200	45	(X)	(X)	(X)	345
Miscellaneous vehicle and mobile equipment mechanics	Percent	100.0%	13.3%	9.3%	64.0%	9.7%	0.8%	1.4%	0.1%	0.3%	0.5%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Miscellaneous vehicle and mobile equipment mechanics	Male																
Miscellaneous vehicle and mobile equipment mechanics	Number	87 075	11 770	8 135	55 730	8 290	665	1 145	100	285	395	200	45	(X)	(X)	(X)	305
Miscellaneous vehicle and mobile equipment mechanics	Percent	98.2%	13.3%	9.2%	62.8%	9.3%	0.7%	1.3%	0.1%	0.3%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.3%
Miscellaneous vehicle and mobile equipment mechanics	Female																
Miscellaneous vehicle and mobile equipment mechanics	Number	1 630	50	90	1 015	340	10	60	0	0	25	0	0	(X)	(X)	(X)	40
Miscellaneous vehicle and mobile equipment mechanics	Percent	1.8%	0.1%	0.1%	1.1%	0.4%	0.0%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Control and valve installers and repairers 7300 (SOC 49-	Total, both sexes																
Control and valve installers and repairers 7300 (SOC 49-	Number	21 835	1 660	1 145	15 945	2 440	115	235	15	30	105	20	50	(X)	(X)	(X)	75
Control and valve installers and repairers 7300 (SOC 49-	Percent	100.0%	7.6%	5.2%	73.0%	11.2%	0.5%	1.1%	0.1%	0.1%	0.5%	0.1%	0.2%	(X)	(X)	(X)	0.3%
Control and valve installers and repairers 7300 (SOC 49-	Male																
Control and valve installers and repairers 7300 (SOC 49-	Number	20 805	1 650	1 115	15 135	2 285	115	225	15	30	90	20	50	(X)	(X)	(X)	75
Control and valve installers and repairers 7300 (SOC 49-	Percent	95.3%	7.6%	5.1%	69.3%	10.5%	0.5%	1.0%	0.1%	0.1%	0.4%	0.1%	0.2%	(X)	(X)	(X)	0.3%
Control and valve installers and repairers 7300 (SOC 49-	Female																
Control and valve installers and repairers 7300 (SOC 49-	Number	1 035	10	30	805	155	0	15	0	0	15	0	0	(X)	(X)	(X)	0
Control and valve installers and repairers 7300 (SOC 49-	Percent	4.7%	0.0%	0.1%	3.7%	0.7%	0.0%	0.1%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Heating air conditioning and refrigeration mechanics and	Total both sexes																
Heating air conditioning and refrigeration mechanics and	Number	377 555	35 675	22 495	281 645	23 980	1 975	6 680	245	850	1 830	690	125	(X)	(X)	(X)	1 365
Heating air conditioning and refrigeration mechanics and	Percent	100.0%	9.4%	6.0%	74.6%	6.4%	0.5%	1.8%	0.1%	0.2%	0.5%	0.2%	0.0%	(X)	(X)	(X)	0.4%
Heating air conditioning and refrigeration mechanics and	Male																
Heating air conditioning and refrigeration mechanics and	Number	372 705	35 235	22 200	278 255	23 510	1 960	6 545	220	850	1 760	690	115	(X)	(X)	(X)	1 360
Heating air conditioning and refrigeration mechanics and	Percent	98.7%	9.3%	5.9%	73.7%	6.2%	0.5%	1.7%	0.1%	0.2%	0.5%	0.2%	0.0%	(X)	(X)	(X)	0.4%
Heating air conditioning and refrigeration mechanics and	Female																
Heating air conditioning and refrigeration mechanics and	Number	4 855	435	295	3 390	470	15	140	25	0	70	0	10	(X)	(X)	(X)	4
Heating air conditioning and refrigeration mechanics and	Percent	1.3%	0.1%	0.1%	0.9%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Home appliance repairers 7320 (SOC 49-9031)	Total both sexes																
Home appliance repairers 7320 (SOC 49-9031)	Number	44 385	4 110	2 550	31 910	3 630	310	1 300	35	100	285	45	25	(X)	(X)	(X)	85
Home appliance repairers 7320 (SOC 49-9031)	Percent	100.0%	9.3%	5.7%	71.9%	8.2%	0.7%	2.9%	0.1%	0.2%	0.6%	0.1%	0.1%	(X)	(X)	(X)	0.2%
Home appliance repairers 7320 (SOC 49-9031)	Male																
Home appliance repairers 7320 (SOC 49-9031)	Number	42 925	3 975	2 465	30 930	3 415	310	1 285	25	90	285	45	25	(X)	(X)	(X)	75
Home appliance repairers 7320 (SOC 49-9031)	Percent	96.7%	9.0%	5.6%	69.7%	7.7%	0.7%	2.9%	0.1%	0.2%	0.6%	0.1%	0.1%	(X)	(X)	(X)	0.2%
Home appliance repairers 7320 (SOC 49-9031)	Female																
Home appliance repairers 7320 (SOC 49-9031)	Number	1,460	140	85	980	215	0	10	4	15	0	0	0	(X)	(X)	(X)	10
Home appliance repairers 7320 (SOC 49-9031)	Percent	3.3%	0.3%	0.2%	2.2%	0.5%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Industrial and refractory machinery mechanics 7330 (SOC	Total both sexes																
Industrial and refractory machinery mechanics 7330 (SOC	Number	421,245	30,735	21,310	320,685	30,730	2,205	10,550	450	500	2,035	615	200	(X)	(X)	(X)	1,235
Industrial and refractory machinery mechanics 7330 (SOC	Percent	100.0%	7.3%	5.1%	76.1%	7.3%	0.5%	2.5%	0.1%	0.1%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Industrial and refractory machinery mechanics 7330 (SOC	Male																
Industrial and refractory machinery mechanics 7330 (SOC	Number	406 155	29 365	20 450	311 180	28 710	2 000	9 795	365	440	1 935	580	200	(X)	(X)	(X)	1 135
Industrial and refractory machinery mechanics 7330 (SOC	Percent	96.4%	7.0%	4.9%	73.9%	6.8%	0.5%	2.3%	0.1%	0.1%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Industrial and refractory machinery mechanics 7330 (SOC	Female																
Industrial and refractory machinery mechanics 7330 (SOC	Number	15 095	1 370	860	9 510	2 020	200	760	85	60	95	35	0	(X)	(X)	(X)	100
Industrial and refractory machinery mechanics 7330 (SOC	Percent	3.6%	0.3%	0.2%	2.3%	0.5%	0.0%	0.2%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Maintenance and repair workers general 7340 (SOC 49-	Total both sexes																
Maintenance and repair workers general 7340 (SOC 49-	Number	497 610	43 670	31 665	350 925	47 375	4 065	12 975	1 245	440	1 995	890	255	(X)	(X)	(X)	2 110
Maintenance and repair workers general 7340 (SOC 49-	Percent	100.0%	8.8%	6.4%	70.5%	9.5%	0.8%	2.6%	0.3%	0.1%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Maintenance and repair workers general 7340 (SOC 49-	Male																
Maintenance and repair workers general 7340 (SOC 49-	Number	480 145	42 620	30 885	339 515	44 395	3 795	12 265	1 215	440	1 930	815	240	(X)	(X)	(X)	2 030
Maintenance and repair workers general 7340 (SOC 49-	Percent	96.5%	8.6%	6.2%	68.2%	8.9%	0.8%	2.5%	0.2%	0.1%	0.4%	0.2%	0.0%	(X)	(X)	(X)	0.4%
Maintenance and repair workers general 7340 (SOC 49-	Female																
Maintenance and repair workers general 7340 (SOC 49-	Number	17 465	1 055	785	11 405	2 980	270	710	30	0	65	75	15	(X)	(X)	(X)	80
Maintenance and repair workers general 7340 (SOC 49-	Percent	3.5%	0.2%	0.2%	2.3%	0.6%	0.1%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Maintenance workers machinery 7350 (SOC 49-9043)	Total both sexes																
Maintenance workers machinery 7350 (SOC 49-9043)	Number	38 810	2 905	2 260	28 945	3 120	290	810	85	20	200	20	4	(X)	(X)	(X)	145
Maintenance workers machinery 7350 (SOC 49-9043)	Percent	100.0%	7.5%	5.8%	74.6%	8.0%	0.7%	2.1%	0.2%	0.1%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.4%
Maintenance workers machinery 7350 (SOC 49-9043)	Male																
Maintenance workers machinery 7350 (SOC 49-9043)	Number	37 230	2 695	2 010	28 130	2 850	290	790	85	20	195	20	4	(X)	(X)	(X)	145
Maintenance workers, machinery 7350 (SOC 49-9043)	Percent	95.9%	6.9%	5.2%	72.5%	7.3%	0.7%	2.0%	0.2%	0.1%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.4%
Maintenance workers machinery 7350 (SOC 49-9043)	Female																
Maintenance workers machinery 7350 (SOC 49-9043)	Number	1 580	210	255	815	275	0	25	0	0	4	0	0	(X)	(X)	(X)	0
Maintenance workers, machinery 7350 (SOC 49-9043)	Percent	4.1%	0.5%	0.7%	2.1%	0.7%	0.0%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Mi lwrights 7360 (SOC 49-9044)	Total both sexes																
Mi lwrights 7360 (SOC 49-9044)	Number	58 295	1 510	1 125	51 940	2 315	375	470	45	60	290	75	10	(X)	(X)	(X)	85
Mi lwrights 7360 (SOC 49-9044)	Percent	100.0%	2.6%	1.9%	89.1%	4.0%	0.6%	0.8%	0.1%	0.1%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Mi lwrights 7360 (SOC 49-9044)	Male																
Mi lwrights 7360 (SOC 49-9044)	Number	56 665	1 375	1 115	50 765	2 150	375	375	15	60	290	75	10	(X)	(X)	(X)	60
Mi lwrights 7360 (SOC 49-9044)	Percent	97.2%	2.4%	1.9%	87.1%	3.7%	0.6%	0.6%	0.0%	0.1%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Mi lwrights 7360 (SOC 49-9044)	Female																
Mi lwrights 7360 (SOC 49-9044)	Number	1 630	135	10	1 175	165	0	95	30	0	4	0	0	(X)	(X)	(X)	20
Mi lwrights 7360 (SOC 49-9044)	Percent	2.8%	0.2%	0.0%	2.0%	0.3%	0.0%	0.2%	0.1%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Electrical power-line installers and repairers 7410 (SOC 49-	Total both sexes																
Electrical power-line installers and repairers 7410 (SOC 49-	Number	119 210	7 400	5 090	93 575	9 750	800	905	170	145	640	280	70	(X)	(X)	(X)	390
Electrical power-line installers and repairers 7410 (SOC 49-	Percent	100.0%	6.2%	4.3%	78.5%	8.2%	0.7%	0.8%	0.1%	0.1%	0.5%	0.2%	0.1%	(X)	(X)	(X)	0.3%
Electrical power-line installers and repairers 7410 (SOC 49-	Male																
Electrical power-line installers and repairers 7410 (SOC 49-	Number	117 480	7 280	4 975	92 360	9 645	745	855	155	145	605	270	70	(X)	(X)	(X)	380
Electrical power-line installers and repairers 7410 (SOC 49-	Percent	98.5%	6.1%	4.2%	77.5%	8.1%	0.6%	0.7%	0.1%	0.1%	0.5%	0.2%	0.1%	(X)	(X)	(X)	0.3%
Electrical power-line installers and repairers 7410 (SOC 49-	Female																
Electrical power-line installers and repairers 7410 (SOC 49-	Number	1 730	120	115	1 220	105	55	50	15	0	30	10	0	(X)	(X)	(X)	10
Electrical power-line installers and repairers 7410 (SOC 49-	Percent	1.5%	0.1%	0.1%	1.0%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Telecommunications line installers and repairers 7420	Total both sexes																
Telecommunications line installers and repairers 7420	Number	174 590	15 215	10 720	116 070	23 740	795	4 885	410	330	860	450	225	(X)	(X)	(X)	895
Telecommunications line installers and repairers 7420	Percent	100.0%	8.7%	6.1%	66.5%	13.6%	0.5%	2.8%	0.2%	0.2%	0.5%	0.3%	0.1%	(X)	(X)	(X)	0.5%
Telecommunications line installers and repairers 7420	Male																
Telecommunications line installers and repairers 7420	Number	164 460	14 590	10 040	109 985	21 735	705	4 500	395	255	860	350	190	(X)	(X)	(X)	850
Telecommunications line installers and repairers 7420	Percent	94.2%	8.4%	5.8%	63.0%	12.4%	0.4%	2.6%	0.2%	0.1%	0.5%	0.2%	0.1%	(X)	(X)	(X)	0.5%
Telecommunications line installers and repairers 7420	Female																
Telecommunications line installers and repairers 7420	Number	10 130	625	680	6 085	2 005	85	385	10	75	0	100	35	(X)	(X)	(X)	45
Telecommunications line installers and repairers 7420	Percent	5.8%	0.4%	0.4%	3.5%	1.1%	0.0%	0.2%	0.0%	0.0%	0.0%	0.1%	0.0%	(X)	(X)	(X)	0.0%
Precision instrument and equipment repairers 7430 (SOC	Total both sexes																
Precision instrument and equipment repairers 7430 (SOC	Number	64 940	3 805	2 785	49 505	4 195	195	3 345	90	135	265	75	80	(X)	(X)	(X)	460
Precision instrument and equipment repairers 7430 (SOC	Percent	100.0%	5.9%	4.3%	76.2%	6.5%	0.3%	5.2%	0.1%	0.2%	0.4%	0.1%	0.1%	(X)	(X)	(X)	0.7%
Precision instrument and equipment repairers 7430 (SOC	Male																
Precision instrument and equipment repairers 7430 (SOC	Number	57 580	3 420	2 310	45 255	2 730	170	2 685	90	135	240	55	80	(X)	(X)	(X)	415
Precision instrument and equipment repairers 7430 (SOC	Percent	88.7%	5.3%	3.6%	69.7%	4.2%	0.3%	4.1%	0.1%	0.2%	0.4%	0.1%	0.1%	(X)	(X)	(X)	0.6%
Precision instrument and equipment repairers 7430 (SOC	Female																
Precision instrument and equipment repairers 7430 (SOC	Number	7 360	385	475	4 250	1 465	25	665	0	0	25	20	0	(X)	(X)	(X)	45
Precision instrument and equipment repairers 7430 (SOC	Percent	11.3%	0.6%	0.7%	6.5%	2.3%	0.0%	1.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Coin vending and amusement machine servicers and	Total both sexes																
Coin vending and amusement machine servicers and	Number	50 185	3 410	2 540	37 095	4 205	795	1 395	45	100	300	75	25	(X)	(X)	(X)	200
Coin vending and amusement machine servicers and	Percent	100.0%	6.8%	5.1%	73.9%	8.4%	1.6%	2.8%	0.1%	0.2%	0.6%	0.1%	0.0%	(X)	(X)	(X)	0.4%
Coin vending and amusement machine servicers and	Male																
Coin vending and amusement machine servicers and	Number	41 045	2 895	2 305	30 050	3 385	525	1 255	35	40	270	55	25	(X)	(X)	(X)	200
Coin vending and amusement machine servicers and	Percent	81.8%	5.8%	4.6%	59.9%	6.7%	1.0%	2.5%	0.1%	0.1%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.4%
Coin vending and amusement machine servicers and	Female																
Coin vending and amusement machine servicers and	Number	9 140	515	240	7 045	820	270	135	4	55	30	20	0	(X)	(X)	(X)	0
Coin vending and amusement machine servicers and	Percent	18.2%	1.0%	0.5%	14.0%	1.6%	0.5%	0.3%	0.0%	0.1%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Locksmiths and safe repairers 7540 (SOC 49-9094)	Total both sexes																
Locksmiths and safe repairers 7540 (SOC 49-9094)	Number	27,630	1,855	1,075	21,935	1,605	145	455	0	0	220	130	10	(X)	(X)	(X)	200
Locksmiths and safe repairers 7540 (SOC 49-9094)	Percent	100.0%	6.7%	3.9%	79.4%	5.8%	0.5%	1.6%	0.0%	0.0%	0.8%	0.5%	0.0%	(X)	(X)	(X)	0.7%
Locksmiths and safe repairers 7540 (SOC 49-9094)	Male																
Locksmiths and safe repairers 7540 (SOC 49-9094)	Number	25,805	1,760	985	20,640	1,340	145	410	0	0	220	95	10	(X)	(X)	(X)	200
Locksmiths and safe repairers 7540 (SOC 49-9094)	Percent	93.4%	6.4%	3.6%	74.7%	4.8%	0.5%	1.5%	0.0%	0.0%	0.8%	0.3%	0.0%	(X)	(X)	(X)	0.7%
Locksmiths and safe repairers 7540 (SOC 49-9094)	Female																
Locksmiths and safe repairers 7540 (SOC 49-9094)	Number	1 825	95	90	1 295	265	0	45	0	0	0	35	0	(X)	(X)	(X)	0
Locksmiths and safe repairers 7540 (SOC 49-9094)	Percent	6.6%	0.3%	0.3%	4.7%	1.0%	0.0%	0.2%	0.0%	0.0%	0.0%	0.1%	0.0%	(X)	(X)	(X)	0.0%
Manufactured building and mobile home installers 7550	Total both sexes																
Manufactured building and mobile home installers 7550	Number	10 925	1 065	660	8 060	820	110	70	4	35	80	4	0	(X)	(X)	(X)	15
Manufactured building and mobile home installers 7550	Percent	100.0%	9.7%	6.0%	73.8%	7.5%	1.0%	0.6%	0.0%	0.3%	0.7%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Manufactured building and mobile home installers 7550	Male																
Manufactured building and mobile home installers 7550	Number	10 235	1 015	630	7 645	650	100	50	4	35	80	4	0	(X)	(X)	(X)	15

Manufactured building and mobile home installers 7550	Percent	93.7%	9.3%	5.8%	70.0%	5.9%	0.9%	0.5%	0.0%	0.3%	0.7%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Manufactured building and mobile home installers 7550	Female																
Manufactured building and mobile home installers 7550	Number	690	45	30	415	170	4	20	0	0	0	0	0	(X)	(X)	(X)	0
Manufactured building and mobile home installers 7550	Percent	6.3%	0.4%	0.3%	3.8%	1.6%	0.0%	0.2%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Riggers 7560 (SOC 49-9096)	Total, both sexes																
Riggers 7560 (SOC 49-9096)	Number	13 050	970	640	9 110	1 795	50	140	40	0	50	55	0	(X)	(X)	(X)	190
Riggers 7560 (SOC 49-9096)	Percent	100.0%	7.4%	4.9%	69.8%	13.8%	0.4%	1.1%	0.3%	0.0%	0.4%	0.4%	0.0%	(X)	(X)	(X)	1.5%
Riggers 7560 (SOC 49-9096)	Male																
Riggers 7560 (SOC 49-9096)	Number	12 780	970	610	8 955	1 745	50	125	40	0	50	55	0	(X)	(X)	(X)	180
Riggers 7560 (SOC 49-9096)	Percent	97.9%	7.4%	4.7%	68.6%	13.4%	0.4%	1.0%	0.3%	0.0%	0.4%	0.4%	0.0%	(X)	(X)	(X)	1.4%
Riggers 7560 (SOC 49-9096)	Female																
Riggers 7560 (SOC 49-9096)	Number	270	0	30	155	55	0	15	0	0	0	0	0	(X)	(X)	(X)	15
Riggers 7560 (SOC 49-9096)	Percent	2.1%	0.0%	0.2%	1.2%	0.4%	0.0%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Helpers--installation maintenance and repair workers	Total, both sexes																
Helpers--installation maintenance and repair workers	Number	28 345	5 355	4 310	14 330	2 705	175	985	65	80	185	60	20	(X)	(X)	(X)	80
Helpers--installation maintenance and repair workers	Percent	100.0%	18.9%	15.2%	50.6%	9.5%	0.6%	3.5%	0.2%	0.3%	0.7%	0.2%	0.1%	(X)	(X)	(X)	0.3%
Helpers--installation maintenance and repair workers	Male																
Helpers--installation maintenance and repair workers	Number	26 225	5 175	4 070	13 015	2 500	175	805	65	80	185	60	20	(X)	(X)	(X)	80
Helpers--installation maintenance and repair workers	Percent	92.5%	18.3%	14.4%	45.9%	8.8%	0.6%	2.8%	0.2%	0.3%	0.7%	0.2%	0.1%	(X)	(X)	(X)	0.3%
Helpers--installation maintenance and repair workers	Female																
Helpers--installation maintenance and repair workers	Number	2 120	180	240	1 315	210	0	180	0	0	0	0	0	(X)	(X)	(X)	0
Helpers--installation maintenance and repair workers	Percent	7.5%	0.6%	0.8%	4.6%	0.7%	0.0%	0.6%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Other installation maintenance and repair workers	Total, both sexes																
Other installation maintenance and repair workers	Number	238 015	24 085	15 860	169 160	17 425	1 615	5 985	345	340	1 355	510	50	(X)	(X)	(X)	1 285
Other installation maintenance and repair workers	Percent	100.0%	10.1%	6.7%	71.1%	7.3%	0.7%	2.5%	0.1%	0.1%	0.6%	0.2%	0.0%	(X)	(X)	(X)	0.5%
Other installation, maintenance, and repair workers,	Male																
Other installation maintenance and repair workers	Number	223 680	23 110	15 160	159 150	15 840	1 505	5 435	270	330	1 280	500	50	(X)	(X)	(X)	1 045
Other installation maintenance and repair workers	Percent	94.0%	9.7%	6.4%	66.9%	6.7%	0.6%	2.3%	0.1%	0.1%	0.5%	0.2%	0.0%	(X)	(X)	(X)	0.4%
Other installation, maintenance, and repair workers,	Female																
Other installation maintenance and repair workers	Number	14 335	980	700	10 010	1 585	110	550	75	10	75	10	0	(X)	(X)	(X)	240
Other installation maintenance and repair workers	Percent	6.0%	0.4%	0.3%	4.2%	0.7%	0.0%	0.2%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.1%
First-line supervisors of production and operating workers	Total, both sexes																
First-line supervisors of production and operating workers	Number	996 450	75 900	61 235	716 370	92 410	4 220	34 970	1 100	1 095	3 640	1 630	650	(X)	(X)	(X)	3 230
First-line supervisors of production and operating workers	Percent	100.0%	7.6%	6.1%	71.9%	9.3%	0.4%	3.5%	0.1%	0.1%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.3%
First-line supervisors of production and operating workers	Male																
First-line supervisors of production and operating workers	Number	804 615	58 930	46 695	594 595	67 880	3 220	24 675	845	800	2 920	1 205	485	(X)	(X)	(X)	2 360
First-line supervisors of production and operating workers	Percent	80.7%	5.9%	4.7%	59.7%	6.8%	0.3%	2.5%	0.1%	0.1%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.2%
First-line supervisors of production and operating workers	Female																
First-line supervisors of production and operating workers	Number	191 835	16 970	14 540	121 775	24 530	995	10 295	260	295	720	425	160	(X)	(X)	(X)	870
First-line supervisors of production and operating workers	Percent	19.3%	1.7%	1.5%	12.2%	2.5%	0.1%	1.0%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Aircraft structure surfaces rigging and systems	Total, both sexes																
Aircraft structure surfaces rigging and systems	Number	11 320	1 630	1 205	6 155	1 215	110	875	0	55	40	15	0	(X)	(X)	(X)	20
Aircraft structure surfaces rigging and systems	Percent	100.0%	14.4%	10.6%	54.4%	10.7%	1.0%	7.7%	0.0%	0.5%	0.4%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Aircraft structure surfaces rigging and systems	Male																
Aircraft structure surfaces rigging and systems	Number	7 355	835	650	4 550	645	40	560	0	30	30	0	0	(X)	(X)	(X)	20
Aircraft structure surfaces rigging and systems	Percent	65.0%	7.4%	5.7%	40.2%	5.7%	0.4%	4.9%	0.0%	0.3%	0.3%	0.0%	0.0%	(X)	(X)	(X)	0.2%
Aircraft structure surfaces rigging and systems	Female																
Aircraft structure surfaces rigging and systems	Number	3 965	800	560	1 600	570	70	315	0	25	10	15	0	(X)	(X)	(X)	0
Aircraft structure surfaces rigging and systems	Percent	35.0%	7.1%	4.9%	14.1%	5.0%	0.6%	2.8%	0.0%	0.2%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.0%
Electrical electronics and electromechanical assemblers	Total, both sexes																
Electrical, electronics, and electromechanical assemblers	Number	192,270	20,800	16,780	92,435	25,120	1,215	33,585	265	350	590	370	60	(X)	(X)	(X)	710
Electrical electronics and electromechanical assemblers	Percent	100.0%	10.8%	8.7%	48.1%	13.1%	0.6%	17.5%	0.1%	0.2%	0.3%	0.2%	0.0%	(X)	(X)	(X)	0.4%
Electrical electronics and electromechanical assemblers	Male																
Electrical, electronics, and electromechanical assemblers	Number	86,110	8,230	6,470	46,155	10,865	585	12,605	130	215	320	175	30	(X)	(X)	(X)	325
Electrical electronics and electromechanical assemblers	Percent	44.8%	4.3%	3.4%	24.0%	5.7%	0.3%	6.6%	0.1%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Electrical electronics and electromechanical assemblers	Female																
Electrical electronics and electromechanical assemblers	Number	106 165	12 570	10 310	46 280	14 260	630	20 980	135	135	270	190	25	(X)	(X)	(X)	380
Electrical electronics and electromechanical assemblers	Percent	55.2%	6.5%	5.4%	24.1%	7.4%	0.3%	10.9%	0.1%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Engine and other machine assemblers 7730 (SOC 51-	Total, both sexes																
Engine and other machine assemblers 7730 (SOC 51-	Number	19 195	1 320	615	14 465	1 875	115	635	20	0	90	35	10	(X)	(X)	(X)	10
Engine and other machine assemblers 7730 (SOC 51-	Percent	100.0%	6.9%	3.2%	75.4%	9.8%	0.6%	3.3%	0.1%	0.0%	0.5%	0.2%	0.1%	(X)	(X)	(X)	0.1%
Engine and other machine assemblers 7730 (SOC 51-	Male																
Engine and other machine assemblers 7730 (SOC 51-	Number	15 575	1 065	460	12 140	1 225	110	450	20	0	70	35	0	(X)	(X)	(X)	0
Engine and other machine assemblers 7730 (SOC 51-	Percent	81.1%	5.5%	2.4%	63.2%	6.4%	0.6%	2.3%	0.1%	0.0%	0.4%	0.2%	0.0%	(X)	(X)	(X)	0.0%
Engine and other machine assemblers 7730 (SOC 51-	Female																
Engine and other machine assemblers 7730 (SOC 51-	Number	3 620	255	155	2 325	650	4	185	0	0	20	0	10	(X)	(X)	(X)	10
Engine and other machine assemblers 7730 (SOC 51-	Percent	18.9%	1.3%	0.8%	12.1%	3.4%	0.0%	1.0%	0.0%	0.0%	0.1%	0.0%	0.1%	(X)	(X)	(X)	0.1%
Structural metal fabricators and fitters 7740 (SOC 51-	Total, both sexes																
Structural metal fabricators and fitters 7740 (SOC 51-	Number	29 340	1 580	1 190	23 035	2 460	195	510	10	30	140	60	30	(X)	(X)	(X)	100
Structural metal fabricators and fitters 7740 (SOC 51-	Percent	100.0%	5.4%	4.1%	78.5%	8.4%	0.7%	1.7%	0.0%	0.1%	0.5%	0.2%	0.1%	(X)	(X)	(X)	0.3%
Structural metal fabricators and fitters 7740 (SOC 51-	Male																
Structural metal fabricators and fitters 7740 (SOC 51-	Number	28 175	1 535	1 080	22 235	2 300	185	485	10	25	140	60	30	(X)	(X)	(X)	100
Structural metal fabricators and fitters 7740 (SOC 51-	Percent	96.0%	5.2%	3.7%	75.8%	7.8%	0.6%	1.7%	0.0%	0.1%	0.5%	0.2%	0.1%	(X)	(X)	(X)	0.3%
Structural metal fabricators and fitters 7740 (SOC 51-	Female																
Structural metal fabricators and fitters 7740 (SOC 51-	Number	1 165	45	115	795	160	10	30	0	4	0	0	0	(X)	(X)	(X)	0
Structural metal fabricators and fitters 7740 (SOC 51-	Percent	4.0%	0.2%	0.4%	2.7%	0.5%	0.0%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Miscellaneous assemblers and fabricators 7750 (SOC 51-	Total, both sexes																
Miscellaneous assemblers and fabricators 7750 (SOC 51-	Number	1 117 435	115 120	96 175	637 270	174 015	5 655	75 860	1 250	2 100	3 955	1 610	765	(X)	(X)	(X)	3 650
Miscellaneous assemblers and fabricators 7750 (SOC 51-	Percent	100.0%	10.3%	8.6%	57.0%	15.6%	0.5%	6.8%	0.1%	0.2%	0.4%	0.1%	0.1%	(X)	(X)	(X)	0.3%
Miscellaneous assemblers and fabricators 7750 (SOC 51-	Male																
Miscellaneous assemblers and fabricators 7750 (SOC 51-	Number	671 125	66 940	54 120	406 320	94 895	3 445	36 380	765	1 555	2 695	1 095	580	(X)	(X)	(X)	2 335
Miscellaneous assemblers and fabricators 7750 (SOC 51-	Percent	60.1%	6.0%	4.8%	36.4%	8.5%	0.3%	3.3%	0.1%	0.1%	0.2%	0.1%	0.1%	(X)	(X)	(X)	0.2%
Miscellaneous assemblers and fabricators 7750 (SOC 51-	Female																
Miscellaneous assemblers and fabricators 7750 (SOC 51-	Number	446 310	48 180	42 055	230 950	79 125	2 215	39 480	485	545	1 260	515	190	(X)	(X)	(X)	1 315
Miscellaneous assemblers and fabricators 7750 (SOC 51-	Percent	39.9%	4.3%	3.8%	20.7%	7.1%	0.2%	3.5%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Bakers 7800 (SOC 51-3011)	Total, both sexes																
Bakers 7800 (SOC 51-3011)	Number	189 835	30 890	23 775	99 335	20 965	1 010	11 025	485	260	620	270	105	(X)	(X)	(X)	1 095
Bakers 7800 (SOC 51-3011)	Percent	100.0%	16.3%	12.5%	52.3%	11.0%	0.5%	5.8%	0.3%	0.1%	0.3%	0.1%	0.1%	(X)	(X)	(X)	0.6%
Bakers 7800 (SOC 51-3011)	Male																
Bakers 7800 (SOC 51-3011)	Number	87 400	18 435	14 495	36 210	9 630	345	7 045	245	125	210	85	65	(X)	(X)	(X)	510
Bakers 7800 (SOC 51-3011)	Percent	46.0%	9.7%	7.6%	19.1%	5.1%	0.2%	3.7%	0.1%	0.1%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.3%
Bakers 7800 (SOC 51-3011)	Female																
Bakers 7800 (SOC 51-3011)	Number	102 435	12 460	9 275	63 125	11 335	665	3 980	240	135	410	185	40	(X)	(X)	(X)	585
Bakers 7800 (SOC 51-3011)	Percent	54.0%	6.6%	4.9%	33.3%	6.0%	0.4%	2.1%	0.1%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Butchers and other meat pou try and fish processing	Total, both sexes																
Butchers and other meat pou try and fish processing	Number	272 910	57 410	44 745	116 620	38 365	1 570	10 825	505	265	835	235	205	(X)	(X)	(X)	1 335
Butchers and other meat pou try and fish processing	Percent	100.0%	21.0%	16.4%	42.7%	14.1%	0.6%	4.0%	0.2%	0.1%	0.3%	0.1%	0.1%	(X)	(X)	(X)	0.5%
Butchers and other meat pou try and fish processing	Male																
Butchers and other meat pou try and fish processing	Number	205 650	41 050	31 785	97 725	23 715	1 250	7 505	430	250	620	195	170	(X)	(X)	(X)	955
Butchers and other meat pou try and fish processing	Percent	75.4%	15.0%	11.6%	35.8%	8.7%	0.5%	2.7%	0.2%	0.1%	0.2%	0.1%	0.1%	(X)	(X)	(X)	0.3%
Butchers and other meat, pou try, and fish processing	Female																
Butchers and other meat pou try and fish processing	Number	67 260	16 360	12 960	18 895	14 650	320	3 320	75	20	215	35	35	(X)	(X)	(X)	380
Butchers and other meat pou try and fish processing	Percent	24.6%	6.0%	4.7%	6.9%	5.4%	0.1%	1.2%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Food and tobacco roasting, baking, and drying machine	Total, both sexes																
Food and tobacco roasting baking and drying machine	Number	12 190	1 720	1 205	6 315	2 040	150	580	20	0	65	25	0	(X)	(X)	(X)	70
Food and tobacco roasting baking and drying machine	Percent	100.0%	14.1%	9.9%	51.8%	16.7%	1.2%	4.8%	0.2%	0.0%	0.5%	0.2%	0.0%	(X)	(X)	(X)	0.6%
Food and tobacco roasting baking and drying machine	Male																
Food and tobacco roasting baking and drying machine	Number	8 145	1 300	780	4 255	1 370	45	325	0	0	20	15	0	(X)	(X)	(X)	40
Food and tobacco roasting baking and drying machine	Percent	66.8%	10.7%	6.4%	34.9%	11.2%	0.4%	2.7%	0.0%	0.0%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Food and tobacco roasting baking and drying machine	Female																
Food and tobacco roasting baking and drying machine	Number	4 040	420	425	2 060	670	105	255	20	0	45	10	0	(X)	(X)	(X)	35
Food and tobacco roasting baking and drying machine	Percent	33.1%	3.4%	3.5%	16.9%	5.5%	0.9%	2.1%	0.2%	0.0%	0.4%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Food batchmakers 7840 (SOC 51-3092)	Total, both sexes																
Food batchmakers 7840 (SOC 51-3092)	Number	90 760	15 035	9 360	49 460	11 395	585	3 385	60	130	595	370	100	(X)	(X)	(X)	290
Food batchmakers 7840 (SOC 51-3092)	Percent	100.0%	16.6%	10.3%	54.5%	12.6%	0.6%	3.7%	0.1%	0.1%	0.7%	0.4%	0.1%	(X)	(X)	(X)	0.3%
Food batchmakers 7840 (SOC 51-3092)	Male																
Food batchmakers 7840 (SOC 51-3092)	Number	36 995	6 600	4 390	18 070	5 870	255	1 255	35	45	245	105	65	(X)	(X)	(X)	65
Food batchmakers 7840 (SOC 51-3092)	Percent	40.8%	7.3%	4.8%	19.9%	6.5%	0.3%	1.4%	0.0%	0.0%	0.3%	0.1%	0.1%	(X)	(X)	(X)	0.1%
Food batchmakers 7840 (SOC 51-3092)	Female																
Food batchmakers 7840 (SOC 51-3092)	Number	53 765	8 430	4 975	31 390	5 525	330	2 130	25	85	350	265	35	(X)	(X)	(X)	225
Food batchmakers 7840 (SOC 51-3092)	Percent	59.2%	9.3%	5.5%	34.6%	6.1%	0.4%	2.3%	0.0%	0.1%	0.4%	0.3%	0.0%	(X)	(X)	(X)	0.2%
Food cooking machine operators and tenders 7850 (SOC	Total, both sexes																
Food cooking machine operators and tenders 7850 (SOC	Number	13 090	1 650	2 070	6 250	1 905	95	810	25	125	100	45	15	(X)	(X)	(X)	10
Food cooking machine operators and tenders 7850 (SOC	Percent	100.0%	12.6%	15.8%	47.7%	14.6%	0.7%	6.2%	0.2%	1.0%	0.8%	0.3%	0.1%	(X)	(X)	(X)	0.1%
Food cooking machine operators and tenders 7850 (SOC	Male																
Food cooking machine operators and tenders 7850 (SOC	Number	7,620	1,110	980	3,630	1,130	20	495	25	120	75	25	4	(X)	(X)	(X)	10
Food cooking machine operators and tenders 7850 (SOC	Percent	58.2%	8.5%	7.5%	27.7%	8.6%	0.2%	3.8%	0.2%	0.9%	0.6%	0.2%	0.0%	(X)	(X)	(X)	0.1%
Food cooking machine operators and tenders 7850 (SOC	Female																
Food cooking machine operators and tenders 7850 (SOC	Number	5,470	540	1,090	2,620	775	75	315	0	4	25	15	15	(X)	(X)	(X)	0
Food cooking machine operators and tenders 7850 (SOC	Percent	41.8%	4.1%	8.3%	20.0%	5.9%	0.6%	2.4%	0.0%	0.0%	0.2%	0.1%	0.1%	(X)	(X)	(X)	0.0%
Food processing workers all other 7855 (SOC 51-3099)	Total, both sexes																
Food processing workers all other 7855 (SOC 51-3099)	Number	134 320	24 005	20 835	55 610	23 660	855	7 355	465	175	520	130	105	(X)	(X)	(X)	610
Food processing workers all other 7855 (SOC 51-3099)	Percent	100.0%	17.9%	15.5%	41.4%	17.6%	0.6%	5.5%	0.3%	0.1%	0.4%	0.1%	0.1%	(X)	(X)	(X)	0.5%
Food processing workers all other 7855 (SOC 51-3099)	Male																
Food processing workers all other 7855 (SOC 51-3099)	Number	84 080	15 230	13 185	36 005	13 460	565	4 505	370	110	300	60	80	(X)	(X)	(X)	215
Food processing workers all other 7855 (SOC 51-3099)	Percent	62.6%	11.3%	9.8%	26.8%	10.0%	0.4%	3.4%	0.3%	0.1%	0.2%	0.0%	0.1%	(X)	(X)	(X)	0.2%
Food processing workers all other 7855 (SOC 51-3099)	Female																
Food processing workers all other 7855 (SOC 51-3099)	Number	50 240	8 775	7 650	19 605	10 200	285	2 850	95	70	220	70	25	(X)	(X)	(X)	395

Food processing workers, all other 7855 (SOC 51-3099)	Percent	37.4%	6.5%	5.7%	14.6%	7.6%	0.2%	2.1%	0.1%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Computer control programmers and operators 7900 (SOC	Total, both sexes																
Computer control programmers and operators 7900 (SOC	Number	74 025	3 815	2 925	58 500	4 230	225	3 605	60	70	385	55	15	(X)	(X)	(X)	145
Computer control programmers and operators 7900 (SOC	Percent	100.0%	5.2%	4.0%	79.0%	5.7%	0.3%	4.9%	0.1%	0.1%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Computer control programmers and operators 7900 (SOC	Male																
Computer control programmers and operators 7900 (SOC	Number	67 005	3 395	2 655	53 225	3 535	190	3 340	60	70	375	55	15	(X)	(X)	(X)	95
Computer control programmers and operators 7900 (SOC	Percent	90.5%	4.6%	3.6%	71.9%	4.8%	0.3%	4.5%	0.1%	0.1%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Computer control programmers and operators 7900 (SOC	Female																
Computer control programmers and operators 7900 (SOC	Number	7 020	420	270	5 275	695	35	265	0	0	10	0	0	(X)	(X)	(X)	50
Computer control programmers and operators 7900 (SOC	Percent	9.5%	0.6%	0.4%	7.1%	0.9%	0.0%	0.4%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Extruding and drawing machine setters operators and	Total, both sexes																
Extruding and drawing machine setters operators and	Number	13 915	715	630	10 950	1 100	80	275	10	0	105	30	0	(X)	(X)	(X)	25
Extruding and drawing machine setters operators and	Percent	100.0%	5.1%	4.5%	78.7%	7.9%	0.6%	2.0%	0.1%	0.0%	0.8%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Extruding and drawing machine setters operators and	Male																
Extruding and drawing machine setters operators and	Number	11 585	570	490	9 205	855	80	225	10	0	95	30	0	(X)	(X)	(X)	25
Extruding and drawing machine setters operators and	Percent	83.3%	4.1%	3.5%	66.2%	6.1%	0.6%	1.6%	0.1%	0.0%	0.7%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Extruding and drawing machine setters operators and	Female																
Extruding and drawing machine setters operators and	Number	2 335	145	145	1 750	240	0	45	0	0	10	0	0	(X)	(X)	(X)	0
Extruding and drawing machine setters operators and	Percent	16.8%	1.0%	1.0%	12.6%	1.7%	0.0%	0.3%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Forging machine setters operators and tenders metal	Total, both sexes																
Forging machine setters operators and tenders metal	Number	8 890	390	425	6 915	860	55	185	4	0	50	10	0	(X)	(X)	(X)	0
Forging machine setters operators and tenders metal	Percent	100.0%	4.4%	4.8%	77.8%	9.7%	0.6%	2.1%	0.0%	0.0%	0.6%	0.1%	0.0%	(X)	(X)	(X)	0.0%
Forging machine setters operators and tenders metal	Male																
Forging machine setters operators and tenders metal	Number	8 575	390	425	6 655	815	55	175	4	0	50	10	0	(X)	(X)	(X)	0
Forging machine setters operators and tenders metal	Percent	96.5%	4.4%	4.8%	74.9%	9.2%	0.6%	2.0%	0.0%	0.0%	0.6%	0.1%	0.0%	(X)	(X)	(X)	0.0%
Forging machine setters, operators, and tenders, metal	Female																
Forging machine setters operators and tenders metal	Number	320	0	0	260	45	4	10	0	0	0	0	0	(X)	(X)	(X)	0
Forging machine setters operators and tenders metal	Percent	3.6%	0.0%	0.0%	2.9%	0.5%	0.0%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Rolling machine setters, operators, and tenders, metal and	Total, both sexes																
Rolling machine setters operators and tenders metal and	Number	12 455	1 020	795	8 520	1 450	135	325	15	55	120	20	0	(X)	(X)	(X)	0
Rolling machine setters operators and tenders metal and	Percent	100.0%	8.2%	6.4%	68.4%	11.6%	1.1%	2.6%	0.1%	0.4%	1.0%	0.2%	0.0%	(X)	(X)	(X)	0.0%
Rolling machine setters operators and tenders metal and	Male																
Rolling machine setters operators and tenders metal and	Number	9 260	700	660	6 185	1 165	105	265	4	40	120	20	0	(X)	(X)	(X)	0
Rolling machine setters operators and tenders metal and	Percent	74.3%	5.6%	5.3%	49.7%	9.4%	0.8%	2.1%	0.0%	0.3%	1.0%	0.2%	0.0%	(X)	(X)	(X)	0.0%
Rolling machine setters operators and tenders metal and	Female																
Rolling machine setters operators and tenders metal and	Number	3 195	320	135	2 335	285	30	60	10	15	0	0	0	(X)	(X)	(X)	0
Rolling machine setters operators and tenders metal and	Percent	25.7%	2.6%	1.1%	18.7%	2.3%	0.2%	0.5%	0.1%	0.1%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Cutting punching and press machine setters operators	Total, both sexes																
Cutting punching and press machine setters operators	Number	113 175	9 995	7 145	78 405	13 440	645	2 220	10	85	695	80	60	(X)	(X)	(X)	385
Cutting punching and press machine setters operators	Percent	100.0%	8.8%	6.3%	69.3%	11.9%	0.6%	2.0%	0.0%	0.1%	0.6%	0.1%	0.1%	(X)	(X)	(X)	0.3%
Cutting punching and press machine setters operators	Male																
Cutting punching and press machine setters operators	Number	89 625	8 540	6 110	61 565	10 150	560	1 625	10	70	605	40	60	(X)	(X)	(X)	285
Cutting punching and press machine setters operators	Percent	79.2%	7.5%	5.4%	54.4%	9.0%	0.5%	1.4%	0.0%	0.1%	0.5%	0.0%	0.1%	(X)	(X)	(X)	0.3%
Cutting punching and press machine setters operators	Female																
Cutting punching and press machine setters operators	Number	23 555	1 455	1 035	16 840	3 290	85	595	0	15	90	40	4	(X)	(X)	(X)	105
Cutting punching and press machine setters operators	Percent	20.8%	1.3%	0.9%	14.9%	2.9%	0.1%	0.5%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Dr lling and boring machine tool setters operators and	Total, both sexes																
Dr lling and boring machine tool setters operators and	Number	5 775	455	220	4 410	480	90	55	20	0	35	0	0	(X)	(X)	(X)	4
Dr lling and boring machine tool setters operators and	Percent	100.0%	7.9%	3.8%	76.4%	8.3%	1.6%	1.0%	0.3%	0.0%	0.6%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Dr lling and boring machine tool setters operators and	Male																
Dr lling and boring machine tool setters, operators, and	Number	4,925	400	190	3,830	365	55	35	20	0	35	0	0	(X)	(X)	(X)	0
Dr lling and boring machine tool setters operators and	Percent	85.3%	6.9%	3.3%	66.3%	6.3%	1.0%	0.6%	0.3%	0.0%	0.6%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Dr lling and boring machine tool setters operators and	Female																
Dr lling and boring machine tool setters, operators, and	Number	850	55	35	585	115	35	20	0	0	0	0	0	(X)	(X)	(X)	4
Dr lling and boring machine tool setters operators and	Percent	14.7%	1.0%	0.6%	10.1%	2.0%	0.6%	0.3%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Grinding lapping polishing and buffing machine tool	Total, both sexes																
Grinding lapping polishing and buffing machine tool	Number	59 575	6 630	6 820	37 045	6 625	360	1 480	60	30	235	50	55	(X)	(X)	(X)	195
Grinding lapping polishing and buffing machine tool	Percent	100.0%	11.1%	11.4%	62.2%	11.1%	0.6%	2.5%	0.1%	0.1%	0.4%	0.1%	0.1%	(X)	(X)	(X)	0.3%
Grinding lapping polishing and buffing machine tool	Male																
Grinding lapping polishing and buffing machine tool	Number	52 300	5 935	6 150	32 160	6 140	280	1 105	60	10	200	50	55	(X)	(X)	(X)	150
Grinding lapping polishing and buffing machine tool	Percent	87.8%	10.0%	10.3%	54.0%	10.3%	0.5%	1.9%	0.1%	0.0%	0.3%	0.1%	0.1%	(X)	(X)	(X)	0.3%
Grinding lapping polishing and buffing machine tool	Female																
Grinding lapping polishing and buffing machine tool	Number	7 280	695	670	4 885	485	80	375	0	20	35	0	0	(X)	(X)	(X)	40
Grinding lapping polishing and buffing machine tool	Percent	12.2%	1.2%	1.1%	8.2%	0.8%	0.1%	0.6%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Lathe and turning machine tool setters operators and	Total, both sexes																
Lathe and turning machine tool setters operators and	Number	14 420	1 200	880	11 030	765	80	320	0	0	80	4	4	(X)	(X)	(X)	60
Lathe and turning machine tool setters operators and	Percent	100.0%	8.3%	6.1%	76.5%	5.3%	0.6%	2.2%	0.0%	0.0%	0.6%	0.0%	0.0%	(X)	(X)	(X)	0.4%
Lathe and turning machine tool setters operators and	Male																
Lathe and turning machine tool setters operators and	Number	12 775	1 055	720	9 925	585	80	275	0	0	70	4	4	(X)	(X)	(X)	60
Lathe and turning machine tool setters operators and	Percent	88.6%	7.3%	5.0%	68.8%	4.1%	0.6%	1.9%	0.0%	0.0%	0.5%	0.0%	0.0%	(X)	(X)	(X)	0.4%
Lathe and turning machine tool setters operators and	Female																
Lathe and turning machine tool setters operators and	Number	1 645	145	160	1 105	180	0	45	0	0	10	0	0	(X)	(X)	(X)	0
Lathe and turning machine tool setters operators and	Percent	11.4%	1.0%	1.1%	7.7%	1.2%	0.0%	0.3%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Machinists 8030 (SOC 51-4041)	Total, both sexes																
Machinists 8030 (SOC 51-4041)	Number	394 735	24 210	17 390	306 205	23 630	2 120	16 170	580	345	2 210	600	150	(X)	(X)	(X)	1 115
Machinists 8030 (SOC 51-4041)	Percent	100.0%	6.1%	4.4%	77.6%	6.0%	0.5%	4.1%	0.1%	0.1%	0.6%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Machinists 8030 (SOC 51-4041)	Male																
Machinists 8030 (SOC 51-4041)	Number	376 520	22 805	16 040	294 545	20 900	2 000	15 610	550	330	2 050	535	150	(X)	(X)	(X)	1 000
Machinists 8030 (SOC 51-4041)	Percent	95.4%	5.8%	4.1%	74.6%	5.3%	0.5%	4.0%	0.1%	0.1%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Machinists 8030 (SOC 51-4041)	Female																
Machinists 8030 (SOC 51-4041)	Number	18 215	1 405	1 350	11 655	2 730	120	565	30	15	160	65	0	(X)	(X)	(X)	115
Machinists 8030 (SOC 51-4041)	Percent	4.6%	0.4%	0.3%	3.0%	0.7%	0.0%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Metal furnace operators tenders pourers and casters	Total, both sexes																
Metal furnace operators tenders pourers and casters	Number	27 030	1 700	1 455	19 180	3 965	185	310	10	15	150	30	0	(X)	(X)	(X)	35
Metal furnace operators tenders pourers and casters	Percent	100.0%	6.3%	5.4%	71.0%	14.7%	0.7%	1.1%	0.0%	0.1%	0.6%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Metal furnace operators tenders pourers and casters	Male																
Metal furnace operators tenders pourers and casters	Number	24 835	1 630	1 335	17 785	3 470	170	230	10	15	125	30	0	(X)	(X)	(X)	35
Metal furnace operators tenders pourers and casters	Percent	91.9%	6.0%	4.9%	65.8%	12.8%	0.6%	0.9%	0.0%	0.1%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Metal furnace operators tenders pourers and casters	Female																
Metal furnace operators tenders pourers and casters	Number	2 195	65	120	1 395	500	15	80	0	0	20	0	0	(X)	(X)	(X)	0
Metal furnace operators tenders pourers and casters	Percent	8.1%	0.2%	0.4%	5.2%	1.8%	0.1%	0.3%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Model makers and patternmakers metal and plastic 8060	Total, both sexes																
Model makers and patternmakers metal and plastic 8060	Number	7 950	575	325	6 495	260	10	165	4	4	50	10	30	(X)	(X)	(X)	25
Model makers and patternmakers metal and plastic 8060	Percent	100.0%	7.2%	4.1%	81.7%	3.3%	0.1%	2.1%	0.1%	0.1%	0.6%	0.1%	0.4%	(X)	(X)	(X)	0.3%
Model makers and patternmakers metal and plastic 8060	Male																
Model makers and patternmakers metal and plastic 8060	Number	6 690	375	255	5 695	220	10	55	4	0	15	10	30	(X)	(X)	(X)	25
Model makers and patternmakers metal and plastic 8060	Percent	84.2%	4.7%	3.2%	71.6%	2.8%	0.1%	0.7%	0.1%	0.0%	0.2%	0.1%	0.4%	(X)	(X)	(X)	0.3%
Model makers and patternmakers metal and plastic 8060	Female																
Model makers and patternmakers metal and plastic 8060	Number	1 260	200	70	800	40	0	110	0	4	35	0	0	(X)	(X)	(X)	0
Model makers and patternmakers metal and plastic 8060	Percent	15.8%	2.5%	0.9%	10.1%	0.5%	0.0%	1.4%	0.0%	0.1%	0.4%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Molders and molding machine setters, operators, and	Total, both sexes																
Molders and molding machine setters operators and	Number	53 865	4 245	3 825	37 065	6 365	200	1 455	105	85	205	70	10	(X)	(X)	(X)	245
Molders and molding machine setters operators and	Percent	100.0%	7.9%	7.1%	68.8%	11.8%	0.4%	2.7%	0.2%	0.2%	0.4%	0.1%	0.0%	(X)	(X)	(X)	0.5%
Molders and molding machine setters, operators, and	Male																
Molders and molding machine setters operators and	Number	43 445	3 310	3 215	30 520	4 495	170	1 170	90	75	140	50	10	(X)	(X)	(X)	205
Molders and molding machine setters operators and	Percent	80.7%	6.1%	6.0%	56.7%	8.3%	0.3%	2.2%	0.2%	0.1%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.4%
Molders and molding machine setters, operators, and	Female																
Molders and molding machine setters operators and	Number	10 420	935	610	6 540	1 870	30	285	15	10	65	20	0	(X)	(X)	(X)	40
Molders and molding machine setters operators and	Percent	19.3%	1.7%	1.1%	12.1%	3.5%	0.1%	0.5%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Tool and die makers 8130 (SOC 51-4111)	Total, both sexes																
Tool and die makers 8130 (SOC 51-4111)	Number	76 410	2 720	1 650	67 795	2 380	115	1 145	35	65	325	60	45	(X)	(X)	(X)	75
Tool and die makers 8130 (SOC 51-4111)	Percent	100.0%	3.6%	2.2%	88.7%	3.1%	0.2%	1.5%	0.0%	0.1%	0.4%	0.1%	0.1%	(X)	(X)	(X)	0.1%
Tool and die makers 8130 (SOC 51-4111)	Male																
Tool and die makers 8130 (SOC 51-4111)	Number	74 230	2 610	1 315	66 405	2 145	115	1 070	35	65	300	60	45	(X)	(X)	(X)	60
Tool and die makers 8130 (SOC 51-4111)	Percent	97.1%	3.4%	1.7%	86.9%	2.8%	0.2%	1.4%	0.0%	0.1%	0.4%	0.1%	0.1%	(X)	(X)	(X)	0.1%
Tool and die makers 8130 (SOC 51-4111)	Female																
Tool and die makers 8130 (SOC 51-4111)	Number	2 180	105	335	1 390	235	0	75	0	0	25	0	0	(X)	(X)	(X)	15
Tool and die makers 8130 (SOC 51-4111)	Percent	2.9%	0.1%	0.4%	1.8%	0.3%	0.0%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Welding soldering and brazing workers 8140 (SOC 51-	Total, both sexes																
Welding soldering and brazing workers 8140 (SOC 51-	Number	648 205	78 545	55 285	430 635	52 875	7 295	15 590	830	580	3 980	615	300	(X)	(X)	(X)	1 675
Welding soldering and brazing workers 8140 (SOC 51-	Percent	100.0%	12.1%	8.5%	66.4%	8.2%	1.1%	2.4%	0.1%	0.1%	0.6%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Welding soldering and brazing workers 8140 (SOC 51-	Male																
Welding soldering and brazing workers 8140 (SOC 51-	Number	611 145	75 275	52 615	408 275	48 150	6 560	12 865	815	500	3 735	560	290	(X)	(X)	(X)	1 505
Welding soldering and brazing workers 8140 (SOC 51-	Percent	94.3%	11.6%	8.1%	63.0%	7.4%	1.0%	2.0%	0.1%	0.1%	0.6%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Welding soldering and brazing workers 8140 (SOC 51-	Female																
Welding, soldering, and brazing workers 8140 (SOC 51-	Number	37,055	3,265	2,665	22,360	4,725	735	2,725	15	80	245	55	10	(X)	(X)	(X)	170
Welding soldering and brazing workers 8140 (SOC 51-	Percent	5.7%	0.5%	0.4%	3.4%	0.7%	0.1%	0.4%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Heat treating equipment setters operators and tenders	Total, both sexes																
Heat treating equipment setters, operators, and tenders,	Number	8,660	590	365	6,420	1,010	90	120	15	10	15	15	0	(X)	(X)	(X)	15
Heat treating equipment setters operators and tenders	Percent	100.0%	6.8%	4.2%	74.1%	11.7%	1.0%	1.4%	0.2%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Heat treating equipment setters operators and tenders	Male																
Heat treating equipment setters operators and tenders	Number	7 735	560	325	5 695	885	90	120	15	10	15	15	0	(X)	(X)	(X)	15
Heat treating equipment setters operators and tenders	Percent	89.3%	6.5%	3.8%	65.8%	10.2%	1.0%	1.4%	0.2%	0.1%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Heat treating equipment setters operators and tenders	Female																
Heat treating equipment setters operators and tenders	Number	925	30	40	725	130	0	0	0	0	0	0	0	(X)	(X)	(X)	0
Heat treating equipment setters operators and tenders	Percent	10.7%	0.3%	0.5%	8.4%	1.5%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Plating and coating machine setters operators and	Total, both sexes																
Plating and coating machine setters operators and	Number	18 855	2 160	1 730	12 210	1 845	55	590	4	70	85	0	15	(X)	(X)	(X)	90

Plating and coating machine setters, operators, and	Percent	100.0%	11.5%	9.2%	64.8%	9.8%	0.3%	3.1%	0.0%	0.4%	0.5%	0.0%	0.1%	(X)	(X)	(X)	0.5%
Plating and coating machine setters operators and	Male																
Plating and coating machine setters operators and	Number	16 870	2 080	1 550	10 735	1 650	45	560	4	70	80	0	15	(X)	(X)	(X)	80
Plating and coating machine setters, operators, and	Percent	89.5%	11.0%	8.2%	56.9%	8.8%	0.2%	3.0%	0.0%	0.4%	0.4%	0.0%	0.1%	(X)	(X)	(X)	0.4%
Plating and coating machine setters operators and	Female																
Plating and coating machine setters operators and	Number	1 985	80	185	1 475	195	10	25	0	0	4	0	0	(X)	(X)	(X)	10
Plating and coating machine setters operators and	Percent	10.5%	0.4%	1.0%	7.8%	1.0%	0.1%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Tool grinders filers and sharpeners 8210 (SOC 51-4194)	Total both sexes																
Tool grinders filers and sharpeners 8210 (SOC 51-4194)	Number	8 760	265	245	7 340	510	30	250	0	0	60	25	0	(X)	(X)	(X)	40
Tool grinders filers and sharpeners 8210 (SOC 51-4194)	Percent	100.0%	3.0%	2.8%	83.8%	5.8%	0.3%	2.9%	0.0%	0.0%	0.7%	0.3%	0.0%	(X)	(X)	(X)	0.5%
Tool grinders filers and sharpeners 8210 (SOC 51-4194)	Male																
Tool grinders filers and sharpeners 8210 (SOC 51-4194)	Number	8 340	220	195	7 020	495	30	250	0	0	60	25	0	(X)	(X)	(X)	40
Tool grinders filers and sharpeners 8210 (SOC 51-4194)	Percent	95.2%	2.5%	2.2%	80.1%	5.7%	0.3%	2.9%	0.0%	0.0%	0.7%	0.3%	0.0%	(X)	(X)	(X)	0.5%
Tool grinders filers and sharpeners 8210 (SOC 51-4194)	Female																
Tool grinders filers and sharpeners 8210 (SOC 51-4194)	Number	420	45	45	320	10	0	0	0	0	0	0	0	(X)	(X)	(X)	0
Tool grinders filers and sharpeners 8210 (SOC 51-4194)	Percent	4.8%	0.5%	0.5%	3.7%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Miscellaneous metal workers and plastic workers	Total both sexes																
Miscellaneous metal workers and plastic workers	Number	463 790	55 090	48 935	258 185	61 580	2 225	32 640	415	450	1 865	505	325	(X)	(X)	(X)	1 565
Miscellaneous metal workers and plastic workers	Percent	100.0%	11.9%	10.6%	55.7%	13.3%	0.5%	7.0%	0.1%	0.1%	0.4%	0.1%	0.1%	(X)	(X)	(X)	0.3%
Miscellaneous metal workers and plastic workers	Male																
Miscellaneous metal workers and plastic workers	Number	353 705	40 810	36 425	203 815	42 775	1 760	24 240	330	325	1 465	390	300	(X)	(X)	(X)	1 065
Miscellaneous metal workers and plastic workers	Percent	76.3%	8.8%	7.9%	43.9%	9.2%	0.4%	5.2%	0.1%	0.1%	0.3%	0.1%	0.1%	(X)	(X)	(X)	0.2%
Miscellaneous metal workers and plastic workers	Female																
Miscellaneous metal workers and plastic workers	Number	110 080	14 280	12 505	54 370	18 805	460	8 400	90	130	400	115	25	(X)	(X)	(X)	500
Miscellaneous metal workers and plastic workers	Percent	23.7%	3.1%	2.7%	11.7%	4.1%	0.1%	1.8%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Prepress technicians and workers 8250 (SOC 51-5111)	Total, both sexes																
Prepress technicians and workers 8250 (SOC 51-5111)	Number	48 120	3 085	2 985	33 490	5 510	140	2 170	70	190	235	90	40	(X)	(X)	(X)	115
Prepress technicians and workers 8250 (SOC 51-5111)	Percent	100.0%	6.4%	6.2%	69.6%	11.5%	0.3%	4.5%	0.1%	0.4%	0.5%	0.2%	0.1%	(X)	(X)	(X)	0.2%
Prepress technicians and workers 8250 (SOC 51-5111)	Male																
Prepress technicians and workers 8250 (SOC 51-5111)	Number	23 540	1 490	1 310	17 115	2 125	55	1 230	0	55	60	50	0	(X)	(X)	(X)	55
Prepress technicians and workers 8250 (SOC 51-5111)	Percent	48.9%	3.1%	2.7%	35.6%	4.4%	0.1%	2.6%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Prepress technicians and workers 8250 (SOC 51-5111)	Female																
Prepress technicians and workers 8250 (SOC 51-5111)	Number	24 580	1 595	1 675	16 375	3 385	85	940	70	130	180	45	40	(X)	(X)	(X)	60
Prepress technicians and workers 8250 (SOC 51-5111)	Percent	51.1%	3.3%	3.5%	34.0%	7.0%	0.2%	2.0%	0.1%	0.3%	0.4%	0.1%	0.1%	(X)	(X)	(X)	0.1%
Printing press operators 8255 (SOC 51-5112)	Total both sexes																
Printing press operators 8255 (SOC 51-5112)	Number	244 330	22 110	16 750	166 885	24 050	935	10 055	265	390	1 145	395	210	(X)	(X)	(X)	1 135
Printing press operators 8255 (SOC 51-5112)	Percent	100.0%	9.0%	6.9%	68.3%	9.8%	0.4%	4.1%	0.1%	0.2%	0.5%	0.2%	0.1%	(X)	(X)	(X)	0.5%
Printing press operators 8255 (SOC 51-5112)	Male																
Printing press operators 8255 (SOC 51-5112)	Number	196 240	16 825	12 990	135 990	18 375	740	8 315	250	315	930	325	165	(X)	(X)	(X)	1 015
Printing press operators 8255 (SOC 51-5112)	Percent	80.3%	6.9%	5.3%	55.7%	7.5%	0.3%	3.4%	0.1%	0.1%	0.4%	0.1%	0.1%	(X)	(X)	(X)	0.4%
Printing press operators 8255 (SOC 51-5112)	Female																
Printing press operators 8255 (SOC 51-5112)	Number	48 090	5 290	3 760	30 895	5 675	195	1 740	15	75	215	70	45	(X)	(X)	(X)	120
Printing press operators 8255 (SOC 51-5112)	Percent	19.7%	2.2%	1.5%	12.6%	2.3%	0.1%	0.7%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Print binding and finishing workers 8256 (SOC 51-5113)	Total both sexes																
Print binding and finishing workers 8256 (SOC 51-5113)	Number	36 810	3 090	1 910	26 315	3 375	150	1 465	60	35	185	35	75	(X)	(X)	(X)	120
Print binding and finishing workers 8256 (SOC 51-5113)	Percent	100.0%	8.4%	5.2%	71.5%	9.2%	0.4%	4.0%	0.2%	0.1%	0.5%	0.1%	0.2%	(X)	(X)	(X)	0.3%
Print binding and finishing workers 8256 (SOC 51-5113)	Male																
Print binding and finishing workers 8256 (SOC 51-5113)	Number	19 085	1 515	1 010	14 250	1 230	40	700	55	35	70	35	40	(X)	(X)	(X)	105
Print binding and finishing workers 8256 (SOC 51-5113)	Percent	51.8%	4.1%	2.7%	38.7%	3.3%	0.1%	1.9%	0.1%	0.1%	0.2%	0.1%	0.1%	(X)	(X)	(X)	0.3%
Print binding and finishing workers 8256 (SOC 51-5113)	Female																
Print binding and finishing workers 8256 (SOC 51-5113)	Number	17,725	1,580	900	12,070	2,145	110	770	4	0	110	0	30	(X)	(X)	(X)	10
Print binding and finishing workers 8256 (SOC 51-5113)	Percent	48.2%	4.3%	2.4%	32.8%	5.8%	0.3%	2.1%	0.0%	0.0%	0.3%	0.0%	0.1%	(X)	(X)	(X)	0.0%
Laundry and dry-cleaning workers 8300 (SOC 51-6011)	Total both sexes																
Laundry and dry-cleaning workers 8300 (SOC 51-6011)	Number	217,680	37,905	30,000	90,820	38,550	1,550	15,505	545	215	875	335	195	(X)	(X)	(X)	1,185
Laundry and dry-cleaning workers 8300 (SOC 51-6011)	Percent	100.0%	17.4%	13.8%	41.7%	17.7%	0.7%	7.1%	0.3%	0.1%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.5%
Laundry and dry-cleaning workers 8300 (SOC 51-6011)	Male																
Laundry and dry-cleaning workers 8300 (SOC 51-6011)	Number	88 725	13 495	11 665	40 485	13 815	320	7 250	325	120	320	240	105	(X)	(X)	(X)	585
Laundry and dry-cleaning workers 8300 (SOC 51-6011)	Percent	40.8%	6.2%	5.4%	18.6%	6.3%	0.1%	3.3%	0.1%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Laundry and dry-cleaning workers 8300 (SOC 51-6011)	Female																
Laundry and dry-cleaning workers 8300 (SOC 51-6011)	Number	128 955	24 410	18 340	50 335	24 735	1 230	8 255	215	100	555	95	90	(X)	(X)	(X)	600
Laundry and dry-cleaning workers 8300 (SOC 51-6011)	Percent	59.2%	11.2%	8.4%	23.1%	11.4%	0.6%	3.8%	0.1%	0.0%	0.3%	0.0%	0.0%	(X)	(X)	(X)	0.3%
Pressers textile garment and related materials 8310	Total both sexes																
Pressers textile garment and related materials 8310	Number	63 480	15 190	12 800	18 240	12 185	265	4 135	50	55	95	65	90	(X)	(X)	(X)	305
Pressers textile garment and related materials 8310	Percent	100.0%	23.9%	20.2%	28.7%	19.2%	0.4%	6.5%	0.1%	0.1%	0.1%	0.1%	0.1%	(X)	(X)	(X)	0.5%
Pressers textile garment and related materials 8310	Male																
Pressers textile garment and related materials 8310	Number	19 085	3 515	3 655	6 465	2 910	95	2 230	0	20	40	50	35	(X)	(X)	(X)	65
Pressers textile garment and related materials 8310	Percent	30.1%	5.5%	5.8%	10.2%	4.6%	0.1%	3.5%	0.0%	0.0%	0.1%	0.1%	0.1%	(X)	(X)	(X)	0.1%
Pressers textile garment and related materials 8310	Female																
Pressers textile garment and related materials 8310	Number	44 400	11 670	9 145	11 775	9 275	170	1 910	50	40	55	15	55	(X)	(X)	(X)	235
Pressers textile garment and related materials 8310	Percent	69.9%	18.4%	14.4%	18.5%	14.6%	0.3%	3.0%	0.1%	0.1%	0.1%	0.0%	0.1%	(X)	(X)	(X)	0.4%
Sewing machine operators 8320 (SOC 51-6031)	Total both sexes																
Sewing machine operators 8320 (SOC 51-6031)	Number	252 005	45 715	46 935	94 350	27 415	1 005	34 500	280	285	625	230	75	(X)	(X)	(X)	590
Sewing machine operators 8320 (SOC 51-6031)	Percent	100.0%	18.1%	18.6%	37.4%	10.9%	0.4%	13.7%	0.1%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Sewing machine operators 8320 (SOC 51-6031)	Male																
Sewing machine operators 8320 (SOC 51-6031)	Number	56 765	13 250	14 970	16 440	7 125	165	4 435	45	70	90	30	40	(X)	(X)	(X)	100
Sewing machine operators 8320 (SOC 51-6031)	Percent	22.5%	5.3%	5.9%	6.5%	2.8%	0.1%	1.8%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Sewing machine operators 8320 (SOC 51-6031)	Female																
Sewing machine operators 8320 (SOC 51-6031)	Number	195 240	32 465	31 970	77 910	20 290	840	30 065	235	215	535	200	30	(X)	(X)	(X)	490
Sewing machine operators 8320 (SOC 51-6031)	Percent	77.5%	12.9%	12.7%	30.9%	8.1%	0.3%	11.9%	0.1%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Shoe and leather workers and repairers 8330 (SOC 51-	Total both sexes																
Shoe and leather workers and repairers 8330 (SOC 51-	Number	11 040	1 900	1 335	6 125	695	60	750	0	40	80	0	0	(X)	(X)	(X)	60
Shoe and leather workers and repairers 8330 (SOC 51-	Percent	100.0%	17.2%	12.1%	55.5%	6.3%	0.5%	6.8%	0.0%	0.4%	0.7%	0.0%	0.0%	(X)	(X)	(X)	0.5%
Shoe and leather workers and repairers 8330 (SOC 51-	Male																
Shoe and leather workers and repairers 8330 (SOC 51-	Number	8 635	1 555	970	4 840	465	30	655	0	0	55	0	0	(X)	(X)	(X)	60
Shoe and leather workers and repairers 8330 (SOC 51-	Percent	78.2%	14.1%	8.8%	43.8%	4.2%	0.3%	5.9%	0.0%	0.0%	0.5%	0.0%	0.0%	(X)	(X)	(X)	0.5%
Shoe and leather workers and repairers 8330 (SOC 51-	Female																
Shoe and leather workers and repairers 8330 (SOC 51-	Number	2 410	345	365	1 280	230	30	95	0	40	25	0	0	(X)	(X)	(X)	0
Shoe and leather workers and repairers 8330 (SOC 51-	Percent	21.8%	3.1%	3.3%	11.6%	2.1%	0.3%	0.9%	0.0%	0.4%	0.2%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Shoe machine operators and tenders 8340 (SOC 51-	Total both sexes																
Shoe machine operators and tenders 8340 (SOC 51-	Number	4 910	710	605	2 625	585	0	325	4	10	10	10	0	(X)	(X)	(X)	25
Shoe machine operators and tenders 8340 (SOC 51-	Percent	100.0%	14.5%	12.3%	53.5%	11.9%	0.0%	6.6%	0.1%	0.2%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.5%
Shoe machine operators and tenders 8340 (SOC 51-	Male																
Shoe machine operators and tenders 8340 (SOC 51-	Number	2 255	340	390	1 190	240	0	75	4	10	10	0	0	(X)	(X)	(X)	4
Shoe machine operators and tenders 8340 (SOC 51-	Percent	45.9%	6.9%	7.9%	24.2%	4.9%	0.0%	1.5%	0.1%	0.2%	0.2%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Shoe machine operators and tenders 8340 (SOC 51-	Female																
Shoe machine operators and tenders 8340 (SOC 51-	Number	2 655	375	215	1 435	345	0	255	0	0	0	10	0	(X)	(X)	(X)	20
Shoe machine operators and tenders 8340 (SOC 51-	Percent	54.1%	7.6%	4.4%	29.2%	7.0%	0.0%	5.2%	0.0%	0.0%	0.0%	0.2%	0.0%	(X)	(X)	(X)	0.4%
Tailors dressmakers and sewers 8350 (SOC 51-6050)	Total both sexes																
Tailors dressmakers and sewers 8350 (SOC 51-6050)	Number	90 355	11 275	8 710	45 740	6 300	205	17 450	80	80	105	145	25	(X)	(X)	(X)	235
Tailors dressmakers and sewers 8350 (SOC 51-6050)	Percent	100.0%	12.5%	9.6%	50.6%	7.0%	0.2%	19.3%	0.1%	0.1%	0.1%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Tailors, dressmakers, and sewers 8350 (SOC 51-6050)	Male																
Tailors dressmakers and sewers 8350 (SOC 51-6050)	Number	20 690	3 055	3 020	8 060	1 540	15	4 925	0	0	0	0	0	(X)	(X)	(X)	75
Tailors dressmakers and sewers 8350 (SOC 51-6050)	Percent	22.9%	3.4%	3.3%	8.9%	1.7%	0.0%	5.5%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Tailors, dressmakers, and sewers 8350 (SOC 51-6050)	Female																
Tailors dressmakers and sewers 8350 (SOC 51-6050)	Number	69 665	8 220	5 690	37 680	4 755	195	12 525	80	80	105	145	25	(X)	(X)	(X)	160
Tailors dressmakers and sewers 8350 (SOC 51-6050)	Percent	77.1%	9.1%	6.3%	41.7%	5.3%	0.2%	13.9%	0.1%	0.1%	0.1%	0.2%	0.0%	(X)	(X)	(X)	0.2%
Textile bleaching and dyeing and cutting machine setters	Total both sexes																
Textile bleaching and dyeing and cutting machine setters	Number	14 660	2 310	1 920	7 565	1 835	85	720	25	25	120	4	20	(X)	(X)	(X)	30
Textile bleaching and dyeing and cutting machine setters	Percent	100.0%	15.8%	13.1%	51.6%	12.5%	0.6%	4.9%	0.2%	0.2%	0.8%	0.0%	0.1%	(X)	(X)	(X)	0.2%
Textile bleaching and dyeing and cutting machine setters	Male																
Textile bleaching and dyeing and cutting machine setters	Number	8 805	1 485	1 135	4 175	1 285	60	545	25	25	50	0	0	(X)	(X)	(X)	15
Textile bleaching and dyeing and cutting machine setters	Percent	60.1%	10.1%	7.7%	28.5%	8.8%	0.4%	3.7%	0.2%	0.2%	0.3%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Textile bleaching and dyeing and cutting machine setters	Female																
Textile bleaching and dyeing and cutting machine setters	Number	5 860	825	785	3 385	550	25	175	0	0	75	4	20	(X)	(X)	(X)	15
Textile bleaching and dyeing and cutting machine setters	Percent	40.0%	5.6%	5.4%	23.1%	3.8%	0.2%	1.2%	0.0%	0.0%	0.5%	0.0%	0.1%	(X)	(X)	(X)	0.1%
Textile knitting and weaving machine setters operators	Total both sexes																
Textile knitting and weaving machine setters operators	Number	13 535	1 205	735	7 880	2 555	245	735	0	0	120	10	0	(X)	(X)	(X)	45
Textile knitting and weaving machine setters operators	Percent	100.0%	8.9%	5.4%	58.2%	18.9%	1.8%	5.4%	0.0%	0.0%	0.9%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Textile knitting and weaving machine setters operators	Male																
Textile knitting and weaving machine setters operators	Number	4 950	625	395	2 615	885	70	275	0	0	80	0	0	(X)	(X)	(X)	0
Textile knitting and weaving machine setters operators	Percent	36.6%	4.6%	2.9%	19.3%	6.5%	0.5%	2.0%	0.0%	0.0%	0.6%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Textile knitting and weaving machine setters operators	Female																
Textile knitting and weaving machine setters operators	Number	8 585	580	340	5 265	1 670	175	460	0	0	40	10	0	(X)	(X)	(X)	45
Textile knitting and weaving machine setters operators	Percent	63.4%	4.3%	2.5%	38.9%	12.3%	1.3%	3.4%	0.0%	0.0%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Textile winding twisting and drawing out machine setters	Total both sexes																
Textile winding, twisting, and drawing out machine setters	Number	18,420	1,300	1,660	9,860	4,865	95	465	0	0	90	35	0	(X)	(X)	(X)	50
Textile winding twisting and drawing out machine setters	Percent	100.0%	7.1%	9.0%	53.5%	26.4%	0.5%	2.5%	0.0%	0.0%	0.5%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Textile winding twisting and drawing out machine setters	Male																
Textile winding, twisting, and drawing out machine setters,	Number	6,305	665	780	3,415	1,240	40	115	0	0	15	0	0	(X)	(X)	(X)	25
Textile winding twisting and drawing out machine setters	Percent	34.2%	3.6%	4.2%	18.5%	6.7%	0.2%	0.6%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Textile winding twisting and drawing out machine setters	Female																
Textile winding twisting and drawing out machine setters	Number	12 120	635	880	6 445	3 625	50	350	0	0	75	35	0	(X)	(X)	(X)	25
Textile winding twisting and drawing out machine setters	Percent	65.8%	3.4%	4.8%	35.0%	19.7%	0.3%	1.9%	0.0%	0.0%	0.4%	0.2%	0.0%	(X)	(X)	(X)	0.1%
Upholsterers 8450 (SOC 51-6093)	Total both sexes																
Upholsterers 8450 (SOC 51-6093)	Number	44 105	6 310	5 990	26 765	3 475	275	855	20	75	170	55	15	(X)	(X)	(X)	100
Upholsterers 8450 (SOC 51-6093)	Percent	100.0%	14.3%	13.6%	60.7%	7.9%	0.6%	1.9%	0.0%	0.2%	0.4%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Upholsterers 8450 (SOC 51-6093)	Male																
Upholsterers 8450 (SOC 51-6093)	Number	36 470	5 645	5 510	20 975	3 035	240	700	20	65	135	25	15	(X)	(X)	(X)	100

Upholsterers 8450 (SOC 51-6093)	Percent	82.7%	12.8%	12.5%	47.6%	6.9%	0.5%	1.6%	0.0%	0.1%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Upholsterers 8450 (SOC 51-6093)	Female																
Upholsterers 8450 (SOC 51-6093)	Number	7 635	665	480	5 790	440	30	155	0	15	30	25	0	(X)	(X)	(X)	0
Upholsterers 8450 (SOC 51-6093)	Percent	17.3%	1.5%	1.1%	13.1%	1.0%	0.1%	0.4%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.0%
Miscellaneous textile apparel and furnishings workers	Total both sexes																
Miscellaneous textile apparel and furnishings workers	Number	29 665	3 335	3 165	15 170	5 195	95	2 390	50	4	100	35	0	(X)	(X)	(X)	125
Miscellaneous textile apparel and furnishings workers	Percent	100.0%	11.2%	10.7%	51.1%	17.5%	0.3%	8.1%	0.2%	0.0%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.4%
Miscellaneous textile apparel and furnishings workers	Male																
Miscellaneous textile apparel and furnishings workers	Number	15 930	1 985	1 380	8 635	2 920	80	790	15	4	75	25	0	(X)	(X)	(X)	25
Miscellaneous textile apparel and furnishings workers	Percent	53.7%	6.7%	4.7%	29.1%	9.8%	0.3%	2.7%	0.1%	0.0%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Miscellaneous textile apparel and furnishings workers	Female																
Miscellaneous textile apparel and furnishings workers	Number	13 735	1 350	1 785	6 535	2 275	20	1 600	35	0	25	10	0	(X)	(X)	(X)	105
Miscellaneous textile apparel and furnishings workers	Percent	46.3%	4.6%	6.0%	22.0%	7.7%	0.1%	5.4%	0.1%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.4%
Cabinetmakers and bench carpenters 8500 (SOC 51-	Total both sexes																
Cabinetmakers and bench carpenters 8500 (SOC 51-	Number	75 220	7 855	5 410	56 515	3 030	290	1 415	40	20	210	155	0	(X)	(X)	(X)	280
Cabinetmakers and bench carpenters 8500 (SOC 51-	Percent	100.0%	10.4%	7.2%	75.1%	4.0%	0.4%	1.9%	0.1%	0.0%	0.3%	0.2%	0.0%	(X)	(X)	(X)	0.4%
Cabinetmakers and bench carpenters 8500 (SOC 51-	Male																
Cabinetmakers and bench carpenters 8500 (SOC 51-	Number	70 525	7 185	5 050	53 325	2 645	290	1 345	20	20	210	155	0	(X)	(X)	(X)	280
Cabinetmakers and bench carpenters 8500 (SOC 51-	Percent	93.8%	9.6%	6.7%	70.9%	3.5%	0.4%	1.8%	0.0%	0.0%	0.3%	0.2%	0.0%	(X)	(X)	(X)	0.4%
Cabinetmakers and bench carpenters 8500 (SOC 51-	Female																
Cabinetmakers and bench carpenters 8500 (SOC 51-	Number	4 690	670	360	3 185	385	4	70	20	0	0	0	0	(X)	(X)	(X)	0
Cabinetmakers and bench carpenters 8500 (SOC 51-	Percent	6.2%	0.9%	0.5%	4.2%	0.5%	0.0%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Furn ture finishers 8510 (SOC 51-7021)	Total both sexes																
Furn ture finishers 8510 (SOC 51-7021)	Number	21 585	2 750	2 510	14 075	1 395	75	385	0	40	165	75	0	(X)	(X)	(X)	115
Furn ture finishers 8510 (SOC 51-7021)	Percent	100.0%	12.7%	11.6%	65.2%	6.5%	0.3%	1.8%	0.0%	0.2%	0.8%	0.3%	0.0%	(X)	(X)	(X)	0.5%
Furn ture finishers 8510 (SOC 51-7021)	Male																
Furn ture finishers 8510 (SOC 51-7021)	Number	17 175	2 215	2 075	11 125	1 050	55	295	0	40	145	65	0	(X)	(X)	(X)	115
Furn ture finishers 8510 (SOC 51-7021)	Percent	79.6%	10.3%	9.6%	51.5%	4.9%	0.3%	1.4%	0.0%	0.2%	0.7%	0.3%	0.0%	(X)	(X)	(X)	0.5%
Furn ture finishers 8510 (SOC 51-7021)	Female																
Furn ture finishers 8510 (SOC 51-7021)	Number	4 410	535	440	2 955	345	20	90	0	0	25	10	0	(X)	(X)	(X)	0
Furn ture finishers 8510 (SOC 51-7021)	Percent	20.4%	2.5%	2.0%	13.7%	1.6%	0.1%	0.4%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Sawing machine setters operators and tenders wood	Total both sexes																
Sawing machine setters operators and tenders wood	Number	43 895	3 685	4 205	30 705	3 915	470	550	0	4	280	0	0	(X)	(X)	(X)	75
Sawing machine setters operators and tenders wood	Percent	100.0%	8.4%	9.6%	70.0%	8.9%	1.1%	1.3%	0.0%	0.0%	0.6%	0.0%	0.0%	(X)	(X)	(X)	0.2%
Sawing machine setters operators and tenders wood	Male																
Sawing machine setters operators and tenders wood	Number	38 710	3 055	3 750	27 355	3 465	430	390	0	4	225	0	0	(X)	(X)	(X)	35
Sawing machine setters operators and tenders wood	Percent	88.2%	7.0%	8.5%	62.3%	7.9%	1.0%	0.9%	0.0%	0.0%	0.5%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Sawing machine setters operators and tenders wood	Female																
Sawing machine setters operators and tenders wood	Number	5 185	630	455	3 355	445	45	160	0	0	60	0	0	(X)	(X)	(X)	40
Sawing machine setters operators and tenders wood	Percent	11.8%	1.4%	1.0%	7.6%	1.0%	0.1%	0.4%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Woodworking machine setters operators and tenders	Total both sexes																
Woodworking machine setters operators and tenders	Number	33 120	3 960	3 055	21 500	3 110	260	470	40	75	365	45	50	(X)	(X)	(X)	185
Woodworking machine setters operators and tenders	Percent	100.0%	12.0%	9.2%	64.9%	9.4%	0.8%	1.4%	0.1%	0.2%	1.1%	0.1%	0.2%	(X)	(X)	(X)	0.6%
Woodworking machine setters operators and tenders	Male																
Woodworking machine setters operators and tenders	Number	26 065	3 010	2 340	17 315	2 230	205	325	40	75	245	45	50	(X)	(X)	(X)	185
Woodworking machine setters operators and tenders	Percent	78.7%	9.1%	7.1%	52.3%	6.7%	0.6%	1.0%	0.1%	0.2%	0.7%	0.1%	0.2%	(X)	(X)	(X)	0.6%
Woodworking machine setters operators and tenders	Female																
Woodworking machine setters operators and tenders	Number	7 055	950	715	4 185	885	55	145	4	0	120	0	0	(X)	(X)	(X)	0
Woodworking machine setters operators and tenders	Percent	21.3%	2.9%	2.2%	12.6%	2.7%	0.2%	0.4%	0.0%	0.0%	0.4%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Miscellaneous woodworkers including model makers and	Total both sexes																
Miscellaneous woodworkers including model makers and	Number	32,525	1,935	1,485	25,675	1,535	505	675	35	75	330	130	40	(X)	(X)	(X)	105
Miscellaneous woodworkers including model makers and	Percent	100.0%	5.9%	4.6%	78.9%	4.7%	1.6%	2.1%	0.1%	0.2%	1.0%	0.4%	0.1%	(X)	(X)	(X)	0.3%
Miscellaneous woodworkers including model makers and	Male																
Miscellaneous woodworkers, including model makers and	Number	29,560	1,615	1,335	23,540	1,450	465	520	35	75	260	120	40	(X)	(X)	(X)	105
Miscellaneous woodworkers including model makers and	Percent	90.9%	5.0%	4.1%	72.4%	4.5%	1.4%	1.6%	0.1%	0.2%	0.8%	0.4%	0.1%	(X)	(X)	(X)	0.3%
Miscellaneous woodworkers including model makers and	Female																
Miscellaneous woodworkers including model makers and	Number	2 965	325	150	2 135	85	40	155	0	0	65	10	0	(X)	(X)	(X)	0
Miscellaneous woodworkers including model makers and	Percent	9.1%	1.0%	0.5%	6.6%	0.3%	0.1%	0.5%	0.0%	0.0%	0.2%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Power plant operators distributors and dispatchers 8600	Total both sexes																
Power plant operators distributors and dispatchers 8600	Number	47 660	1 900	675	39 790	3 300	790	460	0	90	355	145	15	(X)	(X)	(X)	140
Power plant operators distributors and dispatchers 8600	Percent	100.0%	4.0%	1.4%	83.5%	6.9%	1.7%	1.0%	0.0%	0.2%	0.7%	0.3%	0.0%	(X)	(X)	(X)	0.3%
Power plant operators distributors and dispatchers 8600	Male																
Power plant operators distributors and dispatchers 8600	Number	44 335	1 750	630	37 185	2 920	730	425	0	90	340	135	15	(X)	(X)	(X)	115
Power plant operators distributors and dispatchers 8600	Percent	93.0%	3.7%	1.3%	78.0%	6.1%	1.5%	0.9%	0.0%	0.2%	0.7%	0.3%	0.0%	(X)	(X)	(X)	0.2%
Power plant operators distributors and dispatchers 8600	Female																
Power plant operators distributors and dispatchers 8600	Number	3 325	150	45	2 605	380	60	40	0	0	15	10	0	(X)	(X)	(X)	20
Power plant operators distributors and dispatchers 8600	Percent	7.0%	0.3%	0.1%	5.5%	0.8%	0.1%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Stationary engineers and bo ler operators 8610 (SOC 51-	Total both sexes																
Stationary engineers and bo ler operators 8610 (SOC 51-	Number	101 025	5 860	4 910	71 715	12 895	780	3 740	60	50	435	185	15	(X)	(X)	(X)	385
Stationary engineers and bo ler operators 8610 (SOC 51-	Percent	100.0%	5.8%	4.9%	71.0%	12.8%	0.8%	3.7%	0.1%	0.0%	0.4%	0.2%	0.0%	(X)	(X)	(X)	0.4%
Stationary engineers and bo ler operators 8610 (SOC 51-	Male																
Stationary engineers and bo ler operators 8610 (SOC 51-	Number	97 710	5 665	4 805	69 550	12 200	780	3 605	60	50	435	175	15	(X)	(X)	(X)	380
Stationary engineers and bo ler operators 8610 (SOC 51-	Percent	96.7%	5.6%	4.8%	68.8%	12.1%	0.8%	3.6%	0.1%	0.0%	0.4%	0.2%	0.0%	(X)	(X)	(X)	0.4%
Stationary engineers and bo ler operators 8610 (SOC 51-	Female																
Stationary engineers and bo ler operators 8610 (SOC 51-	Number	3 315	195	105	2 165	695	0	140	0	0	0	10	0	(X)	(X)	(X)	4
Stationary engineers and bo ler operators 8610 (SOC 51-	Percent	3.3%	0.2%	0.1%	2.1%	0.7%	0.0%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Water and wastewater treatment plant and system	Total both sexes																
Water and wastewater treatment plant and system	Number	80 770	4 075	2 750	63 025	7 565	1 135	1 020	55	80	640	190	65	(X)	(X)	(X)	170
Water and wastewater treatment plant and system	Percent	100.0%	5.0%	3.4%	78.0%	9.4%	1.4%	1.3%	0.1%	0.1%	0.8%	0.2%	0.1%	(X)	(X)	(X)	0.2%
Water and wastewater treatment plant and system	Male																
Water and wastewater treatment plant and system	Number	76 815	3 885	2 620	60 125	7 050	1 100	955	25	50	590	190	65	(X)	(X)	(X)	165
Water and wastewater treatment plant and system	Percent	95.1%	4.8%	3.2%	74.4%	8.7%	1.4%	1.2%	0.0%	0.1%	0.7%	0.2%	0.1%	(X)	(X)	(X)	0.2%
Water and wastewater treatment plant and system	Female																
Water and wastewater treatment plant and system	Number	3 955	190	130	2 900	515	35	65	30	30	55	0	0	(X)	(X)	(X)	4
Water and wastewater treatment plant and system	Percent	4.9%	0.2%	0.2%	3.6%	0.6%	0.0%	0.1%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Miscellaneous plant and system operators 8630 (SOC 51-	Total both sexes																
Miscellaneous plant and system operators 8630 (SOC 51-	Number	41 950	2 975	1 705	31 515	4 305	295	510	120	0	250	115	20	(X)	(X)	(X)	140
Miscellaneous plant and system operators 8630 (SOC 51-	Percent	100.0%	7.1%	4.1%	75.1%	10.3%	0.7%	1.2%	0.3%	0.0%	0.6%	0.3%	0.0%	(X)	(X)	(X)	0.3%
Miscellaneous plant and system operators 8630 (SOC 51-	Male																
Miscellaneous plant and system operators 8630 (SOC 51-	Number	39 520	2 870	1 595	29 840	3 905	255	495	90	0	250	105	0	(X)	(X)	(X)	115
Miscellaneous plant and system operators 8630 (SOC 51-	Percent	94.2%	6.8%	3.8%	71.1%	9.3%	0.6%	1.2%	0.2%	0.0%	0.6%	0.3%	0.0%	(X)	(X)	(X)	0.3%
Miscellaneous plant and system operators 8630 (SOC 51-	Female																
Miscellaneous plant and system operators 8630 (SOC 51-	Number	2 435	105	110	1 675	400	40	10	30	0	0	10	20	(X)	(X)	(X)	25
Miscellaneous plant and system operators 8630 (SOC 51-	Percent	5.8%	0.3%	0.3%	4.0%	1.0%	0.1%	0.0%	0.1%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Chemical processing machine setters operators and	Total both sexes																
Chemical processing machine setters operators and	Number	58 015	4 240	3 295	39 195	8 550	245	1 545	70	90	310	145	20	(X)	(X)	(X)	315
Chemical processing machine setters operators and	Percent	100.0%	7.3%	5.7%	67.6%	14.7%	0.4%	2.7%	0.1%	0.2%	0.5%	0.2%	0.0%	(X)	(X)	(X)	0.5%
Chemical processing machine setters operators and	Male																
Chemical processing machine setters operators and	Number	50 525	3 490	3 015	34 810	7 225	150	1 215	35	60	255	80	20	(X)	(X)	(X)	175
Chemical processing machine setters operators and	Percent	87.1%	6.0%	5.2%	60.0%	12.5%	0.3%	2.1%	0.1%	0.1%	0.4%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Chemical processing machine setters, operators, and	Female																
Chemical processing machine setters operators and	Number	7 490	750	280	4 385	1 325	95	330	35	30	55	65	0	(X)	(X)	(X)	140
Chemical processing machine setters operators and	Percent	12.9%	1.3%	0.5%	7.6%	2.3%	0.2%	0.6%	0.1%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Crushing, grinding, polishing, mixing, and blending workers	Total, both sexes																
Crushing grinding polishing mixing and blending workers	Number	102 845	13 105	9 625	61 320	13 865	880	2 815	60	45	690	115	95	(X)	(X)	(X)	235
Crushing grinding polishing mixing and blending workers	Percent	100.0%	12.7%	9.4%	59.6%	13.5%	0.9%	2.7%	0.1%	0.0%	0.7%	0.1%	0.1%	(X)	(X)	(X)	0.2%
Crushing grinding polishing mixing and blending workers	Male																
Crushing grinding polishing mixing and blending workers	Number	91 030	11 790	8 730	53 970	12 185	760	2 420	60	45	660	95	95	(X)	(X)	(X)	220
Crushing grinding polishing mixing and blending workers	Percent	88.5%	11.5%	8.5%	52.5%	11.8%	0.7%	2.4%	0.1%	0.0%	0.6%	0.1%	0.1%	(X)	(X)	(X)	0.2%
Crushing grinding polishing mixing and blending workers	Female																
Crushing grinding polishing mixing and blending workers	Number	11 815	1 315	895	7 355	1 675	115	395	0	0	25	20	0	(X)	(X)	(X)	15
Crushing grinding polishing mixing and blending workers	Percent	11.5%	1.3%	0.9%	7.2%	1.6%	0.1%	0.4%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Cutting workers 8710 (SOC 51-9030)	Total both sexes																
Cutting workers 8710 (SOC 51-9030)	Number	85 155	11 945	9 750	48 975	10 375	630	2 365	105	205	415	110	15	(X)	(X)	(X)	280
Cutting workers 8710 (SOC 51-9030)	Percent	100.0%	14.0%	11.4%	57.5%	12.2%	0.7%	2.8%	0.1%	0.2%	0.5%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Cutting workers 8710 (SOC 51-9030)	Male																
Cutting workers 8710 (SOC 51-9030)	Number	63 905	9 045	7 365	37 165	7 600	445	1 460	95	150	270	70	15	(X)	(X)	(X)	230
Cutting workers 8710 (SOC 51-9030)	Percent	75.0%	10.6%	8.6%	43.6%	8.9%	0.5%	1.7%	0.1%	0.2%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Cutting workers 8710 (SOC 51-9030)	Female																
Cutting workers 8710 (SOC 51-9030)	Number	21 250	2 900	2 385	11 805	2 775	185	905	10	55	140	35	0	(X)	(X)	(X)	50
Cutting workers 8710 (SOC 51-9030)	Percent	25.0%	3.4%	2.8%	13.9%	3.3%	0.2%	1.1%	0.0%	0.1%	0.2%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Extruding forming pressing and compacting machine	Total both sexes																
Extruding forming pressing and compacting machine	Number	38 045	3 090	2 290	26 025	5 425	205	685	4	30	155	0	0	(X)	(X)	(X)	140
Extruding forming pressing and compacting machine	Percent	100.0%	8.1%	6.0%	68.4%	14.3%	0.5%	1.8%	0.0%	0.1%	0.4%	0.0%	0.0%	(X)	(X)	(X)	0.4%
Extruding forming pressing and compacting machine	Male																
Extruding, forming, pressing, and compacting machine	Number	30,900	2,825	1,735	21,165	4,235	165	465	4	30	140	0	0	(X)	(X)	(X)	140
Extruding forming pressing and compacting machine	Percent	81.2%	7.4%	4.6%	55.6%	11.1%	0.4%	1.2%	0.0%	0.1%	0.4%	0.0%	0.0%	(X)	(X)	(X)	0.4%
Extruding forming pressing and compacting machine	Female																
Extruding, forming, pressing, and compacting machine	Number	7,145	270	550	4,860	1,185	40	220	0	0	15	0	0	(X)	(X)	(X)	0
Extruding forming pressing and compacting machine	Percent	18.8%	0.7%	1.4%	12.8%	3.1%	0.1%	0.6%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Furnace k ln oven drier and kettle operators and tenders	Total both sexes																
Furnace k ln oven drier and kettle operators and tenders	Number	13 080	750	515	9 475	1 795	175	150	10	25	125	30	0	(X)	(X)	(X)	35
Furnace k ln oven drier and kettle operators and tenders	Percent	100.0%	5.7%	3.9%	72.4%	13.7%	1.3%	1.1%	0.1%	0.2%	1.0%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Furnace k ln oven drier and kettle operators and tenders	Male																
Furnace k ln oven drier and kettle operators and tenders	Number	11 075	625	470	8 200	1 400	115	85	10	25	115	20	0	(X)	(X)	(X)	15
Furnace k ln oven drier and kettle operators and tenders	Percent	84.7%	4.8%	3.6%	62.7%	10.7%	0.9%	0.6%	0.1%	0.2%	0.9%	0.2%	0.0%	(X)	(X)	(X)	0.1%
Furnace k ln oven drier and kettle operators and tenders	Female																
Furnace k ln oven drier and kettle operators and tenders	Number	2 005	125	45	1 275	395	60	65	0	0	10	10	0	(X)	(X)	(X)	15

Furnace, kiln, oven, drier, and kettle operators and tenders	Percent	15.3%	1.0%	0.3%	9.7%	3.0%	0.5%	0.5%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Inspectors testers sorters samplers and weighers 8740	Total both sexes																
Inspectors testers sorters samplers and weighers 8740	Number	826 110	73 870	55 440	528 875	100 270	3 855	51 130	1 530	1 065	4 115	1 665	505	(X)	(X)	(X)	3 790
Inspectors, testers, sorters, samplers, and weighers 8740	Percent	100.0%	8.9%	6.7%	64.0%	12.1%	0.5%	6.2%	0.2%	0.1%	0.5%	0.2%	0.1%	(X)	(X)	(X)	0.5%
Inspectors testers sorters samplers and weighers 8740	Male																
Inspectors testers sorters samplers and weighers 8740	Number	491 880	37 350	26 935	342 075	49 090	2 195	26 285	965	680	2 685	1 095	285	(X)	(X)	(X)	2 235
Inspectors testers sorters samplers and weighers 8740	Percent	59.5%	4.5%	3.3%	41.4%	5.9%	0.3%	3.2%	0.1%	0.1%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Inspectors testers sorters samplers and weighers 8740	Female																
Inspectors testers sorters samplers and weighers 8740	Number	334 230	36 520	28 505	186 800	51 175	1 660	24 845	565	390	1 435	570	220	(X)	(X)	(X)	1 550
Inspectors testers sorters samplers and weighers 8740	Percent	40.5%	4.4%	3.5%	22.6%	6.2%	0.2%	3.0%	0.1%	0.0%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Jewelers and precious stone and metal workers 8750	Total both sexes																
Jewelers and precious stone and metal workers 8750	Number	43 730	5 130	4 070	24 455	1 505	2 420	5 570	30	15	190	110	10	(X)	(X)	(X)	225
Jewelers and precious stone and metal workers 8750	Percent	100.0%	11.7%	9.3%	55.9%	3.4%	5.5%	12.7%	0.1%	0.0%	0.4%	0.3%	0.0%	(X)	(X)	(X)	0.5%
Jewelers and precious stone and metal workers 8750	Male																
Jewelers and precious stone and metal workers 8750	Number	28 100	3 425	2 980	15 335	835	1 550	3 650	30	0	95	70	0	(X)	(X)	(X)	140
Jewelers and precious stone and metal workers 8750	Percent	64.3%	7.8%	6.8%	35.1%	1.9%	3.5%	8.3%	0.1%	0.0%	0.2%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Jewelers and precious stone and metal workers 8750	Female																
Jewelers and precious stone and metal workers 8750	Number	15 630	1 700	1 095	9 120	670	875	1 920	0	15	95	45	10	(X)	(X)	(X)	85
Jewelers and precious stone and metal workers 8750	Percent	35.7%	3.9%	2.5%	20.9%	1.5%	2.0%	4.4%	0.0%	0.0%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Medical dental and ophthalmic laboratory technicians	Total both sexes																
Medical dental and ophthalmic laboratory technicians	Number	89 835	8 255	4 455	61 250	5 415	260	8 860	135	135	195	385	30	(X)	(X)	(X)	465
Medical dental and ophthalmic laboratory technicians	Percent	100.0%	9.2%	5.0%	68.2%	6.0%	0.3%	9.9%	0.2%	0.2%	0.2%	0.4%	0.0%	(X)	(X)	(X)	0.5%
Medical dental and ophthalmic laboratory technicians	Male																
Medical dental and ophthalmic laboratory technicians	Number	44 780	4 365	2 610	29 080	2 610	35	5 400	60	90	85	130	0	(X)	(X)	(X)	315
Medical dental and ophthalmic laboratory technicians	Percent	49.8%	4.9%	2.9%	32.4%	2.9%	0.0%	6.0%	0.1%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.4%
Medical, dental, and ophthalmic laboratory technicians	Female																
Medical dental and ophthalmic laboratory technicians	Number	45 055	3 890	1 845	32 170	2 805	225	3 460	75	45	110	255	30	(X)	(X)	(X)	150
Medical dental and ophthalmic laboratory technicians	Percent	50.2%	4.3%	2.1%	35.8%	3.1%	0.3%	3.9%	0.1%	0.1%	0.1%	0.3%	0.0%	(X)	(X)	(X)	0.2%
Packaging and f lling machine operators and tenders 8800	Total, both sexes																
Packaging and f lling machine operators and tenders 8800	Number	300 120	63 325	53 665	106 400	56 495	1 545	14 545	625	295	910	380	230	(X)	(X)	(X)	1 710
Packaging and f lling machine operators and tenders 8800	Percent	100.0%	21.1%	17.9%	35.5%	18.8%	0.5%	4.8%	0.2%	0.1%	0.3%	0.1%	0.1%	(X)	(X)	(X)	0.6%
Packaging and f lling machine operators and tenders 8800	Male																
Packaging and f lling machine operators and tenders 8800	Number	127 765	25 640	19 530	50 795	23 555	730	5 535	445	195	410	155	130	(X)	(X)	(X)	650
Packaging and f lling machine operators and tenders 8800	Percent	42.6%	8.5%	6.5%	16.9%	7.8%	0.2%	1.8%	0.1%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Packaging and f lling machine operators and tenders 8800	Female																
Packaging and f lling machine operators and tenders 8800	Number	172 355	37 685	34 135	55 605	32 940	815	9 010	185	100	495	225	100	(X)	(X)	(X)	1 060
Packaging and f lling machine operators and tenders 8800	Percent	57.4%	12.6%	11.4%	18.5%	11.0%	0.3%	3.0%	0.1%	0.0%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.4%
Painting workers 8810 (SOC 51-9120)	Total both sexes																
Painting workers 8810 (SOC 51-9120)	Number	176 495	28 740	21 110	101 850	16 830	825	4 140	105	420	1 200	265	90	(X)	(X)	(X)	920
Painting workers 8810 (SOC 51-9120)	Percent	100.0%	16.3%	12.0%	57.7%	9.5%	0.5%	2.3%	0.1%	0.2%	0.7%	0.2%	0.1%	(X)	(X)	(X)	0.5%
Painting workers 8810 (SOC 51-9120)	Male																
Painting workers 8810 (SOC 51-9120)	Number	153 610	25 830	19 040	88 265	13 735	750	3 265	90	355	1 070	245	65	(X)	(X)	(X)	900
Painting workers 8810 (SOC 51-9120)	Percent	87.0%	14.6%	10.8%	50.0%	7.8%	0.4%	1.8%	0.1%	0.2%	0.6%	0.1%	0.0%	(X)	(X)	(X)	0.5%
Painting workers 8810 (SOC 51-9120)	Female																
Painting workers 8810 (SOC 51-9120)	Number	22 890	2 915	2 070	13 590	3 095	75	875	15	65	130	20	25	(X)	(X)	(X)	15
Painting workers 8810 (SOC 51-9120)	Percent	13.0%	1.7%	1.2%	7.7%	1.8%	0.0%	0.5%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Photographic process workers and processing machine	Total both sexes																
Photographic process workers and processing machine	Number	66 460	5 085	3 830	43 050	8 615	190	4 145	100	205	360	355	25	(X)	(X)	(X)	495
Photographic process workers and processing machine	Percent	100.0%	7.7%	5.8%	64.8%	13.0%	0.3%	6.2%	0.2%	0.3%	0.5%	0.5%	0.0%	(X)	(X)	(X)	0.7%
Photographic process workers and processing machine	Male																
Photographic process workers and processing machine	Number	27,040	2,145	1,435	17,610	2,905	60	2,335	4	65	65	175	10	(X)	(X)	(X)	230
Photographic process workers and processing machine	Percent	40.7%	3.2%	2.2%	26.5%	4.4%	0.1%	3.5%	0.0%	0.1%	0.1%	0.3%	0.0%	(X)	(X)	(X)	0.3%
Photographic process workers and processing machine	Female																
Photographic process workers and processing machine	Number	39,415	2,940	2,395	25,440	5,715	130	1,810	95	140	295	180	15	(X)	(X)	(X)	260
Photographic process workers and processing machine	Percent	59.3%	4.4%	3.6%	38.3%	8.6%	0.2%	2.7%	0.1%	0.2%	0.4%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Adhesive bonding machine operators and tenders 8850	Total both sexes																
Adhesive bonding machine operators and tenders 8850	Number	15 150	1 995	1 455	8 635	2 135	85	625	40	4	130	20	0	(X)	(X)	(X)	30
Adhesive bonding machine operators and tenders 8850	Percent	100.0%	13.2%	9.6%	57.0%	14.1%	0.6%	4.1%	0.3%	0.0%	0.9%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Adhesive bonding machine operators and tenders 8850	Male																
Adhesive bonding machine operators and tenders 8850	Number	8 715	1 055	970	5 040	1 060	20	420	40	4	55	20	0	(X)	(X)	(X)	30
Adhesive bonding machine operators and tenders 8850	Percent	57.5%	7.0%	6.4%	33.3%	7.0%	0.1%	2.8%	0.3%	0.0%	0.4%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Adhesive bonding machine operators and tenders 8850	Female																
Adhesive bonding machine operators and tenders 8850	Number	6 435	935	485	3 600	1 070	65	205	0	0	75	0	0	(X)	(X)	(X)	0
Adhesive bonding machine operators and tenders 8850	Percent	42.5%	6.2%	3.2%	23.8%	7.1%	0.4%	1.4%	0.0%	0.0%	0.5%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Cleaning, washing, and metal pickling equipment operators and tenders 8860 (SOC 51-9192)	Total, both sexes																
Cleaning washing and metal pickling equipment operators	Number	10 385	2 075	1 310	5 360	1 315	20	185	60	10	35	0	0	(X)	(X)	(X)	15
Cleaning washing and metal pickling equipment operators	Percent	100.0%	20.0%	12.6%	51.6%	12.7%	0.2%	1.8%	0.6%	0.1%	0.3%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Cleaning washing and metal pickling equipment operators	Male																
Cleaning washing and metal pickling equipment operators	Number	7 540	1 330	965	3 875	1 170	20	85	60	0	30	0	0	(X)	(X)	(X)	10
Cleaning washing and metal pickling equipment operators	Percent	72.6%	12.8%	9.3%	37.3%	11.3%	0.2%	0.8%	0.6%	0.0%	0.3%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Cleaning washing and metal pickling equipment operators	Female																
Cleaning washing and metal pickling equipment operators	Number	2 845	745	345	1 485	150	0	100	0	10	4	0	0	(X)	(X)	(X)	4
Cleaning washing and metal pickling equipment operators	Percent	27.4%	7.2%	3.3%	14.3%	1.4%	0.0%	1.0%	0.0%	0.1%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Etchers and engravers 8910 (SOC 51-9194)	Total both sexes																
Etchers and engravers 8910 (SOC 51-9194)	Number	11 295	810	515	8 620	620	180	385	0	15	65	60	0	(X)	(X)	(X)	30
Etchers and engravers 8910 (SOC 51-9194)	Percent	100.0%	7.2%	4.6%	76.3%	5.5%	1.6%	3.4%	0.0%	0.1%	0.6%	0.5%	0.0%	(X)	(X)	(X)	0.3%
Etchers and engravers 8910 (SOC 51-9194)	Male																
Etchers and engravers 8910 (SOC 51-9194)	Number	7 095	540	265	5 435	330	150	315	0	0	10	40	0	(X)	(X)	(X)	4
Etchers and engravers 8910 (SOC 51-9194)	Percent	62.8%	4.8%	2.3%	48.1%	2.9%	1.3%	2.8%	0.0%	0.0%	0.1%	0.4%	0.0%	(X)	(X)	(X)	0.0%
Etchers and engravers 8910 (SOC 51-9194)	Female																
Etchers and engravers 8910 (SOC 51-9194)	Number	4 200	265	250	3 185	290	30	75	0	15	50	15	0	(X)	(X)	(X)	25
Etchers and engravers 8910 (SOC 51-9194)	Percent	37.2%	2.3%	2.2%	28.2%	2.6%	0.3%	0.7%	0.0%	0.1%	0.4%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Molders, shapers, and casters, except metal and plastic	Total, both sexes																
Molders shapers and casters except metal and plastic	Number	37 610	5 065	3 825	24 700	2 190	250	1 015	10	70	205	130	10	(X)	(X)	(X)	145
Molders shapers and casters except metal and plastic	Percent	100.0%	13.5%	10.2%	65.7%	5.8%	0.7%	2.7%	0.0%	0.2%	0.5%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Molders shapers and casters except metal and plastic	Male																
Molders shapers and casters except metal and plastic	Number	32 155	4 580	3 510	20 835	1 755	220	770	10	50	185	100	10	(X)	(X)	(X)	125
Molders shapers and casters except metal and plastic	Percent	85.5%	12.2%	9.3%	55.4%	4.7%	0.6%	2.0%	0.0%	0.1%	0.5%	0.3%	0.0%	(X)	(X)	(X)	0.3%
Molders shapers and casters except metal and plastic	Female																
Molders shapers and casters except metal and plastic	Number	5 455	485	315	3 865	435	35	245	0	15	20	25	0	(X)	(X)	(X)	20
Molders shapers and casters except metal and plastic	Percent	14.5%	1.3%	0.8%	10.3%	1.2%	0.1%	0.7%	0.0%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Paper goods machine setters operators and tenders 8930	Total both sexes																
Paper goods machine setters operators and tenders 8930	Number	38 230	3 745	3 425	22 470	6 715	345	1 010	75	80	230	55	0	(X)	(X)	(X)	75
Paper goods machine setters operators and tenders 8930	Percent	100.0%	9.8%	9.0%	58.8%	17.6%	0.9%	2.6%	0.2%	0.2%	0.6%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Paper goods machine setters operators and tenders 8930	Male																
Paper goods machine setters operators and tenders 8930	Number	27 330	2 470	1 800	17 335	4 300	255	690	75	80	220	45	0	(X)	(X)	(X)	60
Paper goods machine setters operators and tenders 8930	Percent	71.5%	6.5%	4.7%	45.3%	11.2%	0.7%	1.8%	0.2%	0.2%	0.6%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Paper goods machine setters operators and tenders 8930	Female																
Paper goods machine setters operators and tenders 8930	Number	10 900	1 275	1 625	5 135	2 420	90	320	0	0	10	10	0	(X)	(X)	(X)	15
Paper goods machine setters operators and tenders 8930	Percent	28.5%	3.3%	4.3%	13.4%	6.3%	0.2%	0.8%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Tire builders 8940 (SOC 51-9197)	Total both sexes																
Tire builders 8940 (SOC 51-9197)	Number	17 100	580	705	11 215	3 755	145	315	110	10	210	30	0	(X)	(X)	(X)	25
Tire builders 8940 (SOC 51-9197)	Percent	100.0%	3.4%	4.1%	65.6%	22.0%	0.8%	1.8%	0.6%	0.1%	1.2%	0.2%	0.0%	(X)	(X)	(X)	0.1%
Tire builders 8940 (SOC 51-9197)	Male																
Tire builders 8940 (SOC 51-9197)	Number	15,365	530	630	10,415	3,000	95	315	110	10	210	30	0	(X)	(X)	(X)	25
Tire builders 8940 (SOC 51-9197)	Percent	89.9%	3.1%	3.7%	60.9%	17.5%	0.6%	1.8%	0.6%	0.1%	1.2%	0.2%	0.0%	(X)	(X)	(X)	0.1%
Tire builders 8940 (SOC 51-9197)	Female																
Tire builders 8940 (SOC 51-9197)	Number	1,735	50	75	800	760	50	0	0	0	4	0	0	(X)	(X)	(X)	0
Tire builders 8940 (SOC 51-9197)	Percent	10.1%	0.3%	0.4%	4.7%	4.4%	0.3%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Helpers--production workers 8950 (SOC 51-9198)	Total both sexes																
Helpers--production workers 8950 (SOC 51-9198)	Number	57 025	10 785	9 095	25 520	7 010	570	3 160	105	115	290	80	80	(X)	(X)	(X)	210
Helpers--production workers 8950 (SOC 51-9198)	Percent	100.0%	18.9%	15.9%	44.8%	12.3%	1.0%	5.5%	0.2%	0.2%	0.5%	0.1%	0.1%	(X)	(X)	(X)	0.4%
Helpers--production workers 8950 (SOC 51-9198)	Male																
Helpers--production workers 8950 (SOC 51-9198)	Number	43 145	8 715	7 155	19 450	5 340	365	1 580	30	80	235	40	15	(X)	(X)	(X)	140
Helpers--production workers 8950 (SOC 51-9198)	Percent	75.7%	15.3%	12.5%	34.1%	9.4%	0.6%	2.8%	0.1%	0.1%	0.4%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Helpers--production workers 8950 (SOC 51-9198)	Female																
Helpers--production workers 8950 (SOC 51-9198)	Number	13 885	2 070	1 945	6 070	1 670	205	1 580	75	35	50	45	65	(X)	(X)	(X)	70
Helpers--production workers 8950 (SOC 51-9198)	Percent	24.3%	3.6%	3.4%	10.6%	2.9%	0.4%	2.8%	0.1%	0.1%	0.1%	0.1%	0.1%	(X)	(X)	(X)	0.1%
Other production workers including semiconductor	Total both sexes																
Other production workers including semiconductor	Number	1 195 140	140 410	120 635	679 620	181 255	6 560	52 105	1 815	1 775	4 420	1 655	715	(X)	(X)	(X)	4 170
Other production workers including semiconductor	Percent	100.0%	11.7%	10.1%	56.9%	15.2%	0.5%	4.4%	0.2%	0.1%	0.4%	0.1%	0.1%	(X)	(X)	(X)	0.3%
Other production workers including semiconductor	Male																
Other production workers including semiconductor	Number	835 125	96 365	81 610	489 685	121 400	4 570	31 245	1 285	1 145	3 265	1 120	355	(X)	(X)	(X)	3 080
Other production workers including semiconductor	Percent	69.9%	8.1%	6.8%	41.0%	10.2%	0.4%	2.6%	0.1%	0.1%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Other production workers including semiconductor	Female																
Other production workers including semiconductor	Number	360 015	44 040	39 025	189 935	59 855	1 995	20 860	530	630	1 155	535	365	(X)	(X)	(X)	1 090
Other production workers including semiconductor	Percent	30.1%	3.7%	3.3%	15.9%	5.0%	0.2%	1.7%	0.0%	0.1%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Supervisors of transportation and material moving workers	Total both sexes																
Supervisors of transportation and material moving workers	Number	248 415	21 455	13 965	164 210	33 960	1 540	8 905	915	525	1 010	370	165	(X)	(X)	(X)	1 395
Supervisors of transportation and material moving workers	Percent	100.0%	8.6%	5.6%	66.1%	13.7%	0.6%	3.6%	0.4%	0.2%	0.4%	0.1%	0.1%	(X)	(X)	(X)	0.6%
Supervisors of transportation and material moving workers	Male																
Supervisors of transportation and material moving workers	Number	197 365	17 435	11 325	132 065	25 020	1 110	6 935	720	425	775	275	110	(X)	(X)	(X)	1 170
Supervisors of transportation and material moving workers	Percent	79.4%	7.0%	4.6%	53.2%	10.1%	0.4%	2.8%	0.3%	0.2%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.5%
Supervisors of transportation and material moving workers	Female																
Supervisors of transportation and material moving workers	Number	51 055	4 020	2 640	32 145	8 940	430	1 970	195	100	235	95	55	(X)	(X)	(X)	225
Supervisors of transportation and material moving workers	Percent	20.6%	1.6%	1.1%	12.9%	3.6%	0.2%	0.8%	0.1%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%

Aircraft pilots and flight engineers 9030 (SOC 53-2010)	Total, both sexes																
Aircraft pilots and flight engineers 9030 (SOC 53-2010)	Number	133 640	4 035	1 385	121 020	2 920	500	2 045	250	120	330	480	35	(X)	(X)	(X)	520
Aircraft pilots and flight engineers 9030 (SOC 53-2010)	Percent	100.0%	3.0%	1.0%	90.6%	2.2%	0.4%	1.5%	0.2%	0.1%	0.2%	0.4%	0.0%	(X)	(X)	(X)	0.4%
Aircraft pilots and flight engineers 9030 (SOC 53-2010)	Male																
Aircraft pilots and flight engineers 9030 (SOC 53-2010)	Number	127 360	3 885	1 325	115 315	2 855	495	1 885	225	120	320	400	35	(X)	(X)	(X)	490
Aircraft pilots and flight engineers 9030 (SOC 53-2010)	Percent	95.3%	2.9%	1.0%	86.3%	2.1%	0.4%	1.4%	0.2%	0.1%	0.2%	0.3%	0.0%	(X)	(X)	(X)	0.4%
Aircraft pilots and flight engineers 9030 (SOC 53-2010)	Female																
Aircraft pilots and flight engineers 9030 (SOC 53-2010)	Number	6 280	150	60	5 700	65	4	160	30	0	10	75	0	(X)	(X)	(X)	30
Aircraft pilots and flight engineers 9030 (SOC 53-2010)	Percent	4.7%	0.1%	0.0%	4.3%	0.0%	0.0%	0.1%	0.0%	0.0%	0.0%	0.1%	0.0%	(X)	(X)	(X)	0.0%
Air traffic contro lers and airfield operations specialists	Total both sexes																
Air traffic contro lers and airfield operations specialists	Number	34 835	1 980	660	27 125	3 285	60	905	190	85	150	180	0	(X)	(X)	(X)	225
Air traffic contro lers and airfield operations specialists	Percent	100.0%	5.7%	1.9%	77.9%	9.4%	0.2%	2.6%	0.5%	0.2%	0.4%	0.5%	0.0%	(X)	(X)	(X)	0.6%
Air traffic contro lers and airfield operations specialists	Male																
Air traffic contro lers and airfield operations specialists	Number	28 415	1 555	510	22 380	2 680	50	635	135	80	115	130	0	(X)	(X)	(X)	150
Air traffic contro lers and airfield operations specialists	Percent	81.6%	4.5%	1.5%	64.2%	7.7%	0.1%	1.8%	0.4%	0.2%	0.3%	0.4%	0.0%	(X)	(X)	(X)	0.4%
Air traffic contro lers and airfield operations specialists	Female																
Air traffic contro lers and airfield operations specialists	Number	6 420	425	150	4 745	605	4	270	55	4	35	50	0	(X)	(X)	(X)	75
Air traffic contro lers and airfield operations specialists	Percent	18.4%	1.2%	0.4%	13.6%	1.7%	0.0%	0.8%	0.2%	0.0%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Flight attendants 9050 (SOC 53-2031)	Total both sexes																
Flight attendants 9050 (SOC 53-2031)	Number	97 660	5 740	3 380	70 550	10 115	330	4 775	565	235	395	460	85	(X)	(X)	(X)	1 030
Flight attendants 9050 (SOC 53-2031)	Percent	100.0%	5.9%	3.5%	72.2%	10.4%	0.3%	4.9%	0.6%	0.2%	0.4%	0.5%	0.1%	(X)	(X)	(X)	1.1%
Flight attendants 9050 (SOC 53-2031)	Male																
Flight attendants 9050 (SOC 53-2031)	Number	19 950	2 345	1 100	12 340	2 075	155	1 165	245	30	40	165	25	(X)	(X)	(X)	265
Flight attendants 9050 (SOC 53-2031)	Percent	20.4%	2.4%	1.1%	12.6%	2.1%	0.2%	1.2%	0.3%	0.0%	0.0%	0.2%	0.0%	(X)	(X)	(X)	0.3%
Flight attendants 9050 (SOC 53-2031)	Female																
Flight attendants 9050 (SOC 53-2031)	Number	77,710	3,395	2,280	58,210	8,035	175	3,610	320	205	355	295	60	(X)	(X)	(X)	765
Flight attendants 9050 (SOC 53-2031)	Percent	79.6%	3.5%	2.3%	59.6%	8.2%	0.2%	3.7%	0.3%	0.2%	0.4%	0.3%	0.1%	(X)	(X)	(X)	0.8%
Ambulance drivers and attendants except emergency	Total both sexes																
Ambulance drivers and attendants, except emergency	Number	13,140	1,275	910	7,495	2,785	375	195	0	15	20	10	4	(X)	(X)	(X)	65
Ambulance drivers and attendants except emergency	Percent	100.0%	9.7%	6.9%	57.0%	21.2%	2.9%	1.5%	0.0%	0.1%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.5%
Ambulance drivers and attendants except emergency	Male																
Ambulance drivers and attendants except emergency	Number	10 090	985	730	5 725	2 195	190	195	0	0	20	10	4	(X)	(X)	(X)	45
Ambulance drivers and attendants except emergency	Percent	76.8%	7.5%	5.6%	43.6%	16.7%	1.4%	1.5%	0.0%	0.0%	0.2%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Ambulance drivers and attendants except emergency	Female																
Ambulance drivers and attendants except emergency	Number	3 050	290	180	1 770	590	185	0	0	15	0	0	0	(X)	(X)	(X)	20
Ambulance drivers and attendants except emergency	Percent	23.2%	2.2%	1.4%	13.5%	4.5%	1.4%	0.0%	0.0%	0.1%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.2%
Bus drivers 9120 (SOC 53-3020)	Total both sexes																
Bus drivers 9120 (SOC 53-3020)	Number	608 595	39 840	31 865	349 750	161 280	5 095	10 875	1 370	1 095	2 865	525	955	(X)	(X)	(X)	3 075
Bus drivers 9120 (SOC 53-3020)	Percent	100.0%	6.5%	5.2%	57.5%	26.5%	0.8%	1.8%	0.2%	0.2%	0.5%	0.1%	0.2%	(X)	(X)	(X)	0.5%
Bus drivers 9120 (SOC 53-3020)	Male																
Bus drivers 9120 (SOC 53-3020)	Number	319 235	23 975	19 695	171 330	87 075	2 495	9 475	890	620	1 040	425	390	(X)	(X)	(X)	1 820
Bus drivers 9120 (SOC 53-3020)	Percent	52.5%	3.9%	3.2%	28.2%	14.3%	0.4%	1.6%	0.1%	0.1%	0.2%	0.1%	0.1%	(X)	(X)	(X)	0.3%
Bus drivers 9120 (SOC 53-3020)	Female																
Bus drivers 9120 (SOC 53-3020)	Number	289 360	15 865	12 170	178 420	74 205	2 600	1 400	480	475	1 825	100	565	(X)	(X)	(X)	1 260
Bus drivers 9120 (SOC 53-3020)	Percent	47.5%	2.6%	2.0%	29.3%	12.2%	0.4%	0.2%	0.1%	0.1%	0.3%	0.0%	0.1%	(X)	(X)	(X)	0.2%
Driver/sales workers and truck drivers 9130 (SOC 53-	Total both sexes																
Driver/sales workers and truck drivers 9130 (SOC 53-	Number	3 410 730	335 495	245 305	2 251 200	455 230	19 755	56 335	5 725	5 150	17 355	3 950	2 160	(X)	(X)	(X)	13 065
Driver/sales workers and truck drivers 9130 (SOC 53-	Percent	100.0%	9.8%	7.2%	66.0%	13.3%	0.6%	1.7%	0.2%	0.2%	0.5%	0.1%	0.1%	(X)	(X)	(X)	0.4%
Driver/sales workers and truck drivers 9130 (SOC 53-	Male																
Driver/sales workers and truck drivers 9130 (SOC 53-	Number	3 230 810	322 215	234 990	2 126 055	431 635	17 820	53 935	5 445	4 675	15 930	3 705	1 970	(X)	(X)	(X)	12 440
Driver/sales workers and truck drivers 9130 (SOC 53-	Percent	94.7%	9.4%	6.9%	62.3%	12.7%	0.5%	1.6%	0.2%	0.1%	0.5%	0.1%	0.1%	(X)	(X)	(X)	0.4%
Driver/sales workers and truck drivers 9130 (SOC 53-	Female																
Driver/sales workers and truck drivers 9130 (SOC 53-	Number	179 920	13 280	10 315	125 145	23 595	1 935	2 405	285	475	1 425	240	190	(X)	(X)	(X)	625
Driver/sales workers and truck drivers 9130 (SOC 53-	Percent	5.3%	0.4%	0.3%	3.7%	0.7%	0.1%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Taxi drivers and chauffeurs 9140 (SOC 53-3041)	Total both sexes																
Taxi drivers and chauffeurs 9140 (SOC 53-3041)	Number	335 255	28 975	26 000	151 525	84 215	2 160	36 000	485	685	1 015	665	380	(X)	(X)	(X)	3 150
Taxi drivers and chauffeurs 9140 (SOC 53-3041)	Percent	100.0%	8.6%	7.8%	45.2%	25.1%	0.6%	10.7%	0.1%	0.2%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.9%
Taxi drivers and chauffeurs 9140 (SOC 53-3041)	Male																
Taxi drivers and chauffeurs 9140 (SOC 53-3041)	Number	287 280	24 580	22 965	125 690	71 990	1 460	35 145	360	590	725	630	275	(X)	(X)	(X)	2 875
Taxi drivers and chauffeurs 9140 (SOC 53-3041)	Percent	85.7%	7.3%	6.9%	37.5%	21.5%	0.4%	10.5%	0.1%	0.2%	0.2%	0.2%	0.1%	(X)	(X)	(X)	0.9%
Taxi drivers and chauffeurs 9140 (SOC 53-3041)	Female																
Taxi drivers and chauffeurs 9140 (SOC 53-3041)	Number	47 975	4 400	3 035	25 835	12 230	700	855	125	95	285	35	105	(X)	(X)	(X)	275
Taxi drivers and chauffeurs 9140 (SOC 53-3041)	Percent	14.3%	1.3%	0.9%	7.7%	3.6%	0.2%	0.3%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Motor vehicle operators all other 9150 (SOC 53-3099)	Total both sexes																
Motor vehicle operators all other 9150 (SOC 53-3099)	Number	58 885	5 065	3 630	40 605	7 825	215	850	45	40	200	45	35	(X)	(X)	(X)	335
Motor vehicle operators all other 9150 (SOC 53-3099)	Percent	100.0%	8.6%	6.2%	69.0%	13.3%	0.4%	1.4%	0.1%	0.1%	0.3%	0.1%	0.1%	(X)	(X)	(X)	0.6%
Motor vehicle operators all other 9150 (SOC 53-3099)	Male																
Motor vehicle operators all other 9150 (SOC 53-3099)	Number	51 900	4 375	3 225	36 185	6 500	190	805	40	40	180	35	35	(X)	(X)	(X)	290
Motor vehicle operators all other 9150 (SOC 53-3099)	Percent	88.1%	7.4%	5.5%	61.5%	11.0%	0.3%	1.4%	0.1%	0.1%	0.3%	0.1%	0.1%	(X)	(X)	(X)	0.5%
Motor vehicle operators all other 9150 (SOC 53-3099)	Female																
Motor vehicle operators all other 9150 (SOC 53-3099)	Number	6 990	690	405	4 420	1 325	25	45	4	0	20	10	0	(X)	(X)	(X)	45
Motor vehicle operators all other 9150 (SOC 53-3099)	Percent	11.9%	1.2%	0.7%	7.5%	2.3%	0.0%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Locomotive engineers and operators 9200 (SOC 53-4010)	Total both sexes																
Locomotive engineers and operators 9200 (SOC 53-4010)	Number	52 870	2 315	1 220	39 465	8 125	465	550	20	65	315	35	50	(X)	(X)	(X)	245
Locomotive engineers and operators 9200 (SOC 53-4010)	Percent	100.0%	4.4%	2.3%	74.6%	15.4%	0.9%	1.0%	0.0%	0.1%	0.6%	0.1%	0.1%	(X)	(X)	(X)	0.5%
Locomotive engineers and operators 9200 (SOC 53-4010)	Male																
Locomotive engineers and operators 9200 (SOC 53-4010)	Number	50 235	2 295	1 145	38 070	7 125	455	470	20	45	305	35	45	(X)	(X)	(X)	235
Locomotive engineers and operators 9200 (SOC 53-4010)	Percent	95.0%	4.3%	2.2%	72.0%	13.5%	0.9%	0.9%	0.0%	0.1%	0.6%	0.1%	0.1%	(X)	(X)	(X)	0.4%
Locomotive engineers and operators 9200 (SOC 53-4010)	Female																
Locomotive engineers and operators 9200 (SOC 53-4010)	Number	2 635	20	75	1 400	1 000	10	80	0	25	10	0	4	(X)	(X)	(X)	10
Locomotive engineers and operators 9200 (SOC 53-4010)	Percent	5.0%	0.0%	0.1%	2.6%	1.9%	0.0%	0.2%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Railroad brake signal and switch operators 9230 (SOC	Total both sexes																
Railroad brake signal and switch operators 9230 (SOC	Number	8 000	920	355	5 735	775	75	10	0	45	60	4	0	(X)	(X)	(X)	20
Railroad brake signal and switch operators 9230 (SOC	Percent	100.0%	11.5%	4.4%	71.7%	9.7%	0.9%	0.1%	0.0%	0.6%	0.8%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Railroad brake signal and switch operators 9230 (SOC	Male																
Railroad brake signal and switch operators 9230 (SOC	Number	7 660	835	355	5 505	755	70	10	0	45	60	4	0	(X)	(X)	(X)	20
Railroad brake signal and switch operators 9230 (SOC	Percent	95.8%	10.4%	4.4%	68.8%	9.4%	0.9%	0.1%	0.0%	0.6%	0.8%	0.1%	0.0%	(X)	(X)	(X)	0.3%
Railroad brake signal and switch operators 9230 (SOC	Female																
Railroad brake signal and switch operators 9230 (SOC	Number	335	85	0	230	15	4	0	0	0	0	0	0	(X)	(X)	(X)	0
Railroad brake signal and switch operators 9230 (SOC	Percent	4.2%	1.1%	0.0%	2.9%	0.2%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Railroad conductors and yardmasters 9240 (SOC 53-	Total both sexes																
Railroad conductors and yardmasters 9240 (SOC 53-	Number	50 725	1 805	1 320	38 940	7 350	285	345	75	85	255	70	35	(X)	(X)	(X)	165
Railroad conductors and yardmasters 9240 (SOC 53-	Percent	100.0%	3.6%	2.6%	76.8%	14.5%	0.6%	0.7%	0.1%	0.2%	0.5%	0.1%	0.1%	(X)	(X)	(X)	0.3%
Railroad conductors and yardmasters 9240 (SOC 53-	Male																
Railroad conductors and yardmasters 9240 (SOC 53-	Number	47 195	1 630	1 185	36 830	6 490	210	345	35	85	200	45	25	(X)	(X)	(X)	115
Railroad conductors and yardmasters 9240 (SOC 53-	Percent	93.0%	3.2%	2.3%	72.6%	12.8%	0.4%	0.7%	0.1%	0.2%	0.4%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Railroad conductors and yardmasters 9240 (SOC 53-	Female																
Railroad conductors and yardmasters 9240 (SOC 53-	Number	3 535	175	135	2 110	860	75	0	40	0	55	25	10	(X)	(X)	(X)	50
Railroad conductors and yardmasters 9240 (SOC 53-	Percent	7.0%	0.3%	0.3%	4.2%	1.7%	0.1%	0.0%	0.1%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Subway streetcar and other rail transportation workers	Total both sexes																
Subway, streetcar, and other rail transportation workers	Number	11,210	470	630	6,885	2,625	130	215	15	15	95	0	20	(X)	(X)	(X)	105
Subway streetcar and other rail transportation workers	Percent	100.0%	4.2%	5.6%	61.4%	23.4%	1.2%	1.9%	0.1%	0.1%	0.8%	0.0%	0.2%	(X)	(X)	(X)	0.9%
Subway streetcar and other rail transportation workers	Male																
Subway, streetcar, and other rail transportation workers	Number	9,665	430	585	6,255	1,855	125	185	4	15	85	0	20	(X)	(X)	(X)	105
Subway streetcar and other rail transportation workers	Percent	86.2%	3.8%	5.2%	55.8%	16.5%	1.1%	1.7%	0.0%	0.1%	0.8%	0.0%	0.2%	(X)	(X)	(X)	0.9%
Subway streetcar and other rail transportation workers	Female																
Subway streetcar and other rail transportation workers	Number	1 545	40	45	630	770	4	35	15	0	10	0	0	(X)	(X)	(X)	0
Subway streetcar and other rail transportation workers	Percent	13.8%	0.4%	0.4%	5.6%	6.9%	0.0%	0.3%	0.1%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Sailors and marine oilers and ship engineers 9300 (SOC	Total both sexes																
Sailors and marine oilers and ship engineers 9300 (SOC	Number	29 475	1 285	1 230	21 335	3 815	275	710	65	80	430	85	10	(X)	(X)	(X)	150
Sailors and marine oilers and ship engineers 9300 (SOC	Percent	100.0%	4.4%	4.2%	72.4%	12.9%	0.9%	2.4%	0.2%	0.3%	1.5%	0.3%	0.0%	(X)	(X)	(X)	0.5%
Sailors and marine oilers and ship engineers 9300 (SOC	Male																
Sailors and marine oilers and ship engineers 9300 (SOC	Number	28 195	1 185	1 165	20 535	3 610	260	680	50	80	415	70	10	(X)	(X)	(X)	135
Sailors and marine oilers and ship engineers 9300 (SOC	Percent	95.7%	4.0%	4.0%	69.7%	12.2%	0.9%	2.3%	0.2%	0.3%	1.4%	0.2%	0.0%	(X)	(X)	(X)	0.5%
Sailors and marine oilers and ship engineers 9300 (SOC	Female																
Sailors and marine oilers and ship engineers 9300 (SOC	Number	1 280	105	65	800	205	15	30	15	0	20	10	0	(X)	(X)	(X)	20
Sailors and marine oilers and ship engineers 9300 (SOC	Percent	4.3%	0.4%	0.2%	2.7%	0.7%	0.1%	0.1%	0.1%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Ship and boat captains and operators 9310 (SOC 53-	Total both sexes																
Ship and boat captains and operators 9310 (SOC 53-	Number	39 595	1 495	505	34 490	1 350	700	440	55	70	175	120	10	(X)	(X)	(X)	190
Ship and boat captains and operators 9310 (SOC 53-	Percent	100.0%	3.8%	1.3%	87.1%	3.4%	1.8%	1.1%	0.1%	0.2%	0.4%	0.3%	0.0%	(X)	(X)	(X)	0.5%
Ship and boat captains and operators 9310 (SOC 53-	Male																
Ship and boat captains and operators 9310 (SOC 53-	Number	38 110	1 415	445	33 425	1 215	670	420	40	70	170	95	10	(X)	(X)	(X)	140
Ship and boat captains and operators 9310 (SOC 53-	Percent	96.2%	3.6%	1.1%	84.4%	3.1%	1.7%	1.1%	0.1%	0.2%	0.4%	0.2%	0.0%	(X)	(X)	(X)	0.4%
Ship and boat captains and operators 9310 (SOC 53-	Female																
Ship and boat captains and operators 9310 (SOC 53-	Number	1 485	80	60	1 065	135	30	20	15	0	4	25	0	(X)	(X)	(X)	50
Ship and boat captains and operators 9310 (SOC 53-	Percent	3.8%	0.2%	0.2%	2.7%	0.3%	0.1%	0.1%	0.0%	0.0%	0.0%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Parking lot attendants 9350 (SOC 53-6021)	Total both sexes																
Parking lot attendants 9350 (SOC 53-6021)	Number	83 380	11 690	9 985	36 720	18 630	410	3 965	360	295	260	345	0	(X)	(X)	(X)	720
Parking lot attendants 9350 (SOC 53-6021)	Percent	100.0%	14.0%	12.0%	44.0%	22.3%	0.5%	4.8%	0.4%	0.4%	0.3%	0.4%	0.0%	(X)	(X)	(X)	0.9%
Parking lot attendants 9350 (SOC 53-6021)	Male																
Parking lot attendants 9350 (SOC 53-6021)	Number	72 480	10 695	8 975	32 570	14 815	285	3 600	225	190	235	265	0	(X)	(X)	(X)	625
Parking lot attendants 9350 (SOC 53-6021)	Percent	86.9%	12.8%	10.8%	39.1%	17.8%	0.3%	4.3%	0.3%	0.2%	0.3%	0.3%	0.0%	(X)	(X)	(X)	0.7%
Parking lot attendants 9350 (SOC 53-6021)	Female																
Parking lot attendants 9350 (SOC 53-6021)	Number	10 900	995	1 010	4 150	3 815	130	365	135	105	25	75	0	(X)	(X)	(X)	95
Parking lot attendants 9350 (SOC 53-6021)	Percent	13.1%	1.2%	1.2%	5.0%	4.6%	0.2%	0.4%	0.2%	0.1%	0.0%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Automotive and watercraft service attendants 9360 (SOC	Total both sexes																
Automotive and watercraft service attendants 9360 (SOC	Number	133 050	9 270	6 185	91 575	13 890	1 780	7 445	195	445	920	415	130	(X)	(X)	(X)	795
Automotive and watercraft service attendants 9360 (SOC	Percent	100.0%	7.0%	4.6%	68.8%	10.4%	1.3%	5.6%	0.1%	0.3%	0.7%	0.3%	0.1%	(X)	(X)	(X)	0.6%

Automotive and watercraft service attendants 9360 (SOC	Male																
Automotive and watercraft service attendants 9360 (SOC	Number	100 765	7 705	5 120	67 165	10 700	1 250	6 510	180	335	725	335	70	(X)	(X)	(X)	665
Automotive and watercraft service attendants 9360 (SOC	Percent	75.7%	5.8%	3.8%	50.5%	8.0%	0.9%	4.9%	0.1%	0.3%	0.5%	0.3%	0.1%	(X)	(X)	(X)	0.5%
Automotive and watercraft service attendants 9360 (SOC	Female																
Automotive and watercraft service attendants 9360 (SOC	Number	32 285	1 565	1 065	24 415	3 190	530	930	15	110	195	80	55	(X)	(X)	(X)	130
Automotive and watercraft service attendants 9360 (SOC	Percent	24.3%	1.2%	0.8%	18.4%	2.4%	0.4%	0.7%	0.0%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Transportation inspectors 9410 (SOC 53-6051)	Total, both sexes																
Transportation inspectors 9410 (SOC 53-6051)	Number	52 585	4 480	3 025	36 660	6 170	250	1 525	80	30	145	70	20	(X)	(X)	(X)	120
Transportation inspectors 9410 (SOC 53-6051)	Percent	100.0%	8.5%	5.8%	69.7%	11.7%	0.5%	2.9%	0.2%	0.1%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Transportation inspectors 9410 (SOC 53-6051)	Male																
Transportation inspectors 9410 (SOC 53-6051)	Number	43 855	3 500	2 315	31 620	4 555	190	1 330	15	30	145	60	0	(X)	(X)	(X)	95
Transportation inspectors 9410 (SOC 53-6051)	Percent	83.4%	6.7%	4.4%	60.1%	8.7%	0.4%	2.5%	0.0%	0.1%	0.3%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Transportation inspectors 9410 (SOC 53-6051)	Female																
Transportation inspectors 9410 (SOC 53-6051)	Number	8 730	980	710	5 040	1 615	60	195	70	0	4	10	20	(X)	(X)	(X)	25
Transportation inspectors 9410 (SOC 53-6051)	Percent	16.6%	1.9%	1.4%	9.6%	3.1%	0.1%	0.4%	0.1%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Transportation attendants except flight attendants 9415	Total, both sexes																
Transportation attendants except flight attendants 9415	Number	35 790	3 400	2 645	15 330	12 205	180	1 410	115	145	95	35	65	(X)	(X)	(X)	165
Transportation attendants except flight attendants 9415	Percent	100.0%	9.5%	7.4%	42.8%	34.1%	0.5%	3.9%	0.3%	0.4%	0.3%	0.1%	0.2%	(X)	(X)	(X)	0.5%
Transportation attendants except flight attendants 9415	Male																
Transportation attendants except flight attendants 9415	Number	11 630	1 435	1 040	4 710	3 370	30	825	55	60	20	10	10	(X)	(X)	(X)	55
Transportation attendants except flight attendants 9415	Percent	32.5%	4.0%	2.9%	13.2%	9.4%	0.1%	2.3%	0.2%	0.2%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.2%
Transportation attendants except flight attendants 9415	Female																
Transportation attendants except flight attendants 9415	Number	24 160	1 965	1 605	10 620	8 835	145	585	60	85	70	25	55	(X)	(X)	(X)	105
Transportation attendants except flight attendants 9415	Percent	67.5%	5.5%	4.5%	29.7%	24.7%	0.4%	1.6%	0.2%	0.2%	0.2%	0.1%	0.2%	(X)	(X)	(X)	0.3%
Miscellaneous transportation workers, including bridge and	Total, both sexes																
Miscellaneous transportation workers, including bridge and	Number	23,635	1,645	1,360	14,525	4,070	255	955	315	25	80	65	15	(X)	(X)	(X)	325
Miscellaneous transportation workers, including bridge and	Percent	100.0%	7.0%	5.8%	61.5%	17.2%	1.1%	4.0%	1.3%	0.1%	0.3%	0.3%	0.1%	(X)	(X)	(X)	1.4%
Miscellaneous transportation workers, including bridge and	Male																
Miscellaneous transportation workers, including bridge and	Number	20,540	1,485	1,090	12,630	3,565	235	845	300	0	50	35	15	(X)	(X)	(X)	290
Miscellaneous transportation workers, including bridge and	Percent	86.9%	6.3%	4.6%	53.4%	15.1%	1.0%	3.6%	1.3%	0.0%	0.2%	0.1%	0.1%	(X)	(X)	(X)	1.2%
Miscellaneous transportation workers, including bridge and	Female																
Miscellaneous transportation workers, including bridge and	Number	3 095	160	270	1 895	505	20	105	15	25	30	30	0	(X)	(X)	(X)	35
Miscellaneous transportation workers, including bridge and	Percent	13.1%	0.7%	1.1%	8.0%	2.1%	0.1%	0.4%	0.1%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Crane and tower operators 9510 (SOC 53-7021)	Total, both sexes																
Crane and tower operators 9510 (SOC 53-7021)	Number	72 165	4 775	3 195	52 470	9 665	570	175	155	295	615	80	0	(X)	(X)	(X)	175
Crane and tower operators 9510 (SOC 53-7021)	Percent	100.0%	6.6%	4.4%	72.7%	13.4%	0.8%	0.2%	0.2%	0.4%	0.9%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Crane and tower operators 9510 (SOC 53-7021)	Male																
Crane and tower operators 9510 (SOC 53-7021)	Number	70 250	4 470	3 110	51 435	9 245	560	160	155	295	585	80	0	(X)	(X)	(X)	150
Crane and tower operators 9510 (SOC 53-7021)	Percent	97.3%	6.2%	4.3%	71.3%	12.8%	0.8%	0.2%	0.2%	0.4%	0.8%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Crane and tower operators 9510 (SOC 53-7021)	Female																
Crane and tower operators 9510 (SOC 53-7021)	Number	1 915	305	85	1 035	420	10	15	0	0	30	0	0	(X)	(X)	(X)	25
Crane and tower operators 9510 (SOC 53-7021)	Percent	2.7%	0.4%	0.1%	1.4%	0.6%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Dredge, excavating, and loading machine operators 9520	Total, both sexes																
Dredge, excavating, and loading machine operators 9520	Number	53 335	4 550	2 710	42 420	2 415	410	140	0	30	510	45	0	(X)	(X)	(X)	105
Dredge, excavating, and loading machine operators 9520	Percent	100.0%	8.5%	5.1%	79.5%	4.5%	0.8%	0.3%	0.0%	0.1%	1.0%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Dredge, excavating, and loading machine operators 9520	Male																
Dredge, excavating, and loading machine operators 9520	Number	52 710	4 540	2 710	41 865	2 385	400	110	0	30	510	45	0	(X)	(X)	(X)	105
Dredge, excavating, and loading machine operators 9520	Percent	98.8%	8.5%	5.1%	78.5%	4.5%	0.7%	0.2%	0.0%	0.1%	1.0%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Dredge, excavating, and loading machine operators 9520	Female																
Dredge, excavating, and loading machine operators 9520	Number	625	10	0	555	30	10	30	0	0	0	0	0	(X)	(X)	(X)	0
Dredge, excavating, and loading machine operators 9520	Percent	1.2%	0.0%	0.0%	1.0%	0.1%	0.0%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Conveyor operators and tenders, and hoist and winch	Total, both sexes																
Conveyor operators and tenders, and hoist and winch	Number	14 420	1 395	750	9 950	1 815	180	150	50	0	115	4	0	(X)	(X)	(X)	10
Conveyor operators and tenders, and hoist and winch	Percent	100.0%	9.7%	5.2%	69.0%	12.6%	1.2%	1.0%	0.3%	0.0%	0.8%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Conveyor operators and tenders, and hoist and winch	Male																
Conveyor operators and tenders, and hoist and winch	Number	12 890	1 340	640	8 960	1 475	165	150	50	0	95	4	0	(X)	(X)	(X)	10
Conveyor operators and tenders, and hoist and winch	Percent	89.4%	9.3%	4.4%	62.1%	10.2%	1.1%	1.0%	0.3%	0.0%	0.7%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Conveyor operators and tenders, and hoist and winch	Female																
Conveyor operators and tenders, and hoist and winch	Number	1 535	55	110	990	340	15	0	0	0	20	4	0	(X)	(X)	(X)	0
Conveyor operators and tenders, and hoist and winch	Percent	10.6%	0.4%	0.8%	6.9%	2.4%	0.1%	0.0%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Industrial truck and tractor operators 9600 (SOC 53-7051)	Total, both sexes																
Industrial truck and tractor operators 9600 (SOC 53-7051)	Number	584 370	80 550	65 940	283 885	132 250	3 335	8 780	1 515	1 510	2 475	835	630	(X)	(X)	(X)	2 665
Industrial truck and tractor operators 9600 (SOC 53-7051)	Percent	100.0%	13.8%	11.3%	48.6%	22.6%	0.6%	1.5%	0.3%	0.3%	0.4%	0.1%	0.1%	(X)	(X)	(X)	0.5%
Industrial truck and tractor operators 9600 (SOC 53-7051)	Male																
Industrial truck and tractor operators 9600 (SOC 53-7051)	Number	538 320	76 400	62 760	257 100	121 435	3 085	8 460	1 480	1 380	2 250	825	580	(X)	(X)	(X)	2 555
Industrial truck and tractor operators 9600 (SOC 53-7051)	Percent	92.1%	13.1%	10.7%	44.0%	20.8%	0.5%	1.4%	0.3%	0.2%	0.4%	0.1%	0.1%	(X)	(X)	(X)	0.4%
Industrial truck and tractor operators 9600 (SOC 53-7051)	Female																
Industrial truck and tractor operators 9600 (SOC 53-7051)	Number	46 050	4 150	3 180	26 780	10 810	250	315	35	130	230	15	50	(X)	(X)	(X)	110
Industrial truck and tractor operators 9600 (SOC 53-7051)	Percent	7.9%	0.7%	0.5%	4.6%	1.8%	0.0%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Cleaners of vehicles and equipment 9610 (SOC 53-7061)	Total, both sexes																
Cleaners of vehicles and equipment 9610 (SOC 53-7061)	Number	390 400	69 055	55 700	176 975	70 545	2 250	8 370	1 280	1 030	2 035	870	175	(X)	(X)	(X)	2 115
Cleaners of vehicles and equipment 9610 (SOC 53-7061)	Percent	100.0%	17.7%	14.3%	45.3%	18.1%	0.6%	2.1%	0.3%	0.3%	0.5%	0.2%	0.0%	(X)	(X)	(X)	0.5%
Cleaners of vehicles and equipment 9610 (SOC 53-7061)	Male																
Cleaners of vehicles and equipment 9610 (SOC 53-7061)	Number	331 545	59 010	47 760	148 105	61 675	1 680	6 695	1 070	915	1 735	780	165	(X)	(X)	(X)	1 950
Cleaners of vehicles and equipment 9610 (SOC 53-7061)	Percent	84.9%	15.1%	12.2%	37.9%	15.8%	0.4%	1.7%	0.3%	0.2%	0.4%	0.2%	0.0%	(X)	(X)	(X)	0.5%
Cleaners of vehicles and equipment 9610 (SOC 53-7061)	Female																
Cleaners of vehicles and equipment 9610 (SOC 53-7061)	Number	58 855	10 045	7 940	28 865	8 870	565	1 675	210	115	300	90	10	(X)	(X)	(X)	165
Cleaners of vehicles and equipment 9610 (SOC 53-7061)	Percent	15.1%	2.6%	2.0%	7.4%	2.3%	0.1%	0.4%	0.1%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Laborers and freight, stock, and material movers, hand	Total, both sexes																
Laborers and freight, stock, and material movers, hand	Number	2 297 785	254 590	197 320	1 342 505	387 030	18 520	55 175	6 035	7 770	10 780	4 845	2 235	(X)	(X)	(X)	10 990
Laborers and freight, stock, and material movers, hand	Percent	100.0%	11.1%	8.6%	58.4%	16.8%	0.8%	2.4%	0.3%	0.3%	0.5%	0.2%	0.1%	(X)	(X)	(X)	0.5%
Laborers and freight, stock, and material movers, hand	Male																
Laborers and freight, stock, and material movers, hand	Number	1 882 770	209 660	160 635	1 097 380	322 485	15 055	42 100	5 010	6 730	8 890	4 120	1 905	(X)	(X)	(X)	8 805
Laborers and freight, stock, and material movers, hand	Percent	81.9%	9.1%	7.0%	47.8%	14.0%	0.7%	1.8%	0.2%	0.3%	0.4%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Laborers and freight, stock, and material movers, hand	Female																
Laborers and freight, stock, and material movers, hand	Number	415 015	44 925	36 685	245 125	64 545	3 470	13 075	1 025	1 040	1 885	725	325	(X)	(X)	(X)	2 180
Laborers and freight, stock, and material movers, hand	Percent	18.1%	2.0%	1.6%	10.7%	2.8%	0.2%	0.6%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Machine feeders and offbearers 9630 (SOC 53-7063)	Total, both sexes																
Machine feeders and offbearers 9630 (SOC 53-7063)	Number	39 695	4 355	3 480	22 595	7 305	150	1 120	130	90	230	60	20	(X)	(X)	(X)	165
Machine feeders and offbearers 9630 (SOC 53-7063)	Percent	100.0%	11.0%	8.8%	56.9%	18.4%	0.4%	2.8%	0.3%	0.2%	0.6%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Machine feeders and offbearers 9630 (SOC 53-7063)	Male																
Machine feeders and offbearers 9630 (SOC 53-7063)	Number	21 690	2 335	1 930	12 240	3 870	70	625	100	90	195	60	20	(X)	(X)	(X)	155
Machine feeders and offbearers 9630 (SOC 53-7063)	Percent	54.6%	5.9%	4.9%	30.8%	9.7%	0.2%	1.6%	0.3%	0.2%	0.5%	0.2%	0.1%	(X)	(X)	(X)	0.4%
Machine feeders and offbearers 9630 (SOC 53-7063)	Female																
Machine feeders and offbearers 9630 (SOC 53-7063)	Number	18 010	2 020	1 555	10 355	3 430	80	500	30	0	35	0	0	(X)	(X)	(X)	10
Machine feeders and offbearers 9630 (SOC 53-7063)	Percent	45.4%	5.1%	3.9%	26.1%	8.6%	0.2%	1.3%	0.1%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Packers and packagers, hand 9640 (SOC 53-7064)	Total, both sexes																
Packers and packagers, hand 9640 (SOC 53-7064)	Number	501 795	116 095	97 835	171 125	82 005	2 355	25 750	1 190	1 020	1 215	555	390	(X)	(X)	(X)	2 255
Packers and packagers, hand 9640 (SOC 53-7064)	Percent	100.0%	23.1%	19.5%	34.1%	16.3%	0.5%	5.1%	0.2%	0.2%	0.2%	0.1%	0.1%	(X)	(X)	(X)	0.4%
Packers and packagers, hand 9640 (SOC 53-7064)	Male																
Packers and packagers, hand 9640 (SOC 53-7064)	Number	207,250	42,420	36,615	75,720	38,200	985	10,035	695	535	575	335	245	(X)	(X)	(X)	885
Packers and packagers, hand 9640 (SOC 53-7064)	Percent	41.3%	8.5%	7.3%	15.1%	7.6%	0.2%	2.0%	0.1%	0.1%	0.1%	0.1%	0.0%	(X)	(X)	(X)	0.2%
Packers and packagers, hand 9640 (SOC 53-7064)	Female																
Packers and packagers, hand 9640 (SOC 53-7064)	Number	294,540	73,675	61,220	95,405	43,805	1,370	15,715	495	485	640	220	145	(X)	(X)	(X)	1,370
Packers and packagers, hand 9640 (SOC 53-7064)	Percent	58.7%	14.7%	12.2%	19.0%	8.7%	0.3%	3.1%	0.1%	0.1%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.3%
Pumping station operators 9650 (SOC 53-7070)	Total, both sexes																
Pumping station operators 9650 (SOC 53-7070)	Number	22 210	1 455	900	18 280	910	190	150	15	50	225	15	0	(X)	(X)	(X)	30
Pumping station operators 9650 (SOC 53-7070)	Percent	100.0%	6.6%	4.1%	82.3%	4.1%	0.9%	0.7%	0.1%	0.2%	1.0%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Pumping station operators 9650 (SOC 53-7070)	Male																
Pumping station operators 9650 (SOC 53-7070)	Number	21 410	1 435	870	17 630	825	180	150	15	50	210	15	0	(X)	(X)	(X)	30
Pumping station operators 9650 (SOC 53-7070)	Percent	96.4%	6.5%	3.9%	79.4%	3.7%	0.8%	0.7%	0.1%	0.2%	0.9%	0.1%	0.0%	(X)	(X)	(X)	0.1%
Pumping station operators 9650 (SOC 53-7070)	Female																
Pumping station operators 9650 (SOC 53-7070)	Number	795	15	25	650	85	10	0	0	0	10	0	0	(X)	(X)	(X)	0
Pumping station operators 9650 (SOC 53-7070)	Percent	3.6%	0.1%	0.1%	2.9%	0.4%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Refuse and recyclable material collectors 9720 (SOC 53-	Total, both sexes																
Refuse and recyclable material collectors 9720 (SOC 53-	Number	101 085	12 980	10 225	50 185	23 680	1 055	1 070	195	310	520	145	80	(X)	(X)	(X)	640
Refuse and recyclable material collectors 9720 (SOC 53-	Percent	100.0%	12.8%	10.1%	49.6%	23.4%	1.0%	1.1%	0.2%	0.3%	0.5%	0.1%	0.1%	(X)	(X)	(X)	0.6%
Refuse and recyclable material collectors 9720 (SOC 53-	Male																
Refuse and recyclable material collectors 9720 (SOC 53-	Number	91 760	11 440	9 390	45 595	21 960	930	840	155	310	410	105	80	(X)	(X)	(X)	545
Refuse and recyclable material collectors 9720 (SOC 53-	Percent	90.8%	11.3%	9.3%	45.1%	21.7%	0.9%	0.8%	0.2%	0.3%	0.4%	0.1%	0.1%	(X)	(X)	(X)	0.5%
Refuse and recyclable material collectors 9720 (SOC 53-	Female																
Refuse and recyclable material collectors 9720 (SOC 53-	Number	9 325	1 540	835	4 590	1 720	125	225	40	0	110	35	0	(X)	(X)	(X)	95
Refuse and recyclable material collectors 9720 (SOC 53-	Percent	9.2%	1.5%	0.8%	4.5%	1.7%	0.1%	0.2%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.1%
Miscellaneous material moving workers, including mine	Total, both sexes																
Miscellaneous material moving workers, including mine	Number	62 175	6 155	4 650	36 890	12 075	450	790	175	190	335	40	70	(X)	(X)	(X)	360
Miscellaneous material moving workers, including mine	Percent	100.0%	9.9%	7.5%	59.3%	19.4%	0.7%	1.3%	0.3%	0.3%	0.5%	0.1%	0.1%	(X)	(X)	(X)	0.6%
Miscellaneous material moving workers, including mine	Male																
Miscellaneous material moving workers, including mine	Number	52 945	5 190	4 050	31 840	9 845	395	605	145	175	290	10	45	(X)	(X)	(X)	355
Miscellaneous material moving workers, including mine	Percent	85.2%	8.3%	6.5%	51.2%	15.8%	0.6%	1.0%	0.2%	0.3%	0.5%	0.0%	0.1%	(X)	(X)	(X)	0.6%
Miscellaneous material moving workers, including mine	Female																
Miscellaneous material moving workers, including mine	Number	9 230	965	600	5 050	2 230	55	185	30	10	45	30	30	(X)	(X)	(X)	4
Miscellaneous material moving workers, including mine	Percent	14.8%	1.6%	1.0%	8.1%	3.6%	0.1%	0.3%	0.0%	0.0%	0.1%	0.0%	0.0%	(X)	(X)	(X)	0.0%
Unemployed, no work experience in the last 5 years or	Total, both sexes																
Unemployed, no work experience in the last 5 years or	Number	1 666 735	202 035	165 990	708 065	434 665	18 110	93 100	4 130	9 270	9 315	6 335	3 340	(X)	(X)	(X)	12 380
Unemployed, no work experience in the last 5 years or	Percent	100.0%	12.1%	10.0%	42.5%	26.1%	1.1%	5.6%	0.2%	0.6%	0.6%	0.4%	0.2%	(X)	(X)	(X)	0.7%
Unemployed, no work experience in the last 5 years or	Male																
Unemployed, no work experience in the last 5 years or	Number	834 965	92 130	76 695	359 630	230 850	9 410	43 460	1 740	4 690	4 620	3 635	1 785	(X)	(X)	(X)	6 320
Unemployed, no work experience in the last 5 years or	Percent	50.1%	5.5%	4.6%	21.6%	13.9%	0.6%	2.6%	0.1%	0.3%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.4%

Unemployed, no work experience in the last 5 years or	Female																
Unemployed no work experience in the last 5 years or	Number	831 770	109 905	89 295	348 435	203 815	8 700	49 635	2 390	4 575	4 690	2 705	1 555	(X)	(X)	(X)	6 060
Unemployed no work experience in the last 5 years or	Percent	49.9%	6.6%	5.4%	20.9%	12.2%	0.5%	3.0%	0.1%	0.3%	0.3%	0.2%	0.1%	(X)	(X)	(X)	0.4%

Data are based on a sample and are subject to sampling variabi ity. The degree of uncertainty for an estimate arising from sampling variability is represented through the use of a margin of error. The value shown here is the 90 percent margin of error. The margin of error can be interpreted roughly as providing a 90 percent probability that the interval defined by the estimate minus the margin of error and the estimate plus the margin of error (the lower and upper confidence bounds) contains the true value. In addition to sampling variabi ity, the ACS estimates are subject to nonsampling error (for a discussion of nonsampling variability, see Accuracy of the Data). The effect of nonsamp ing error is not represented in these tables.

Source U.S. Census Bureau, 2006-2010 American Community Survey

Explanation of Symbols
An '**' entry in the margin of error column indicates that e ther no sample observations or too few sample
The U.S. Census Bureau co lects race data in accordance with guidelines provided by the U.S. Office of Management and Budget (OMB). Except for the total, all race and ethnicity categories are mutually exclusive. "Black" refers to Black or African American; "AIAN" refers to American Indian and Alaska Native; and "NHPI" refers to Native Hawaiian and Other Pacific Islander. The reference to "Hawa i only" indicates that these columns are only tabulated for areas in the state of Hawaii. "Balance of Not Hispanic or Latino" includes the balance of non-Hispanic individuals who reported multiple races or reported Some Other Race alone. For more information on race and Hispanic origin, see the Subject Definitions at http //www.census.gov/acs/www/data_documentation/documentation_main/.

Race and Hispanic origin are separate concepts on the American Community Survey. "White alone Hispanic or Latino" includes respondents who reported Hispanic or Latino origin and reported race as "White" and no other race. "All other Hispanic or Latino" includes respondents who reported Hispanic or Latino origin and
reported a race other than "White," either alone or in combination. To get a total for Occupation codes are 4-digit codes and are based on Standard Occupational

U.S. Equal Employment Opportunity Commission

Overview

The U.S. Equal Employment Opportunity Commission (EEOC) is responsible for enforcing federal laws that make it illegal to discriminate against a job applicant or an employee because of the person's race, color, religion, sex (including pregnancy), national origin, age (40 or older), disability or genetic information. It is also illegal to discriminate against a person because the person complained about discrimination, filed a charge of discrimination, or participated in an employment discrimination investigation or lawsuit.

Most employers with at least 15 employees are covered by EEOC laws (20 employees in age discrimination cases). Most labor unions and employment agencies are also covered.

The laws apply to all types of work situations, including hiring, firing, promotions, harassment, training, wages, and benefits.

The EEOC's Vision is:

Justice and Equality in the Workplace

The EEOC's Mission is to:

Stop and Remedy Unlawful Employment Discrimination

Read more about:

- The laws enforced by EEOC
- EEOC's charge handling process
- EEOC's outreach and educational programs
- EEOC's federal sector program
- How to contact us

Authority & Role

The EEOC has the authority to investigate charges of discrimination against employers who are covered by the law. Our role in an investigation is to fairly and accurately assess the allegations in the charge and then make a finding. If we find that discrimination has occurred, we will try to settle the charge. If we aren't successful, we have the authority to file a lawsuit to protect the rights of individuals and the interests of the public. We do not, however, file lawsuits in all cases where we find discrimination.

We also work to prevent discrimination before it occurs through outreach, education and technical assistance programs.

The EEOC provides leadership and guidance to federal agencies on all aspects of the federal government's equal employment opportunity program. EEOC assures federal agency and department compliance with EEOC regulations, provides technical assistance to federal agencies concerning EEO complaint adjudication, monitors and evaluates federal agencies' affirmative employment programs, develops and distributes federal sector educational materials and conducts training for stakeholders, provides guidance and assistance to our Administrative Judges who conduct hearings on EEO complaints, and adjudicates appeals from administrative decisions made by federal agencies on EEO complaints.

Location

We carry out our work through our headquarters offices in Washington, D.C. and through 53 field offices serving every part of the nation.

U.S. Equal Employment Opportunity Commission

EQUAL EMPLOYMENT OPPORTUNITY COMMISSION

EQUAL EMPLOYMENT OPPORTUNITY

MANAGEMENT DIRECTIVE 715

EEO MD-715

EFFECTIVE DATE: October 1, 2003

TO THE HEADS OF FEDERAL AGENCIES:

1. **SUBJECT.** Federal responsibilities under Section 717 of Title VII and Section 501 of the Rehabilitation Act.

2. **PURPOSE.** This Directive provides policy guidance and standards for establishing and maintaining effective affirmative programs of equal employment opportunity under Section 717 of Title VII (PART A) and effective affirmative action programs under Section 501 of the Rehabilitation Act (PART B). The Directive also sets forth general reporting requirements (PART C). Additional guidance and instructions for implementing the policies set forth herein will be issued separately.

3. **ORIGINATOR.** Equal Employment Opportunity Commission, Office of Federal Operations.

4. **SUPERSESSION.** This Directive SUPERSEDES EEO Management Directives 712 (dated March 29, 1983), and 713 and 714 (both dated October 6, 1987), and all related interpretative memoranda.

5. **AUTHORITY.** This Management Directive is prepared pursuant to EEOC's authority under Section 717 of the Civil Rights Act of 1964, as amended, 42 U.S.C. § 2000e-16; Reorganization Plan No. 1 of 1978, issued pursuant to 5 U.S.C. § 901 et seq.; Executive Order 11748; and Section 501 of the Rehabilitation Act of 1973, as amended by Pub. L. 99-506, 100 Stat. 1807, October 21, 1986.

6. **APPLICABILITY AND SCOPE.** This Directive applies to all executive agencies and military departments (except uniformed members) as defined in Sections 102 and 105 of Title 5 U.S.C. (including those with employees and applicants for employment who are paid from nonappropriated funds), the United States Postal Service, the Postal Rate Commission, the Tennessee Valley Authority, the Smithsonian Institution, and those units of the judicial branch of the federal government having positions in the competitive service.

7. **POLICY INTENT.** The overriding objective of this Directive is to ensure that all employees and applicants for employment enjoy equality of opportunity in the federal workplace regardless of race, sex, national origin, color, religion, disability or reprisal for engaging in prior protected activity.

8. **RESPONSIBILITIES.**

a. Agency Heads are responsible for the following:
   1. Ensuring compliance with this Directive and those implementing instructions issued by EEOC in accordance with existing law and authority.
   2. Developing systems for the evaluation of program effectiveness and barrier identification and elimination; ensuring that the agency has adequate data systems for effective analyses of applicant flow, on-board workforce and personnel transactions data; providing current guidance for the development of program plans to all component and field installations; establishing agency-wide objectives and developing and submitting program plans; and preparing accomplishment reports and plan updates for timely submission to EEOC.
   3. Ensuring the accuracy of all data submitted to the Office of Personnel Management's Central Personnel Data File (CPDF), as well as all data submitted to EEOC under this Directive.
   4. Demonstrating commitment to equality of opportunity for all employees and applicants for employment that is communicated through the ranks from the top down.

b. EEOC is responsible for the following:
   1. Reviewing and evaluating the operation of all agency equal employment opportunity programs.
   2. Reviewing and approving agency EEO plans and reports and communicating the results of evaluations to each agency, and directing agencies, as appropriate, to develop additional program objectives.

3. Providing technical assistance and training to agencies.
4. Submitting an annual report on the federal workforce based upon agency reports submitted during the fiscal year, data from the Central Personnel Data File, onsite program reviews and other audits to the President, Congress and appropriate Congressional committees.

9. **DEFINITIONS.** Definitions that apply to this Directive are located in Appendix A.

10. **POLICIES AND PROCEDURES.** This Directive provides policy guidance and standards for establishing and maintaining effective affirmative programs of equal employment opportunity under Section 717 of Title VII (PART A) and effective affirmative action programs under Section 501 of the Rehabilitation Act (PART B). The Directive also sets forth general reporting requirements (PART C). EEOC will separately issue additional guidance and instructions for implementing the policies set forth herein. In addition, EEOC will provide technical assistance and training necessary to assist agencies in the accomplishment of these objectives.

11. **REPORTING REQUIREMENTS.** The reporting requirements under this Directive are set out in Part C.

12. **LIST OF APPENDICES.**

Appendix	Title
A	Definitions
B	Authorities Relevant to Federal EEO Responsibilities

13. **INQUIRIES.**

Further information concerning this Directive may be obtained by contacting:

```
Director, Federal Sector Programs
Office of Federal Operations
Equal Employment Opportunity Commission
1801 L Street NW
Washington, D.C. 20507
Telephone:  (202) 663-4599


Date: August 25, 2003                  /s Cari M. Dominguez, Chair
```

Model Agency Title VII and Rehabilitation Act Programs

I. Introduction

The United States government employs over two million men and women across the country and around the world. The ability of our government to meet the complex needs of our nation and the American people rests squarely on these dedicated and hard-working individuals. Perhaps now more than ever before – with increasing public expectations of governmental institutions – federal agencies must position themselves to attract, develop and retain a top-quality workforce that can deliver results and ensure our nation's continued growth and prosperity.

Equal opportunity in the federal workplace is key to accomplishing this goal. In order to develop a competitive, highly qualified workforce, federal agencies must fully utilize all workers' talents, without regard to race, color, religion, national origin, sex or disability. While the promise of workplace equality is a legal right afforded all of our nation's workers, equal opportunity is more than a matter of social justice. It is a national economic imperative. Federal agencies must make full use of our nation's human capital by promoting workplace practices that free up opportunities for the best and brightest talent available. All workers must compete on a fair and level playing field and have the opportunity to achieve their fullest potential.

Policies and practices that impede fair and open competition in the federal workplace cost the American economy millions of dollars each year. The most obvious costs are out-of-pocket costs borne by both agencies and federal workers in connection with workplace disputes. Perhaps less obvious – but just as expensive – are costs associated with decreased morale and productivity and the ineffective and inefficient use of human capital resources. These costs can – and should – be avoided. Agencies must make a firm commitment to the principles of equal opportunity and make those principles a fundamental part of agency culture.

Title VII of the Civil Rights Act of 1964 (Title VII) and Section 501 of the Rehabilitation Act of 1973 (Rehabilitation Act) mandate that all federal personnel decisions be made free of discrimination on the basis of race, color,

religion, sex, national origin, reprisal or disability[1] and also require that agencies establish a program of equal employment opportunity for all federal employees and job applicants. 42 U.S.C. §2000e-16 and 29 U.S.C. §791. The Equal Employment Opportunity Commission (EEOC) has adjudicatory responsibilities in the federal EEO complaints process and oversight responsibility for federal programs required by Section 717 of Title VII and Section 501 of the Rehabilitation Act generally.

This Directive, which reflects recent and significant changes in the law, including recent Supreme Court decisions, supersedes earlier EEOC Management Directives and related interpretative memoranda on this subject and provides new guidance on the elements of legally compliant Title VII and Rehabilitation Act programs. This Directive requires agencies to take appropriate steps to ensure that all employment decisions are free from discrimination. It also sets forth the standards by which EEOC will review the sufficiency of agency Title VII and Rehabilitation Act programs, which include periodic agency self-assessments and the removal of barriers to free and open workplace competition.

Additional information concerning federal sector equal employment opportunity law and programs can be found at EEOC's website at www.eeoc.gov. The EEOC will also supplement this Directive on an as-needed basis through the issuance of additional guidance and technical assistance. Questions concerning this Directive should be directed to EEOC's Office of Federal Operations.

II. Essential Elements of Model Agency Title VII and Rehabilitation Act Programs

The essential elements of model Title VII and Rehabilitation Act programs are:

- Demonstrated commitment from agency leadership;
- Integration of EEO into the agency's strategic mission;
- Management and program accountability;
- Proactive prevention of unlawful discrimination;
- Efficiency; and
- Responsiveness and legal compliance.

A. Demonstrated Commitment From Agency Leadership
   - This Directive requires agency heads and other senior management officials to demonstrate a firm commitment to equality of opportunity for all employees and applicants for employment. Even the best workplace policies and procedures will fail if they are not trusted, respected and vigorously enforced. Agencies must translate equal opportunity into every day practice and make those principles a fundamental part of agency culture. This commitment to equal opportunity must be embraced by agency leadership and communicated through the ranks from the top down. It is the responsibility of each agency head to take such measures as may be necessary to incorporate the principles of equal employment opportunity into the agency's organizational structure.
   - To this end, agency heads must issue a written policy statement expressing their commitment to equal employment opportunity (EEO) and a workplace free of discriminatory harassment. This statement should be issued at the beginning of their tenure and thereafter on an annual basis and disseminated to all employees. In addition, agency heads and other senior management officials may, at their discretion, issue similar statements when important issues relating to equal employment opportunity arise within their agency or when important developments in the law occur.

B. Integration of EEO Into The Agency's Strategic Mission

   Equality of opportunity is essential to attracting, developing and retaining the most qualified workforce to support the agency's achievement of its strategic mission. To this end, and in addition to the regulatory requirements found at 29 C.F.R. § 1614.102(b)(4), as interpreted in Management Directive 110 at 1-1, agencies must:

   - Maintain a reporting structure that provides the agency's EEO Director with regular access to the agency head and other senior management officials for reporting on the effectiveness, efficiency and legal compliance of the agency's Title VII and Rehabilitation Act programs. To emphasize the importance of the position, the agency head should be involved in the selection and performance review of the EEO Director.
   - Ensure EEO professionals are involved with, and consulted on, the management and deployment of human resources. The EEO Director should be a regular participant in senior staff meetings and regularly consulted on human resources issues.
   - Allocate sufficient resources to create and/or maintain Title VII and Rehabilitation Act programs that: 1) identify and eliminate barriers that impair the ability of individuals to compete in the workplace because of race, national origin, sex or disability; 2) establish and maintain training and education programs designed to provide maximum opportunity for all employees to advance; and 3) ensure that unlawful discrimination in the workplace is promptly corrected and addressed.
   - Attract, develop and retain EEO staff with the strategic competencies necessary to accomplish the agency's EEO mission, and interface with agency officials, managers and employees.

- Recruit, hire, develop and retain supervisors and managers who have effective managerial, communications and interpersonal skills. Provide managers and supervisors with appropriate training and other resources to understand and successfully discharge their duties and responsibilities.
- Involve managers and employees in the implementation of the agency's Title VII and Rehabilitation Act programs.
- Use various media to distribute EEO information concerning federal EEO laws, regulations and requirements, rights, duties and responsibilities and to promote best workplace practices.

C. Management and Program Accountability

A model Title VII and Rehabilitation Act program will hold managers, supervisors, EEO officials and personnel officers accountable for the effective implementation and management of the agency's program. In ensuring such accountability, the agency must:

- Conduct regular internal audits, on at least an annual basis, to assess the effectiveness and efficiency of the Title VII and Rehabilitation Act programs and to ascertain whether the agency has made a good faith effort to identify and remove barriers to equality of opportunity in the workplace.
- Establish procedures to prevent all forms of discrimination, including harassment, retaliation and failure to provide reasonable accommodation to qualified individuals with disabilities.
- Evaluate managers and supervisors on efforts to ensure equality of opportunity for all employees.
- Maintain clearly defined, well-communicated, consistently applied and fairly implemented personnel policies, selection and promotion procedures, evaluation procedures, rules of conduct and training systems.
- Implement effective reasonable accommodation procedures that comply with applicable executive orders, EEOC guidance, the Architectural and Transportation Barriers Compliance Board's Uniform Federal Accessibility Standards and Electronic and Information Technology Accessibility Standards. Ensure that EEOC has reviewed those procedures when initially developed and if procedures are later significantly modified.
- Be mindful of the agency's disability program obligations, including the provision of reasonable accommodations, when negotiating collective bargaining agreements with recognized labor organization (s) representing agency employees.
- Ensure effective coordination between the agency's EEO programs and related human resource programs, including the Federal Equal Opportunity Recruitment Program (FEORP), the Selective Placement Programs and the Disabled Veterans Affirmative Action Program (DVAAP).
- Review each finding of discrimination to determine the appropriateness of taking disciplinary action against agency officials involved in the matter. Track these decisions and report trends, issues and problems to agency leadership for appropriate action.
- Ensure compliance with settlement agreements and orders issued by the agency, EEOC, and EEO-related cases from the Merit Systems Protection Board, labor arbitrators, and the Federal Labor Relations Authority.

D. Proactive Prevention of Unlawful Discrimination

- Agencies have an ongoing obligation to prevent discrimination on the bases of race, color, national origin, religion, sex, age, reprisal and disability, and eliminate barriers that impede free and open competition in the workplace. As part of this on-going obligation, agencies must conduct a self-assessment on at least an annual basis to monitor progress, identify areas where barriers may operate to exclude certain groups and develop strategic plans to eliminate identified barriers. A more detailed explanation of this process follows at Part A (Title VII) and Part B (Rehabilitation Act) of this Directive.

E. Efficiency

- Agencies must have an efficient and fair dispute resolution process and effective systems for evaluating the impact and effectiveness of their EEO programs.
- Maintain an efficient, fair and impartial complaint resolution process. Agencies should benchmark against EEOC regulations at 29 C.F.R. Part 1614 and other federal agencies of similar size highly ranked in EEOC's Annual Report on the federal sector complaints process.
- Ensure that the investigation and adjudication function of the agency's complaint resolution process are kept separate from the legal defense arm of the agency or other agency offices with conflicting or competing interests.
- Establish and encourage the widespread use of a fair alternative dispute resolution (ADR) program that facilitates the early, effective and efficient informal resolution of disputes. Appoint a senior official as the dispute resolution specialist of the agency charged with implementing a program to provide significant opportunities for ADR for the full range of employment-related disputes. Whenever ADR is offered in a particular workplace matter, ensure that managers at all appropriate levels will participate in the ADR process.
- Use a complaint tracking and monitoring system that permits the agency to identify the location, status, and length of time elapsed at each stage of the agency's complaint resolution process, the issues and the bases of the complaints, the aggrieved individuals/complainants, the involved management officials and other information necessary to analyze complaint activity and identify trends.

- Identify, monitor and report significant trends reflected in complaint processing activity. Analysis of data relating to the nature and disposition of EEO complaints can provide useful insight into the extent to which an agency is meeting its obligations under Title VII and the Rehabilitation Act.
- Ensure timely and complete compliance with EEOC orders and the provisions of settlement/resolution agreements.
- Maintain a system that collects and maintains accurate information on the race, national origin, sex and disability status of agency employees. See 29 C.F.R. § 1614.601 for further guidance.
- Maintain a system that tracks applicant flow data, which identifies applicants by race, national origin, sex and disability status and the disposition of all applications. EEOC will issue more detailed guidance on collecting and maintaining applicant flow data.
- Maintain a tracking system of recruitment activities to permit analyses of these efforts in any examination of potential barriers to equality of opportunity.
- Identify and disseminate best workplace practices.

F. Responsiveness and Legal Compliance

Federal agencies must:

- Ensure that they are in full compliance with the law, including EEOC regulations, orders and other written instructions. See 42 U.S.C. § 2000e-16(b).
- Report agency program efforts and accomplishments to EEOC and respond to EEOC directives and orders in accordance with EEOC instructions and time frames.
- Ensure that management fully and timely complies with final EEOC orders for corrective action and relief in EEO matters.

PART A

SECTION 717 OF TITLE VII

Proactive Prevention of Unlawful Discrimination

I. Introduction

The United States government must ensure that all its personnel actions are "made free" of any discrimination based on race, color, religion, sex, national origin or reprisal and that each of its agencies has "an affirmative program of equal employment opportunity" for all employees and applicants for employment. Section 717 of Title VII of the Civil Rights Act of 1964, as amended, 42 U.S.C. § 2000e-16. The Equal Employment Opportunity Commission (EEOC) is responsible for the review and evaluation of all federal sector equal employment opportunity (EEO) efforts.

Thus, Section 717 of Title VII requires federal agencies to take proactive steps to ensure equal employment opportunity for all their employees and applicants for employment. This means that agencies must work to proactively prevent potential discrimination before it occurs and establish systems to monitor compliance with Title VII. Agencies must regularly evaluate their employment practices to identify barriers to equality of opportunity for all individuals. Where such barriers are identified, agencies must take measures to eliminate them. With these steps, agencies will ensure that all persons are provided opportunities to participate in the full range of employment opportunities and achieve to their fullest potential.

II. Agency Self-Assessment

Agencies have an ongoing obligation to eliminate barriers that impede free and open competition in the workplace and prevent individuals of any racial or national origin group or either sex from realizing their full potential. As part of this on-going obligation, agencies must conduct a self-assessment on at least an annual basis to monitor progress and identify areas where barriers may operate to exclude certain groups. A first step in conducting this self-assessment involves looking at the racial, national origin and gender profile of relevant occupational categories in an agency's workforce. Guidance on how to group occupational categories will be provided separately. This "snapshot" can serve as a diagnostic tool to help agencies determine possible areas where barriers may exist and may require closer attention.

Agencies should be mindful, however, that statistics are only a starting point and alone rarely serve to provide a complete picture of the existence of workplace barriers. Agencies must look at statistics in the context of the totality of the circumstances. A statistical snapshot may be useful as an initial diagnostic tool, but conclusions concerning the existence of workplace barriers cannot be drawn from gross numerical assessments. Rather, the identification of workplace barriers will require a thorough examination of all of the circumstances.

The initial snapshot conducted by the agency must include, but not necessarily be limited to, an evaluation of the following data relating to the agency's status as of the end of each fiscal year:

- Total workforce distribution by race, national origin and sex for both the permanent and temporary[2] workforce;
- Permanent and temporary workforce participation rates for each grade level by race, national origin and sex;
- Permanent and temporary workforce participation rates for each of the agency's major occupational categories (divided by grade level) by race, national origin and sex;
- Participation rates in supervisory and management positions by race, national origin and sex;
- The race, national origin and sex of applicants for both permanent and temporary employment;
- The rates of selections for promotions, training opportunities and performance incentives by race, national origin and sex; and
- The rates of both voluntary and involuntary separations from employment by race, national origin and sex.

This type of information should help an agency identify any meaningful disparities and further focus its self-assessment.

In conducting its self-assessment, agencies shall compare their internal participation rates with corresponding participation rates in the relevant civilian labor force (CLF). Geographic areas of recruitment and hiring are integral factors in determining "relevant" civilian labor force participation rates. EEOC will provide appropriate civilian labor force data for use by agencies. With respect to positions typically filled through the internal promotion process or through transfers from other federal agencies, a self-assessment will involve looking at the racial, national origin and gender profile of the occupational categories and/or grade levels from which such promotions or transfers are typically made. EEOC will, from time to time, provide additional guidance on conducting the analysis.

This Directive requires agencies to collect and maintain race, national origin and gender data on employees in their permanent and temporary workforce. Such data is also required to be collected and maintained for applicants for employment. Agencies should obtain identifying information from employees and applicants by requesting voluntary self-identification. See 29 C.F.R. 1614.601. Separate guidance, including updated information on racial and national origin groupings, will be issued from EEOC concerning the collection of this data.

III. Barriers to Equal Employment Opportunity

Where an agency's self-assessment indicates that a racial, national origin or gender group may have been denied equal access to employment opportunities, the agency must take steps to identify the potential barrier. Workplace barriers can take various forms and sometimes involve a policy or practice that is neutral on its face. Identifying and evaluating potential barriers requires an agency to examine all relevant policies, practices, procedures and conditions in the workplace. The process further requires each agency to eliminate or modify, where appropriate, any policy, practice or procedure that creates a barrier to equality of opportunity.

For example, if a self-assessment revealed that Hispanics are virtually absent from the workforce in a facility, it would be logical for the agency to initially focus attention on its hiring and recruitment activities. The agency could rule out potential recruitment concerns if it determined that Hispanics were well represented among its applicants for employment. It would then be appropriate for the agency to examine all other aspects of the hiring process to identify the factor(s) responsible for the statistical disparity.

It is crucial for agencies to ensure that their barrier analyses are focused, methodical and involve the participation of all relevant agency officials. Depending on the nature of the potential problem an agency might consider the following questions:

- Are recruitment efforts resulting in a cross-section of qualified applicants? Is there a significant disparity between the proportion of a racial, national origin or gender group in the agency's applicant pools and the proportion of that group in the relevant labor markets from which applicants are drawn?
- In a workforce where employees of a particular group are virtually absent, to what extent are employment opportunities unnecessarily restricted to internal applicants?
- Have supervisors, managers and executives been adequately trained on the agency's obligations under Title VII?
- Are there decision makers whose employment decisions have excluded individuals on the basis of race, national origin or sex?
- Are there any selection criteria that tend to screen out a particular racial, national origin or gender group?

IV. Barrier Evaluation and Elimination

Once an agency identifies a likely factor (or combination of factors) adversely affecting the employment opportunities of a racial, national origin or gender group, it must decide how to respond. For example, statistical disparities are identified in an agency's auditor occupational group and further examination of the situation

reveals the following: In the past, the auditor occupational group was racially diverse, including at the higher grade levels. However, after the agency instituted a requirement that auditors must be certified public accountants (CPAs) in order to be promoted to the GS-14 level or higher, few internal candidates held CPAs and therefore did not qualify for promotional opportunities to the higher level grades. As a result, the agency recruited candidates for these positions from a local business school with a student population that primarily came from the same racial group. Over time, auditors at the grade 14 level and above did not reflect the racial diversity of auditors at the lower grade levels. Assuming the requirement for a CPA is justified by business necessity, the agency has several options to consider in designing a response to this situation. Most obviously, the agency should increase its applicant pool for positions at the grade 14 and above by recruiting at other business schools with more diverse student populations. As an additional option, the agency might take steps to encourage its own auditors at the lower grade levels to pursue a CPA.

Each agency must assess the appropriateness of any policy, practice, procedure or condition determined to negatively correlate with race, national origin or sex. In making its assessment, the agency should consider, as appropriate, the following:

- whether the agency head can do more to demonstrate to the workforce, his or her commitment to equal employment opportunity;
- whether there are budgetary or other restrictions governing a decision to limit recruitment to internal applicants;
- whether certain qualification standards are truly necessary to the successful performance in a position; and
- whether selection criteria used to assess qualifications that have been found to exclude or adversely impact a particular racial, national origin or gender group truly measure the knowledge, skills and abilities that they purport to measure, and whether alternative criteria are available that do not disadvantage any particular group.

Where it is determined that an identified barrier serves no legitimate purpose with respect to the operation of an agency, this Directive requires that agencies take immediate steps to eliminate the barrier. Even where a policy or practice that poses a barrier can be justified on grounds of business necessity, agencies must investigate whether less exclusionary policies or practices can be used that serve the same business purpose. Identified barriers that are not within the control or authority of the agency to change should be brought to the attention of the responsible entity and EEOC.

In addition to identifying and eliminating barriers, agencies may consider measures to enhance and maximize opportunities for all employees, such as:

- Identifying career enhancing opportunities such as details, developmental assignments, mentoring programs, etc. Structuring details or developmental assignments to expose a broad range of employees to a variety of positions within the agency.
- Assessing internal availability of candidates by identifying job-related skills, education, knowledge and abilities that may be obtained at lower levels in the same or similar occupational series.
- Conducting a skills-building inventory of agency employees, including but not limited to, current and potential gaps in skills and the distribution of skills. Developing an action plan to address these gaps.
- When appropriate, developing broad criteria for evaluating the knowledge, skills and abilities of applicants for particular positions that takes into account a range of experience and skills.

PART B

SECTION 501 OF THE REHABILITATION ACT

Proactive Prevention of Unlawful Discrimination

I. Introduction

Section 501 of the Rehabilitation Act of 1973, as amended, 29 U.S.C. § 791, requires federal agencies to take proactive steps to provide equal opportunity to qualified individuals with disabilities in all aspects of federal employment. Congress has directed the federal government serve as a model employer of people with disabilities. Toward that end, each agency must develop and maintain "an affirmative action program plan for the hiring, placement, and advancement of individuals with disabilities" that, among other things, provides adequate employment opportunities and sets out the ways in which an agency will meet the needs of its employees with disabilities.

The mandate to serve as a model employer requires several things. First, agencies may not discriminate against qualified individuals with disabilities. But non-discrimination alone is not enough. The Rehabilitation Act also requires agencies to take proactive steps to ensure equal employment opportunity for individuals with

disabilities. This means agencies must attempt to prevent discrimination before it occurs and must establish systems to monitor their own compliance with the Act. Agencies must regularly evaluate their employment practices to identify barriers to equality of opportunity for individuals with disabilities. Where such barriers are identified, agencies must eliminate them. With these steps, agencies will ensure that individuals with disabilities are provided opportunities to fully participate in employment opportunities and achieve to their fullest potential.

II. Non-Discrimination

The Rehabilitation Act requires agencies to ensure that employment decisions are free of unlawful discrimination on the basis of disability. In 1992, Congress amended the Rehabilitation Act to incorporate the non-discrimination standards of the Americans with Disabilities Act (ADA). Under the ADA, the term "discriminate"[3] generally includes:

- making unlawful medical examinations or inquiries;
- not providing reasonable accommodations to an otherwise qualified individual with a disability unless the agency can demonstrate that the accommodation would impose an undue hardship on its operations;
- denying job opportunities to an otherwise qualified applicant or employee because of the need for a reasonable accommodation;
- using qualification standards, employment tests or other selection criteria that screen out, or tend to screen out, individuals with disabilities unless shown to be job-related for the position in question and consistent with business necessity;
- failing to select and administer employment tests in the most effective manner to ensure that when the test is administered, the test results accurately reflect the skills, aptitudes or other factors the test purports to measure, rather than reflecting the impaired sensory, manual or speaking skills of the employee or applicant[4];
- using standards, criteria, or methods of administration that have the effect of discrimination on the basis of disability or that perpetuate the discrimination of others who are subject to common administrative control;
- limiting, segregating, or classifying a job applicant or employee in a way that adversely affects the opportunities or status of such applicant or employee because of the disability of such applicant or employee;
- participating in a contractual or other arrangement or relationship that has the effect of subjecting a qualified applicant or employee with a disability to prohibited discrimination; and
- excluding or otherwise denying equal jobs or benefits to a qualified individual because of the known disability of an individual with whom the qualified individual is known to have a relationship or association.

The Rehabilitation Act also prohibits retaliation against an individual because such individual has opposed any act or practice made unlawful by the Act or because such individual made a charge, testified, assisted or participated in any manner in an investigation, proceeding, or hearing under the Act.

III. Agency Self-Analysis

Each agency is required to conduct an internal review and analysis of the effects of all current and proposed policies, practices, procedures and conditions that, directly or indirectly, relate to the employment of individuals with disabilities. For purposes of this requirement, the term "employment" refers to the full range of employment decisions, including (but not limited to) hiring, advancement, retention, and other general terms, conditions and privileges of employment. The term "conditions" is intended to refer to the full range of environmental circumstances within an agency, including the physical layout and design of the structure in which the agency is located. In this regard, agencies should be mindful of their obligation to ensure that their physical structures and facilities comply with the requirements of the Architectural Barriers Act (42 U.S.C. § 4151 et seq) and relevant titles of the ADA.

The self-assessment required by this Directive is an ongoing obligation that must be undertaken on at least an annual basis. Each agency must collect[5] and evaluate information and data necessary to make an informed assessment about the extent to which the agency is meeting its responsibility to provide employment opportunities for qualified applicants and employees with disabilities, especially those with targeted disabilities.

A snapshot of the numerical representation and distribution of applicants and employees with disabilities can alert an agency to possible barriers that may impede employment opportunities for this group. However, agencies must be mindful that, while such numerical analyses can be useful as initial diagnostic and measuring tools, not all issues relating to their obligations under the Rehabilitation Act will lend themselves to such an analysis. Moreover, an agency can be liable for discrimination under the Rehabilitation Act if its practices exclude even one individual on the basis of that individual's disability. It is the responsibility of each agency to be sensitive to any employment circumstance or condition that may be relevant to its ability to meet its fundamental obligation to effect appropriate hiring, advancement and retention of individuals with disabilities, especially those with targeted disabilities.

The self assessment must encompass the full spectrum of employment within the agency and must include, but not be limited to, an evaluation of the following with respect to the agency's status at the end of each fiscal year:

- Total workforce distribution of employees with disabilities[6] for both the permanent and temporary workforce;
- Representation and distribution of employees with disabilities, by grade, in both the permanent and temporary workforce;
- Permanent and temporary workforce participation of employees with disabilities in major occupational groups by grades;
- The representation of individuals with disabilities among applicants for permanent and temporary employment;
- The representation of employees with disabilities among those who received promotions, training opportunities and performance incentives;
- The representation of employees with disabilities among those who were voluntarily and involuntarily separated;
- The effectiveness and efficiency with which the agency processes requests for reasonable accommodation under the Rehabilitation Act;
- The extent to which an agency is in compliance with Section 508 of the Rehabilitation Act's requirement to provide employees with disabilities access to information and data that is comparable to that provided to those without disabilities; and
- Information and trend data reflecting the nature, status and disposition of complaints in the administrative process (EEOC, MSPB and FLRA) and in court alleging violations of the Rehabilitation Act.

Although the census provides data reflecting the general and specific workforce participation rates of racial, national origin and gender groups, there is no comparable data currently available for individuals with disabilities. It is therefore difficult to perform a reliable statistical analysis, based on general workforce data, to determine the expected rate at which individuals with disabilities should be hired absent discrimination.

However, a review of agency annual submissions to the EEOC reveals that some agencies favorably distinguish themselves (compared to the federal government in general) through the number of employees with disabilities in their workforce. Until such time as reliable data is developed and disseminated concerning the general availability of individuals with disabilities in the workforce, this Directive recommends agencies evaluate themselves against the workforce profile of the federal government in general and that of agencies ranked highly, in this respect, in the most recent EEOC annual report on the federal workforce. All agencies, regardless of their relative standing, are strongly encouraged to effect steady and measurable progress with respect to the employment and advancement of individuals with disabilities.

In addition to the absence of reliable availability data for individuals with disabilities, any statistical analysis is complicated by the fact that disabilities are individual in nature, making gross statistical comparisons of limited value. Notwithstanding these limitations, an agency's analysis of the above information can help facilitate an assessment concerning the extent to which individuals with disabilities, especially those with targeted disabilities, are provided equal employment opportunities. Statistical information may be a useful starting point for a more thorough examination of the agency's physical facilities, electronic and information processes, personnel policies, selection and promotion procedures, evaluation procedures, rules of conduct and training systems to ensure full accessibility for individuals with disabilities.

Collecting and Maintaining Information About Disability

Meeting the standards of the self-analysis under the Rehabilitation Act necessarily requires an agency to obtain and maintain information regarding whether applicants and employees have disabilities. Such disability-related information is considered to be "medical information," the collection and maintenance of which is restricted by law. Agencies must adopt procedures to ensure that all disability-related "medical" information is collected and managed in accordance with the law's requirements.

Collecting Disability-Related Information

The Rehabilitation Act restricts how agencies may collect disability-related "medical" information[7]. Individuals with disabilities may be identified in one of the following ways:

- Agencies may use information obtained from Standard Form 256, the "Self-Identification of Handicap" form (SF 256) issued by the Office of Personnel Management, or other information that individuals choose to disclose about the existence of disabilities. See 29 C.F.R. § 1614.601(f).
- Agencies tracking applications from individuals with disabilities, or considering the use of excepted appointing authorities or other special programs, may invite applicants to indicate if they have the types of disabilities that are covered by the program at issue.

Whenever an agency invites an applicant or employee to provide information about his/her disability, the agency must clearly notify such individual that: (a) response to the invitation is voluntary and refusal to provide the information will not subject the individual to any adverse treatment; (b) the information will be kept confidential and used only for affirmative action purposes; and (c) individuals may self-identify at any time during their

employment and failure to complete SF 256 or to respond to pre-offer invitations will not excuse the agency from Rehabilitation Act requirements.

Confidentiality of Disability-Related Information

All medical or disability-related information must be kept confidential in accordance with EEOC regulations. Under these regulations, such information must be collected and maintained on separate forms, kept in separate files and treated as confidential medical records. 29 C.F.R. § 1630.14(b)(1).

For affirmative action purposes alone, medical and disability-related information may be disclosed to managers and others involved in a selection process, as well as to those responsible for affirmative action, where the information indicates that an applicant may be included under excepted appointing authorities or eligible to receive other affirmative action benefits. Moreover, disability-related information may be used to manage, evaluate, and report on EEO and affirmative action programs; data from SF 256 may, for example, be provided to those who will generate the statistics necessary for the workforce analyses required by this Directive.

All persons to whom information is disclosed for Rehabilitation Act program purposes must be informed about the restrictions placed on use of the information and instructed not to disclose it further than necessary to satisfy those purposes.

IV. Barriers to Equal Employment Opportunity

Where an agency's self-assessment indicates that qualified individuals with disabilities may have been, or may currently be, denied equal access to employment opportunities, the agency must take steps to identify the potential barrier. Workplace barriers can take various forms and sometimes involves a policy or practice that is neutral on its face. Identifying and evaluating potential barriers requires an agency to methodically examine the full range of policies, practices, procedures and conditions in the workplace. The process requires each agency to eliminate or modify, where appropriate, any factor that negatively correlates with disability.

Investigating potential barriers requires an agency to identify all policies, practices, procedures and conditions that may be relevant to the potential concern identified by the self-assessment. It is crucial for agencies to ensure that their investigations are focused and methodical. Such investigations should involve the participation of all relevant agency officials. Depending on the nature of the potential problem identified, an agency might consider the following questions:

- Are the agency's recruitment efforts resulting in sufficient numbers of applicants with disabilities, especially targeted disabilities?
- Are there opportunities to re-survey the agency's workforce at least every other year to maintain accurate and updated statistics on employees with disabilities?
- Is the physical structure and layout of the agency facility in compliance with applicable accessibility standards?
- Even if the agency is in compliance with accessibility standards, are there other physical barriers that remain?
- Is there evidence in the workplace of actions or practices reflecting myths, fears and stereotyping regarding individuals with disabilities?
- In a workforce where employees with disabilities are virtually absent, to what extent are employment opportunities restricted to internal applicants? Could hiring be expanded to include external candidates?
- Has the agency adequately trained its supervisors, managers and executives on the requirements of the Rehabilitation Act, including the duty to provide reasonable accommodations to otherwise qualified individuals with disabilities?
- Does the agency have an adequately funded and effective procedure for providing reasonable accommodations to employees with disabilities?
- Are there particular decision makers or groups of decision makers whose employment decisions consistently exclude qualified individuals on the basis of disability?
- Do selection criteria tend to exclude individuals with disabilities, in general, or to exclude a person with particular types of disabilities? If so, are these standards necessary to the successful performance of a particular job? Does the selection criteria at issue truly measure the knowledge, skills and abilities it purports to measure and are there alternative criteria that would serve the same purpose?

V. Barrier Evaluation and Elimination

Once an agency identifies a barrier to equal opportunities for individuals with disabilities, it must decide how to respond. Each agency must assess the appropriateness of any policy, practice, procedure or condition determined to negatively correlate with disability.

Where it is determined that a barrier to equal employment opportunity is not job-related and consistent with business necessity, this Directive requires that the agency immediately take steps to eliminate the barrier. Even

where a policy or practice can be justified on grounds of business necessity, agencies must investigate whether less exclusionary policies or practices can be used that serve the same business purpose, including the provision of reasonable accommodation. Identified barriers that are not within the control or authority of the agency to change should be brought to the attention of the responsible entity and EEOC. Any barrier associated with myths, fears or stereotyping must be eliminated immediately.

Where, as a result of its self-assessment, an agency determines that merely eliminating a barrier would not adequately address the harm caused by the barrier, it must then consider other neutral alternatives to remedy the lingering effects of the problem.

In eliminating barriers, agencies should pay special attention to ensuring their reasonable accommodation procedures are effective and in compliance with applicable executive orders and EEOC guidance.

Establishing Written Procedures For Reasonable Accommodation Requests

Agencies are required to establish and publicize specific written procedures for the prompt and efficient resolution of requests for reasonable accommodation.[8] Such procedures should address the scope of the agency's obligation to provide reasonable accommodation and the types of accommodations that must be considered. In addition, the procedures should address at least the following:

- the personnel whom employees, selectees or applicants should initially contact to request a reasonable accommodation;
- the personnel forms, if any, that an individual may be asked to complete in connection with a request for an accommodation;
- the circumstances in which supervisors or others should initiate inquiries about the need for accommodation;
- the personnel and/or offices that must approve an accommodation request;
- the amount of time decision makers have to answer requests for accommodation;
- an explanation of when decision makers may request documentation of the existence of a disability or the need for an accommodation;
- the resources, including technical assistance, available to decision makers to gain information about possible accommodations for particular disabilities;
- the ways in which accommodations can be funded or effected;
- the documentation, if any, that must be maintained concerning the consideration and disposition of requests for accommodation; and
- the process, if any, that individuals may follow to appeal denials of requests for accommodation or for specific accommodations.

In drafting procedures, agencies should ensure that requests for accommodations are handled expeditiously by knowledgeable personnel. Procedures should maximize the agency's ability to provide reasonable accommodation to all individuals who require accommodation. For example, agencies might consider establishing a central pool of staffing slots to provide readers, interpreters and personal assistants to individuals with disabilities throughout the agency or agency component.

VI. Setting Goals

The steps described above -- conducting work force analyses, reviewing agency policies, practices and facilities, and fulfilling obligations to people with disabilities under the Rehabilitation Act -- should enable an agency to make substantial progress in promoting the employment of qualified individuals with disabilities. However, such efforts may well be insufficient to provide the adequate employment opportunities that are required by the Rehabilitation Act for individuals with disabilities. Indeed, Congress anticipated that the federal government, as a model employer of individuals with disabilities, would take additional steps to include individuals with disabilities at all levels of the federal workforce.

This Directive requires agencies with 1,000 employees or more to maintain a special recruitment program for individuals with targeted disabilities and to establish specific goals for the employment and advancement of such individuals.[9] For these purposes, targeted disabilities may be considered as a group. Agency goals should be set and accomplished in such a manner as will effect measurable progress from the preceding fiscal year.

To accomplish established goals, agencies should, as appropriate: 1) engage in outreach and targeted recruitment; 2) take advantage of excepted appointing authorities;[10] 3) create training and development plans for individuals with disabilities; and 4) take disability into account in selection decisions where an individual with a disability is otherwise qualified with or without a reasonable accommodation. To achieve maximum impact through their Rehabilitation Act program, agencies are required, under this Directive, to give special attention to those with targeted disabilities in each of the activities discussed herein.

PART C

EEOC OVERSIGHT AND TECHNICAL ASSISTANCE

FOR MANAGEMENT DIRECTIVE 715

(PARTS A & B)

I. REPORTING

This Directive requires each agency to report annually on the status of activities undertaken pursuant to its equal employment opportunity program under Title VII and activities undertaken pursuant to its affirmative action obligations under the Rehabilitation Act. Agency reports must also include a plan that sets forth steps it will take in the future to correct deficiencies or further improve efforts undertaken pursuant to this Directive. Additional instructions regarding the format and content requirements of reports will be issued separately and may be modified on a periodic basis as needed. Agency reports must be submitted to the EEOC annually and should include (but not necessarily be limited to) the following:

- The name and location of the agency or reporting component;
- The number of permanent and temporary employees employed;
- The name of the head of the agency or reporting component;
- The name, title, grade and qualifications of the principal EEO official(s) responsible for overseeing the program and preparing the report;
- Copies of relevant EEO policy statements issued or reinforced during the previous fiscal year;
- A narrative description of the agency's mission, mission-related functions, and a copy of the agency's organizational chart;
- A description of how the agency's Title VII and Rehabilitation Act programs measure up against the essential elements of a model program described in this Directive;
- A description of activities undertaken during the preceding year in connection with the self-assessment and barrier identification and elimination under Parts A and B of this Directive;
- A description of action items and plans to be implemented or accomplished by the agency during the upcoming year in connection with carrying out its responsibilities under this Directive;
- A description of action items and plans to provide maximum opportunity for employees to advance to their highest level of potential under Parts A and B of this Directive;
- Data required in connection with Form 462 reporting; and
- Other information, in such format as EEOC may prescribe, required in the instructions supplementing this Directive.

Reports filed by agencies pursuant this Directive will be evaluated for clarity and content by EEOC. EEOC will approve or disapprove specific plans as appropriate. In addition, EEOC will periodically conduct evaluations and program reviews to more closely assess whether the program elements of this Directive are being met and will be available on an ongoing basis as issues arise for agencies to consult with in facilitating program improvements.

There are many consequences associated with an agency's failure to fully implement effective EEO programs, including the out-of pocket costs that will be borne by the agency in connection with workplace disputes, especially after the passage of the No Fear Act, and the very real costs associated with decreased morale and productivity resulting from the ineffective and inefficient use of human capital resources. Moreover, where annual reports or information otherwise obtained by EEOC suggest that an agency is giving insufficient attention to its obligations under this Directive, EEOC will inform the President and appropriate Congressional committees.

II. TRAINING AND TECHNICAL ASSISTANCE

The EEOC is available to provide training and technical assistance to facilitate agency compliance with this Directive. Information may be obtained by contacting EEOC as follows:

- (800) 669 - EEOC (the telephone information hotline)
- (202) 663-4599 (the Office of Federal Operations)
- www.eeoc.gov (EEOC's website)

Agencies may also contact the EEOC by regular mail addressed to:

```
Director, Federal Sector Programs
Office of Federal Operations
Equal Employment Opportunity Commission
1801 L Street NW
```

Washington, D.C. 20507

III. PROGRAM EVALUATIONS BY EEOC

EEOC may conduct evaluations of federal agency EEO programs to ensure compliance with this Directive, other policy guidance issued by EEOC and the statutes and regulations that EEOC enforces.

APPENDIX A

DEFINITIONS

The following definitions apply to this Directive:

- **Applicant:** A person who applies for employment.
- **Applicant Flow Data:** Information reflecting characteristics of the pool of individuals applying for an employment opportunity.
- **Barrier:** An agency policy, principle, practice or condition that limits or tends to limit employment opportunities for members of a particular gender, race or ethnic background or for an individual (or individuals) based on disability status.
- **Disability:** For the purpose of statistics, recruitment, and targeted goals, the number of employees in the workforce who have indicated having a disability on a Office of Personnel Management Standard Form (SF) 256. For all other purposes, the definition contained in 29 C.F.R. § 1630.2 applies.
- **Civilian Labor Force (CLF):** Persons 16 years of age and over, except those in the armed forces, who are employed or are unemployed and seeking work.
- **Employees:** Members of the agency's permanent or temporary work force, whether full or part-time and whether in competitive or excepted service positions.
- **Employment Decision:** Any decision affecting the terms and conditions of an individual's employment, including but not limited to hiring, promotion, demotion, disciplinary action and termination.
- **Feeder Group or Pool:** Occupational group(s) from which selections to a particular job are typically made.
- **Fiscal Year:** The period from October 1 of one year to September 30 of the following year.
- **Goal:** Under the Rehabilitation Act, an identifiable objective set by an agency to address or eliminate barriers to equal employment opportunity or to address the lingering effects of past discrimination.
- **Major Occupations:** Agency occupations that are mission related and heavily populated, relative to other occupations within the agency.
- **Onsite Program Review:** Visit by EEOC representatives to an agency to evaluate the agency's compliance with the terms of this Directive and/or to provide technical assistance.
- **Reasonable Accommodation:** Generally, any modification or adjustment to the work environment, or to the manner or circumstances under which work is customarily performed, that enables an individual with a disability to perform the essential functions of a position or enjoy equal benefits and privileges of employment as are enjoyed by similarly situated individuals without a disability. For a more complete definition, see 29 C.F.R. § 1630.2(o). See also, EEOC's Enforcement Guidance on Reasonable Accommodation and Undue Hardship under the Americans with Disabilities Act, No. 915.002 (October 17, 2002).
- **Relevant Labor Force:** The source from which an agency draws or recruits applicants for employment or an internal selection such as a promotion.
- **Section 501 Program:** The affirmative program plan that each agency is required to maintain under Section 501 of the Rehabilitation Act to provide individuals with disabilities adequate hiring, placement, and advancement opportunities.
- **Section 717 Program:** The affirmative program of equal employment opportunity that each agency is required to maintain for all employees and applicants for employment under Section 717 of Title VII.
- **Selection Procedure:** Any employment policy or practice that is used as a basis for an employment decision.
- **Special Recruitment Program:** A program designed to monitor recruitment of, and track applications from, persons with targeted disabilities.
- **Targeted Disabilities:** Disabilities that the federal government, as a matter of policy, has identified for special emphasis in affirmative action programs. They are: 1) deafness; 2) blindness; 3) missing extremities; 4) partial paralysis; 5) complete paralysis; 6) convulsive disorders; 7) mental retardation; 8) mental illness; and 9) distortion of limb and/or spine.
- **Technical Assistance:** Training, assistance or guidance provided by the EEOC in writing, over the telephone or in person.

APPENDIX B

AUTHORITIES RELEVANT TO FEDERAL EEO RESPONSIBILITIES

A. AUTHORITIES RELEVANT TO TITLE VII

STATUTES

Section 717 of Title VII of 1964, as amended, 42 U.S.C. § 2000e-16, requires that personnel actions be free from discrimination on the basis of race, sex, color, national origin and religion and that agencies establish affirmative programs of equal employment opportunity.

Section 715 of Title VII establishes the EEOC as the lead agency for "developing and implementing agreements, policies and practices designed to maximize effort, promote efficiency, and eliminate conflict, competition, duplication and inconsistency among ...various departments, agencies and branches of the Federal Government responsible for the implementation and enforcement of equal employment opportunity legislation, orders, and policies...."

Section 703(k) of Title VII sets forth the criteria for establishing a claim of unlawful adverse impact.

REGULATIONS

29 C.F.R. §1604 Sets forth policies and principles governing discrimination on the basis of sex.

29 C.F.R. §1606 Sets forth policies and principles governing discrimination on the basis of national origin.

29 C.F.R. §1607 Establishes policies, principles and procedures for determining when a "selection procedure" has an unlawful impact on the hiring, promotion, or other employment opportunities of members of any race, sex, or ethnic group.

29 C.F.R. §1608.4 Governs affirmative action in the private sector and requires that an affirmative action plan or program under Title VII contain three elements: a reasonable self analysis; a reasonable basis for concluding action is appropriate; and reasonable action.

29 C.F.R. Part 1614 Sets forth policies and regulations to effectuate the Government's obligation to promote equal employment opportunity and to prohibit discrimination in employment because of race, color, religion, sex, national origin, age or disability.

29 C.F.R.§1614.601 Requires each agency to establish a system to collect and maintain accurate employment information on the race, national origin, sex and disability of its employees. 1614.601(b) states that data on race, national origin and sex should be collected by voluntary self identification. Subsection (e) states that an agency shall not establish a quota for the employment of persons based on race, color, religion, sex, or national origin. Subsection (g) states that an agency shall report to the Commission on employment by race, national origin, sex and disability in the form, and at such times, as the Commission may require.

29 C.F.R.§1614.602 Requires that each agency report to the Commission complaint processing information. Subsection (c) states that each agency shall submit annually for the review and approval of the Commission written national and regional equal employment opportunity plans of action. The plans shall be in a format prescribed by the Commission.

29 C.F.R. §1690 Sets forth procedures for the prescribed coordination between the EEOC and other federal agencies having responsibility for enforcement of statutes, regulations, Executive Orders and policies which require equal employment opportunity without regard to race, color, national origin, sex, religion, age or disability.

EXECUTIVE ORDERS

Executive Order 11478, as amended (1971)- Reiterated the policy of the federal government to provide equal employment opportunity on the basis of merit and fitness and "without discrimination because of race, color, religion, sex, or national origin. To promote the full realization of this policy, the Order requires, inter alia, that agencies and departments establish "continuing affirmative programs" to ensure that equal employment opportunity is an "integral part of every aspect of personnel policy and practice in the employment, development, advancement, and treatment of civilian employees in the Federal Government."

Executive Order 12106 (1978) - Amended Executive Order 11478 to include, in its coverage, non-discrimination based on age and disability. The Order further transferred federal equal employment opportunity enforcement authority to the Equal Employment Opportunity Commission and made the EEOC responsible for "directing and furthering" the implementation of equal employment opportunity policy.

Executive Order 12067 (1978) - Effected the transfer of the functions of the Equal Employment Opportunity Coordinating Council to the EEOC and delineated the EEOC's responsibility for "develop[ing] uniform standards, guidelines, and policies for promoting and furthering equal employment opportunity in the government.

B. AUTHORITIES RELEVANT TO REHABILITATION ACT

STATUTES

Section 501 of the Rehabilitation Act of 1973, as amended, 29 U.S.C. § 791, requires each covered agency to establish an affirmative action program plan for the hiring, placement, and advancement of individuals with disabilities. Section 501(g) of the Act incorporates the legal standards of title I of the Americans with Disabilities Act (42 U.S.C. § 12111 et seq) for complaints alleging "nonaffirmative action employment discrimination" and the provisions of sections 501 through 504, and 510, of the ADA (42 U.S.C. §§ 12201-12204 and 12210) "as such sections relate to employment."

Section 508 of the Rehabilitation Act requires agencies to provide federal employees with disabilities access to information and data that is comparable to the access provided to federal employees without disabilities.[11]

The Architectural Barriers Act, 42 U.S.C. § 4151 et seq is enforced by the Architectural and Transportation Barriers Compliance Board and requires that buildings and facilities be accessible to people with disabilities if they were constructed or altered by or on behalf of the federal government or with certain federal funds, or leased to the government, after 1968.

REGULATIONS

29 C.F.R. Part 1614 Sets forth policies and regulations to effectuate the Government's obligation to promote equal employment opportunity and to prohibit discrimination in employment because of race, color, religion, sex, national origin, age or disability.

29 C.F.R. Part 1630 Regulations implementing the equal employment provisions of the Americans with Disabilities Act.

5 C.F.R. § 213.3102(t),(u) OPM special appointing authority governing employment of individuals who are mentally retarded (t) and those with severe physical "handicaps"(u).

5 C.F.R. § 213.3102 OPM special appointing authority governing persons with psychiatric disabilities. Under this provision such employees may be converted to competitive status after completion of two years of satisfactory service in their excepted positions.

5 C.F.R § 213.3202(11) OPM special appointing authority for employment of readers, interpreters, and personal assistants for employees with disabilities.

5 C.F.R. § 315.709 Authorizes employees with severe physical disabilities and mental retardation to convert to competitive status after completion of two years of satisfactory service in their excepted positions.

EXECUTIVE ORDERS

Executive Order 13078, as amended (2000) – Established the National Task Force on Employment of Adults with Disabilities (now called the Presidential Task Force). The purpose of the Task Force is to implement a national policy to effect gainful employment of adults with disabilities, including employment in the Federal Government.

Executive Order 13145 (2000) – Prohibits discrimination in federal employment on the basis of genetic information.

Executive Order 13163 (2000)– Promotes a policy to increase opportunities for individuals with disabilities employed at all levels and occupations in the federal government.

Executive Order 13164 (2000) – Requires agencies to establish written procedures to facilitate the provision of reasonable accommodations under the Rehabilitation Act.

---

[1] It should be noted that federal employees and applicants for employment are also protected from discrimination by the Age Discrimination in Employment Act of 1967 (ADEA) and the Equal Pay Act of 1963.

[2] In the past, EEOC has only required consideration of temporary employees in connection with agencies' Rehabilitation Act programs. However, as the nature of federal employment changes and more employees occupy temporary positions, an examination of Title VII data relating to temporary employees, where they comprise a significant portion of an agency's workforce, may assist an agency in identifying any meaningful disparities resulting from barriers to equality of opportunity. It is recognized that temporary employees will not experience the same career progression as the permanent workforce, and certain data, such as promotion rates, may not be relevant to temporary employees. EEOC will issue more detailed guidance to agencies concerning Title VII program treatment of temporary employees.

[3]See 42 U.S.C. § 12112(b).

[4]It is permissible for a test to measure sensory, manual or speaking skills where such skills are necessary for the performance of an essential function of the job for which the test has been designed.

[5]See 29 C.F.R. § 1614.601 for further guidance. In addition, EEOC will issue more detailed guidance on collecting and maintaining applicant flow data.

[6]Agencies should separately identify applicants and employees with targeted disabilities. Targeted disabilities are those that the federal government, as a matter of policy, has identified for special emphasis. Targeted disabilities (and the codes that represent them on Standard Form 256) are: 1. deafness (16 and 17); 2. blindness (23 and 25); 3. missing extremities (28 and 32 through 38); 4. partial paralysis (64 through 68); 5. complete paralysis (71 through 78); 6. convulsive disorders (82); 7. mental retardation (90); 8. mental illness (91); and 9. distortion of limb and/or spine (92).

[7]See 29 C.F.R. pt. 1630 app. §§ 1630.13, 14. In most cases, the Rehabilitation Act bars disability-related questions until after an agency has made a conditional job offer to an applicant and requires that any inquiries of employees be job-related and consistent with business necessity. The Commission has recognized, however, that employers may extend invitations to self-identify for purposes of their affirmative action programs. See EEOC ADA Enforcement Guidance: Preemployment Disability-Related Question and Medical Examinations (10/95) at p. 12.

[8]See Executive Order 13164 (July 26, 2000). See also EEOC Policy Guidance on Executive Order 13164 (October 20, 2000).

[9]The Rehabilitation Act requires each Federal agency to submit to the EEOC for review and approval "an affirmative action program plan for the hiring, placement, and advancement of individuals with disabilities." The statute makes clear that EEOC is to approve these plans only after it "determines...that such plan provides sufficient assurances, procedures and commitments to provide adequate hiring, placement, and advancement opportunities for individuals with disabilities." 29 U.S.C. § 791(b).

[10]There are excepted appointing authorities that apply only to those with targeted disabilities. See 5 C.F.R. §§ 213.3102(t), (u); 213.3202(k) (1996). Agencies should follow the requirements of those authorities, which are enforced by the Office of Personnel Management, in assessing whether a particular individual with a disability is eligible for an excepted appointment.

[11]National security systems, as defined in the Clinger-Cohen Act, 40 U.S.C. § 1452 are exempt from these requirements. See 29 U.S.C. § 794d(a)(5).

Laws, Regulations, Guidance & MOUs

Overview

Laws

Regulations

Guidance

Memoranda of Understanding

Discrimination by Type

Prohibited Practices

Home > Laws, Regulations & Guidance > Types of Discrimination

Harassment

Harassment is a form of employment discrimination that violates Title VII of the Civil Rights Act of 1964, the Age Discrimination in Employment Act of 1967, (ADEA), and the Americans with Disabilities Act of 1990, (ADA).

Harassment is unwelcome conduct that is based on race, color, religion, sex (including pregnancy), national origin, age (40 or older), disability or genetic information. Harassment becomes unlawful where 1) enduring the offensive conduct becomes a condition of continued employment, or 2) the conduct is severe or pervasive enough to create a work environment that a reasonable person would consider intimidating, hostile, or abusive. Anti-discrimination laws also prohibit harassment against individuals in retaliation for filing a discrimination charge, testifying, or participating in any way in an investigation, proceeding, or lawsuit under these laws; or opposing employment practices that they reasonably believe discriminate against individuals, in violation of these laws.

Petty slights, annoyances, and isolated incidents (unless extremely serious) will not rise to the level of illegality. To be unlawful, the conduct must create a work environment that would be intimidating, hostile, or offensive to reasonable people.

Offensive conduct may include, but is not limited to, offensive jokes, slurs, epithets or name calling, physical assaults or threats, intimidation, ridicule or mockery, insults or put-downs, offensive objects or pictures, and interference with work performance. Harassment can occur in a variety of circumstances, including, but not limited to, the following:

- The harasser can be the victim's supervisor, a supervisor in another area, an agent of the employer, a co-worker, or a non-employee.
- The victim does not have to be the person harassed, but can be anyone affected by the offensive conduct.

Employer Coverage

15 or more employees under Title VII and the ADA, 20 or more employees under the ADEA

Time Limits

180 days to file a charge
(may be extended by state laws)

Federal employees have 45 days to contact an EEO counselor

For more information:

- Title VII of the Civil Rights Act
- The Age Discrimination in Employment Act
- The Americans with Disabilities Act
- Policy & Guidance
- Statistics

- Unlawful harassment may occur without economic injury to, or discharge of, the victim.

Prevention is the best tool to eliminate harassment in the workplace. Employers are encouraged to take appropriate steps to prevent and correct unlawful harassment. They should clearly communicate to employees that unwelcome harassing conduct will not be tolerated. They can do this by establishing an effective complaint or grievance process, providing anti-harassment training to their managers and employees, and taking immediate and appropriate action when an employee complains. Employers should strive to create an environment in which employees feel free to raise concerns and are confident that those concerns will be addressed.

Employees are encouraged to inform the harasser directly that the conduct is unwelcome and must stop. Employees should also report harassment to management at an early stage to prevent its escalation.

Employer Liability for Harassment

The employer is automatically liable for harassment by a supervisor that results in a negative employment action such as termination, failure to promote or hire, and loss of wages. If the supervisor's harassment results in a hostile work environment, the employer can avoid liability only if it can prove that: 1) it reasonably tried to prevent and promptly correct the harassing behavior; and 2) the employee unreasonably failed to take advantage of any preventive or corrective opportunities provided by the employer.

The employer will be liable for harassment by non-supervisory employees or non-employees over whom it has control (e.g., independent contractors or customers on the premises), if it knew, or should have known about the harassment and failed to take prompt and appropriate corrective action.

When investigating allegations of harassment, the EEOC looks at the entire record: including the nature of the conduct, and the context in which the alleged incidents occurred. A determination of whether harassment is severe or pervasive enough to be illegal is made on a case-by-case basis.

If you believe that the harassment you are experiencing or witnessing is of a specifically sexual nature, you may want to see EEOC's information on sexual harassment.

Laws, Regulations, Guidance & MOUs

Overview

Laws

Regulations

Guidance

Memoranda of Understanding

Discrimination by Type

Prohibited Practices

Retaliation

All of the laws we enforce make it illegal to fire, demote, harass, or otherwise "retaliate" against people (applicants or employees) because they filed a charge of discrimination, because they complained to their employer or other covered entity about discrimination on the job, or because they participated in an employment discrimination proceeding (such as an investigation or lawsuit).

For example, it is illegal for an employer to refuse to promote an employee because she filed a charge of discrimination with the EEOC, even if EEOC later determined no discrimination occurred.

Retaliation & Work Situations

The law forbids retaliation when it comes to any aspect of employment, including hiring, firing, pay, job assignments, promotions, layoff, training, fringe benefits, and any other term or condition of employment.

Employer Coverage

15 or more employees under Title VII and ADA

20 or more employees under ADEA

Virtually all employers under EPA

Time Limits

180 days to file a charge *(may be extended by state laws)*

Federal employees have 45 days to contact an EEO Counselor

For more information, see:

- Facts About Retaliation
- Equal Pay Act
- Title VII of the Civil Rights Act of 1964
- Age Discrimination in Employment Act
- Americans with Disabilities Act
- Regulations: 29 C.F.R. Part 1606
- Policy & Guidance

Laws, Regulations, Guidance & MOUs

Overview

Laws

Regulations

Guidance

Memoranda of Understanding

Discrimination by Type

Prohibited Practices

Retaliation

All of the laws we enforce make it illegal to fire, demote, harass, or otherwise "retaliate" against people (applicants or employees) because they filed a charge of discrimination, because they complained to their employer or other covered entity about discrimination on the job, or because they participated in an employment discrimination proceeding (such as an investigation or lawsuit).

For example, it is illegal for an employer to refuse to promote an employee because she filed a charge of discrimination with the EEOC, even if EEOC later determined no discrimination occurred.

Retaliation & Work Situations

The law forbids retaliation when it comes to any aspect of employment, including hiring, firing, pay, job assignments, promotions, layoff, training, fringe benefits, and any other term or condition of employment.

Employer Coverage

15 or more employees under Title VII and ADA

20 or more employees under ADEA

Virtually all employers under EPA

Time Limits

180 days to file a charge *(may be extended by state laws)*

Federal employees have 45 days to contact an EEO Counselor

For more information, see:

- Facts About Retaliation
- Equal Pay Act
- Title VII of the Civil Rights Act of 1964
- Age Discrimination in Employment Act
- Americans with Disabilities Act
- Regulations: 29 C.F.R. Part 1606
- Policy & Guidance

EEO-1 JOINT REPORTING COMMITTEE
- Equal Employment Opportunity Commission
- Office of Federal Contract Compliance Programs

O.M.B. No. 3046-0007
Approval Expires 1/2009

EQUAL EMPLOYMENT
OPPORTUNITY COMMISSION

WASHINGTON, D.C. 20507

EQUAL EMPLOYMENT OPPORTUNITY

STANDARD FORM 100, REV. January 2006, EMPLOYER INFORMATION REPORT EEO-1

INSTRUCTION BOOKLET

The Employer Information EEO-1 survey is conducted annually under the authority of Title VII of the Civil Rights Act of 1964, 42 U.S.C. 2000e, et. seq., as amended. All employers with 15 or more employees are covered by Title VII and are required to keep employment records as specified by Commission regulations. Based on the number of employees and federal contract activities, certain large employers are required to file an EEO-1 report on an annual basis.

See the Appendix for the applicable provisions of the law, Section 709(c) of Title VII, and the applicable regulations, Sections 1602.7-1602.14, Chapter XIV, Title 29 of the Code of Federal Regulations. State and local governments, school systems and educational institutions are covered by other employment surveys and are excluded from Standard Form 100, Employer Information Report EEO-1.

In the interests of consistency, uniformity and economy, Standard Form 100 has been jointly developed by the Equal Employment Opportunity Commission and the Office of Federal Contract Compliance Programs of the U. S. Department of Labor, as a single form which meets the statistical needs of both programs. In addition, this form should be a valuable tool for companies to use in evaluating their own internal programs for insuring equal employment opportunity.

As stated above, the filing of Standard Form 100 is required by law; *it is not voluntary*. Under section 709(c) of Title VII, the Equal Employment Opportunity Commission may compel an employer to file this form by obtaining an order from the United States District Court.

Under Section 209(a) of Executive Order 11246, the penalties for failure by a federal contractor or subcontractor to comply may include termination of the federal government contract and debarment from future federal contracts.

1. WHO MUST FILE

Standard Form 100 must be filed by —

(A) All private employers who are: (1) subject to Title VII of the Civil Rights Act of 1964, as amended, with 100 or more employees **EXCLUDING** State and local governments, primary and secondary school systems, institutions of higher education, Indian tribes and tax-exempt private membership clubs other than labor organizations; OR (2) subject to Title VII who have fewer than 100 employees if the company is owned or affiliated with another company, or there is centralized ownership, control or management (such as central control of personnel policies and labor relations) so that the group legally constitutes a single enterprise, and the entire enterprise employs a total of 100 or more employees.

(B) All federal contractors (private employers), who: (1) are not exempt as provided for by 41 CFR 60-1.5; (2) have 50 or more employees; **and** (a) are prime contractors or first-tier subcontractors, and have a contract, subcontract, or purchase order amounting to $50,000 or more; or (b) serve as a depository of government funds in any amount, or (c) is a financial institution which is an issuing and paying agent for U.S. Savings Bonds and Notes.

Only those establishments located in the District of Columbia and the 50 states are required to submit Standard Form 100. No reports should be filed for establishments in Puerto Rico, the Virgin Islands or other American Protectorates.

2. HOW TO FILE

NOTE: Submission of EEO-1 data through the *EEO-1 Online Filing System* or as an electronically transmitted data file is strongly preferred. See paragraph 6, "EEO-1 Alternate Reporting Formats."

Single-establishment employers, i.e., employers doing business at only one establishment in one location must complete a single EEO-1 online data record or submit a single EEO-1 paper report.

Multi-establishment employers, i.e., employers doing business at more than one establishment, must complete online: (1) a report covering the principal or headquarters office; (2) a separate report for **EACH** establishment employing 50 or more persons; and (3) a separate report (Type 8 record) for each establishment employing fewer than 50 employees, OR an

Establishment List (Type 6 record), showing the name, address, and total employment for each establishment employing fewer than 50 persons, including a Type 6 employment data grid that combines all employees working at establishments employing fewer than 50 employees by race, sex, and job category. For the EEO-1 online application, keyed employment data automatically transfers to the overall Consolidated Report.

The total number of employees indicated on the headquarters report, **PLUS** the establishment reports, **PLUS** the list of establishments employing fewer than 50 employees, **MUST** equal the total number of employees shown on the Consolidated Report.

Employment data for multi-establishment companies, including parent corporations and their subsidiary holdings, must report all employees working at each company establishment or subsidiary establishment. For the purposes of this report, the term **parent corporation** refers to any corporation which owns all or the majority stock of another corporation so that the latter relates to it as a subsidiary.

3. WHEN TO FILE

This annual report must be filed not later than September 30. Employment figures from any pay period in July through September may be used.

4. WHERE TO FILE [Paper EEO-1 form(s) ONLY]

Mail one copy to the address indicated in the annual survey mailout memorandum.

5. REQUESTS FOR INFORMATION AND SPECIAL PROCEDURES

An employer who claims that preparation or the filing of Standard Form 100 would create undue hardship may apply to the Commission for a special reporting procedure. In such cases, the employer must submit **in writing** a detailed alternative proposal for compiling and reporting information to: **The EEO-1 Coordinator, EEOC-Survey Division, 1801 L Street, NW, Washington, DC 20507.**

Only those special procedures approved **in writing** by the Commission are authorized. Such authorizations remain in effect until notification of cancellation is given. All requests for information should be sent to the address above.

6. EEO-1 ALTERNATE REPORTING FORMATS

EEO-1 reporting is an electronic, online application. Pursuant to the Government Paperwork Elimination Act of 1998, we **STRONGLY** recommend that EEO-1 reports be submitted via the *EEO-1 Online Filing System*, or as an electronically transmitted data file. A copy of the **prescribed** EEO-1 data file format is available at the website address in the survey mailout memorandum; or by calling the telephone number or writing to the address in the survey mailout memorandum. *Paper EEO-1 forms will be generated on request **only**, in extreme cases where Internet access is not available to the employer*. An EEO-1 report submitted on paper must be prepared following the directions in paragraph 2, "HOW TO FILE".

7. CONFIDENTIALITY

All reports and information from individual reports will be kept confidential, as required by Section 709(e) of Title VII. Only data aggregating information by industry or area, in such a way as not to reveal any particular employer's statistics, will be made public. The prohibition against disclosure mandated by Section 709(e) does not apply to the Office of Federal Contract Compliance Programs and contracting agencies of the federal government which require submission of SF 100 pursuant to Executive Order 11246. Reports from prime contractors and subcontractors doing business with the federal government may not be confidential under Executive Order 11246.

8. ESTIMATE OF BURDEN

Public reporting burden for this collection of information is estimated to average three and five tenths (3.5) hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed and completing and reviewing the collection of information. A response is defined as one survey form. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to:

The EEOC Clearance Officer
Office of the Chief Financial Officer and Administrative Services – Room 2100
1801 L Street, N.W.
Washington, D.C. 20507

AND

Paperwork Reduction Project (3046-0007)
Office of Management and Budget
Washington, D.C. 20503

The full text of the OMB regulations may be found at 5 CFR Part 1320**. PLEASE DO NOT SEND YOUR COMPLETED REPORT TO EITHER OF THESE ADDRESSES.**

EEO-1 Terms Applicable To All Reporting Formats

Type of Report (Status Code)

1– Single-establishment company

Multi-establishment company
2– Consolidated Report (Required)
3 – Headquarters Report (Required)
4 – Establishment Report (50 or more employees)
6 – Establishment List (Option 1)
8 – Establishment Report (less than 50 employees) (Option 2)

Company Identification

Refers to the company name and address of the headquarters office of the multi-establishment company (Report Types 2 and 3); or the establishment name and address.

Employers Who Are Required To File

Questions 1, 2 and 3 **MUST** be answered by all employers. If the answer to Question C-3 is "Yes", please enter the company's Dun and Bradstreet identification number if the company has one. If the answer is "Yes" to question 1, 2, or 3, complete the entire form. Otherwise skip to Section G.

Employment Data

Employment data must include **ALL** full-time and part-time employees who were employed during the selected payroll period, except those employees specifically excluded as indicated in the Appendix. Employees must be counted by sex and race or ethnic category for each of the ten occupational categories and subcategories. See Appendix for detailed explanation of job categories and race and ethnic identification.

Every employee must be accounted for in one and **ONLY** one of the categories in Columns A thru N.

Occupational Data—Employment data must be reported by job category. Report each employee in only one job category. In order to simplify and standardize the method of reporting, all jobs are considered as belonging in one of the broad occupations shown in the table. To assist you in determining where to place your jobs within the occupational categories, a description of job categories is in the ***EEO-1 Job Classification Guide*** or you may consult the "EEO-1-Census Codes Cross Walk" on the Commission's web site. For further clarification, you may wish to consult the Alphabetical and Classified Indices of Industries and Occupations (2000 Census) published by the U.S. Department of Commerce, Census Bureau.

Establishment Information

The major activity should be sufficiently descriptive to identify the industry and product produced or service provided. If an establishment is engaged in more than one activity, describe the activity at which the **greatest** number of employees work.

The description of the major activity indicated on the Headquarters' Report (Type 3) must reflect the dominant economic activity of the company in which the greatest number of employees are engaged.

Remarks

Include in this section any remarks, explanations, or other pertinent information regarding this report.

Certification

If all reports have been completed at headquarters, the authorized official should check Item 1 and sign the Consolidated Report only. If the reports have been completed by the individual establishments, the authorized official should check Item 2 and sign the establishment report.

APPENDIX

1. DEFINITIONS APPLICABLE TO ALL EMPLOYERS

a. "Commission" refers to the Equal Employment Opportunity Commission.

b. "OFCCP" refers to the Office of Federal Contract Compliance Programs, U.S. Department of Labor, established to implement Executive Order 11246, as amended.

c. "Joint Reporting Committee" is the committee representing the Commission and OFCCP for the purpose of administering this report system.

d. "Employer" under Section 701(b), Title VII of the Civil Rights Act of 1964, as amended, means a person engaged in an industry affecting commerce who has fifteen or more employees for each working day in each of twenty or more calendar weeks in the current or preceding calendar year, and any agent of such a person, but such term does not include the United States, a corporation wholly owned by the government of the United States, an Indian tribe, or any department or agency of the District of Columbia subject by statute to procedures of the competitive service (as defined in section 2102 of Title 5 of the United States Code), or a bona fide private membership club (other than a labor organization) which is exempt from taxation under Section 501(c) of the Internal Revenue Code of 1954; OR any person or entity subject to Executive Order 11246 who is a federal government prime contractor or subcontractor at any tier (including a bank or other establishment serving as a depository of federal government funds, or an issuing and paying agent of U.S. Savings Bonds and Notes, or a holder of a federal government bill of lading) or a federally-assisted construction prime contractor or subcontractor at any tier.

e. "Employee" means any individual on the payroll of an employer who is an employee for purposes of the employer's withholding of Social Security taxes except insurance sales agents who are considered to be employees for such purposes solely because of the provisions of 26 USC 3121 (d) (3) (B) (the Internal Revenue Code). Leased employees are included in this definition. Leased Employee means a permanent employee provided by an employment agency for a fee to an outside company for which the employment agency handles all personnel tasks including payroll, staffing, benefit payments and compliance reporting. The employment agency shall, therefore, include leased employees in its EEO-1 report. The term "employee" SHALL NOT include persons who are hired on a casual basis for a specified time, or for the duration of a specified job (for example, persons at a construction site whose employment relationship is expected to terminate with the end of the employee's work at the site); persons temporarily employed in any industry other than construction, such as temporary office workers, mariners, stevedores, lumber yard workers, etc., who are hired through a hiring hall or other referral arrangement, through an employee contractor or agent, or by some individual hiring arrangement, or persons **(EXCEPT** leased employees) on the payroll of an employment agency who are referred by such agency for work to be performed on the premises of another employer under that employer's direction and control.

It is the opinion of the General Counsel of the Commission that Section 702, Title VII of the Civil Rights Act of 1964, as

amended, does not authorize a complete exemption of religious organizations from the coverage of the Act or of the reporting requirements of the Commission. The exemption for religious organizations applies to discrimination on the basis of religion. Therefore, since the Standard Form 100 does not provide for information as to the religion of employees, religious organizations must report all information required by this form.

f. "Commerce" means trade, traffic, commerce, transportation, transmission, or communication among the several States; or between a State and any place outside thereof; or within the District of Columbia, or a possession of the United States; or between points in the same State but through a point outside thereof.

g. "Industry Affecting Commerce" means any activity, business or industry in commerce or in which a labor dispute would hinder or obstruct commerce or the free flow of commerce and includes any activity or industry "affecting commerce" within the meaning of the Labor Management Reporting and Disclosure Act of 1959. Any employer of 15 or more persons is presumed to be in an "industry affecting commerce."

h. "Establishment" is an economic unit which produces goods or services, such as a factory, office, store, or mine. In most instances, the establishment is at a single physical location and is engaged in one, or predominantly one, type of economic activity. (definition adapted from the ***North American Industry Classification System - 2002***).

Units at different physical locations, even though engaged in the same kind of business operation, must be reported as separate establishments. For locations involving construction, transportation, communications, electric, gas, and sanitary services, oil and gas fields, and similar types of physically dispersed industrial activities, however, it is not necessary to list separately each individual site, project, field, line, etc., unless it is treated by you as a separate legal entity. For these types of activities, list as establishments only those relatively permanent main or branch offices, terminals, stations etc., which are either: (a) directly responsible for supervising such dispersed activities; or (b) the base from which personnel and equipment operate to carry out these activities. (Where these dispersed activities cross State lines, at least one such "establishment" should be listed for each State involved.)

i. "Major Activity" means the major product or group of products produced or handled, or services rendered by the reporting unit (e.g., manufacturing airplane parts, retail sales of office furniture) in terms of the activity at which the greatest number of all employees work. The description includes the type of product manufactured or sold or the type of service provided.

2. DEFINITIONS APPLICABLE ONLY TO GOVERNMENT CONTRACTORS SUBJECT TO EXECUTIVE ORDER 11246

a. "Order" means Executive Order 11246, as amended.

b. "Contract" means any government contract or any federally-assisted construction contract.

c. "Prime Contractor" means any employer having a government contract or any federally-assisted construction contract, or any employer serving as a depository of federal government funds.

d. "Subcontractor" means any employer having a contract with a prime contractor or another subcontractor calling for supplies or services required for the performance of a government contract or federally assisted construction contract.

e. "Contracting Agency" means any department, agency and establishment in the executive branch of the government, including any wholly-owned government corporation, which enters into contracts.

f. "Administering Agency" means any department, agency and establishment in the executive branch of the government, including any wholly-owned government corporation, which administers a program involving federally-assisted construction contracts.

3. RESPONSIBILITIES OF PRIME CONTRACTORS

a. At the time of an award of a subcontract subject to these reporting requirements, the prime contractor shall inform the subcontractor of its responsibility to submit annual EEO-1 employment data in accordance with these instructions.

b. If prime contractors are required by their Contracting Officer or subcontractors by their prime contractors, to submit notification of filing, they shall do so by ordinary correspondence. However, such notification is not required by and should not be sent to the Joint Reporting Committee.

4. RACE AND ETHNIC IDENTIFICATION

Self-identification is the preferred method of identifying the race and ethnic information necessary for the EEO-1 report. Employers are required to attempt to allow employees to use self-identification to complete the EEO-1 report. If an employee declines to self-identify, employment records or observer identification may be used.

Where records are maintained, it is recommended that they be kept separately from the employee's basic personnel file or other records available to those responsible for personnel decisions.

Race and ethnic designations as used by the Equal Employment Opportunity Commission do not denote scientific definitions of anthropological origins. Definitions of the race and ethnicity categories are as follows:

Hispanic or Latino - A person of Cuban, Mexican, Puerto Rican, South or Central American, or other Spanish culture or origin regardless of race.

White (Not Hispanic or Latino) - A person having origins in any of the original peoples of Europe, the Middle East, or North Africa.

Black or African American (Not Hispanic or Latino) - A person having origins in any of the black racial groups of Africa.

Native Hawaiian or Other Pacific Islander (Not Hispanic or Latino) - A person having origins in any of the peoples of Hawaii, Guam, Samoa, or other Pacific Islands.

Asian (Not Hispanic or Latino) - A person having origins in any of the original peoples of the Far East, Southeast Asia, or the Indian Subcontinent, including, for example, Cambodia, China, India, Japan, Korea, Malaysia, Pakistan, the Philippine Islands, Thailand, and Vietnam.

American Indian or Alaska Native (Not Hispanic or Latino) - A person having origins in any of the original peoples of North and South America (including Central America), and who maintain tribal affiliation or community attachment.

Two or More Races (Not Hispanic or Latino) - All persons who identify with more than one of the above five races.

Instructions for assigning employees into the race/ethnic categories:

Hispanic or Latino - Include all employees who answer YES to the question, "Are you Hispanic or Latino". Report all Hispanic males in Column A and Hispanic females in Column B.

White (Not Hispanic or Latino) - Include all employees who identify as White males in Column C and as White females in Column I.

Black or African American (Not Hispanic or Latino)- Include all employees who identify as Black males in Column D and as Black females in Column J.

Native Hawaiian or Other Pacific Islander (Not Hispanic or Latino) - Include all employees who identify as Native Hawaiian or Other Pacific Islander males in Column E and as Native Hawaiian or Other Pacific Islander females in Column K.

Asian (Not Hispanic or Latino) - Include all employees who identify as Asian males in Column F and as Asian females in Column L.

American Indian or Alaska Native (Not Hispanic or Latino) - Include all employees who identify as American Indian or Alaska Native males in Column G and as American Indian or Alaska Native females in Column M.

Two or More Races (Not Hispanic or Latino) - Report all male employees who identify with more than one of the above five races in Column H and all female employees who identify with more than one of the above five races in Column N.

As to the method of collecting data, the basic principles for ethnic and racial self-identification for purposes of the EEO-1 report are:

(1) Offer employees the opportunity to self-identify

(2) Provide a statement about the voluntary nature of this inquiry for employees. For example, language such as the following may be used (employers may adapt this language):

> "The employer is subject to certain governmental recordkeeping and reporting requirements for the administration of civil rights laws and regulations. In order to comply with these laws, the employer invites employees to voluntarily self-identify their race or ethnicity. Submission of this information is voluntary and refusal to provide it will not subject you to any adverse treatment. The information obtained will be kept confidential and may only be used in accordance with the provisions of applicable laws, executive orders, and regulations, including those that require the information to be summarized and reported to the federal government for civil rights enforcement. When reported, data will not identify any specific individual."

5. DESCRIPTION OF JOB CATEGORIES

The major job categories are listed below, including a brief description of the skills and training required for occupations in that category and examples of the job titles that fit each category. The examples shown below are illustrative and not intended to be exhaustive of all job titles in a job category. These job categories are primarily based on the average skill level, knowledge, and responsibility involved in each occupation within the job category.

The Officials and Managers category as a whole is to be divided into the following two subcategories: Executive/Senior Level Officials and Managers and First/Mid Level Officials and Managers. These subcategories are intended to mirror the employer's own well established hierarchy of management positions. Small employers who may not have two well-defined hierarchical steps of management should report their management employees in the appropriate categories.

Executive/Senior Level Officials and Managers. Individuals who plan, direct and formulate policies, set strategy and provide the overall direction of enterprises/organizations for the development and delivery of products or services, within the parameters approved by boards of directors or other governing bodies. Residing in the highest levels of organizations, these executives plan, direct or coordinate activities with the support of subordinate executives and staff managers. They include, in larger organizations, those individuals within two reporting levels of the CEO, whose responsibilities require frequent interaction with the CEO. Examples of these kinds of managers are: chief executive officers, chief operating officers, chief financial officers, line of business heads, presidents or executive vice presidents of functional areas or operating groups, chief information officers, chief human resources officers, chief marketing officers, chief legal officers, management directors and managing partners.

First/Mid Level Officials and Managers. Individuals who serve as managers, other than those who serve as Executive/Senior Level Officials and Managers, including those who oversee and direct the delivery of products, services or functions at group, regional or divisional levels of organizations. These managers receive directions from the Executive/Senior Level management and typically lead major business units. They implement policies, programs and directives of executive/senior management through subordinate managers and within the parameters set by Executive/Senior Level management. Examples of these kinds of managers are: vice presidents and directors, group, regional or divisional controllers; treasurers; human resources, information systems, marketing, and operations managers. The First/Mid Level Officials and Managers subcategory also includes those who report directly to middle managers. These individuals serve at functional, line of business segment or branch levels and are responsible for directing and executing the day-to-day operational objectives of enterprises/organizations, conveying the directions of higher level officials and managers to subordinate personnel and, in some instances, directly supervising the activities of exempt and non-exempt personnel. Examples of these kinds of managers are: first-line managers; team managers; unit managers; operations and production mangers; branch managers; administrative services managers; purchasing and transportation managers; storage and distribution managers; call center or customer service managers; technical support managers; and brand or product mangers.

Professionals. Most jobs in this category require bachelor and graduate degrees, and/or professional certification. In some instances, comparable experience may establish a person's qualifications. Examples of these kinds of positions include: accountants and auditors; airplane pilots and flight engineers; architects; artists; chemists; computer programmers; designers; dieticians; editors; engineers; lawyers; librarians; mathematical scientists; natural scientists; registered nurses; physical scientists; physicians and surgeons; social scientists; teachers; and surveyors.

Technicians. Jobs in this category include activities that require applied scientific skills, usually obtained by post secondary education of varying lengths, depending on the particular occupation, recognizing that in some instances additional training,

certification, or comparable experience is required. Examples of these types of positions include: drafters; emergency medical technicians; chemical technicians; and broadcast and sound engineering technicians.

Sales Workers. These jobs include non-managerial activities that wholly and primarily involve direct sales. Examples of these types of positions include: advertising sales agents; insurance sales agents; real estate brokers and sales agents; wholesale sales representatives; securities, commodities, and financial services sales agents; telemarketers; demonstrators; retail salespersons; counter and rental clerks; and cashiers.

Administrative Support Workers. These jobs involve non-managerial tasks providing administrative and support assistance, primarily in office settings. Examples of these types of positions include: office and administrative support workers; bookkeeping; accounting and auditing clerks; cargo and freight agents; dispatchers; couriers; data entry keyers; computer operators; shipping, receiving and traffic clerks; word processors and typists; proofreaders; desktop publishers; and general office clerks.

Craft Workers (formerly Craft Workers (Skilled)). Most jobs in this category includes higher skilled occupations in construction (building trades craft workers and their formal apprentices) and natural resource extraction workers. Examples of these types of positions include: boilermakers; brick and stone masons; carpenters; electricians; painters (both construction and maintenance); glaziers; pipelayers, plumbers, pipefitters and steamfitters; plasterers; roofers; elevator installers; earth drillers; derrick operators; oil and gas rotary drill operators; and blasters and explosive workers. This category also includes occupations related to the installation, maintenance and part replacement of equipment, machines and tools, such as: automotive mechanics; aircraft mechanics; and electric and electronic equipment repairers. This category also includes some production occupations that are distinguished by the high degree of skill and precision required to perform them, based on clearly defined task specifications, such as: millwrights; etchers and engravers; tool and die makers; and pattern makers.

Operatives (formerly Operatives (Semi-skilled)). Most jobs in this category include intermediate skilled occupations and include workers who operate machines or factory-related processing equipment. Most of these occupations do not usually require more than several months of training. Examples include: textile machine workers; laundry and dry cleaning workers; photographic process workers; weaving machine operators; electrical and electronic equipment assemblers; semiconductor processors; testers, graders and sorters; bakers; and butchers and other meat, poultry and fish processing workers. This category also includes occupations of generally intermediate skill levels that are concerned with operating and controlling equipment to facilitate the movement of people or materials, such as: bridge and lock tenders; truck, bus or taxi drivers; industrial truck and tractor (forklift) operators; parking lot attendants; sailors; conveyor operators; and hand packers and packagers.

Laborers and Helpers (formerly Laborers (Unskilled)). Jobs in this category include workers with more limited skills who require only brief training to perform tasks that require little or no independent judgment. Examples include: production and construction worker helpers; vehicle and equipment cleaners; laborers; freight, stock and material movers; service station attendants; construction laborers; refuse and recyclable materials collectors; septic tank servicers; and sewer pipe cleaners.

Service Workers. Jobs in this category include food service, cleaning service, personal service, and protective service activities. Skill may be acquired through formal training, job-related training or direct experience. Examples of food service positions include: cooks; bartenders; and other food service workers. Examples of personal service positions include: medical assistants and other healthcare support positions; hairdressers; ushers; and transportation attendants. Examples of cleaning service positions include: cleaners; janitors; and porters. Examples of protective service positions include: transit and railroad police and fire fighters; guards; private detectives and investigators.

6. LEGAL BASIS FOR REQUIREMENTS

SECTION 709(c), TITLE VII, CIVIL RIGHTS ACT OF 1964, AS AMENDED

Recordkeeping; reports

Every employer, employment agency, and labor organization subject to this title shall (1) make and keep such records relevant to the determinations of whether unlawful employment practices have been or are being committed, (2) preserve such records for such periods, and (3) make such reports therefrom as the Commission shall prescribe by regulation or order, after public hearing, as reasonable, necessary, or appropriate for the enforcement of this title or the regulations or orders thereunder. The Commission shall, by regulation, require each employer, labor organization, and joint labor-management committee subject to this title which controls an apprenticeship or other training program to maintain such records as are reasonably necessary to carry out the purposes of this title, including, but not limited to, a list of applicants who wish to participate in such program, including the chronological order in which applications were received, and to furnish to the Commission upon request, a detailed description of the manner in which persons are selected to participate in the apprenticeship or other training program. Any employer, employment agency, labor organization, or joint labor-management committee which believes that the application to it of any regulation or order issued under this section would result in undue hardship may apply to the Commission for an exemption from the application of such regulation or order, and, if such application for an exemption is denied, bring a civil action in the United States District Court for the district where such records are kept. If the Commission or the court, as the case may be, finds that the application of the regulation or order to the employer, employment agency, or labor organization in question would impose an undue hardship, the Commission or the court, as the case may be, may grant appropriate relief. If any person required to comply with the provisions of this subsection fails or refuses to do so, the United States District Court for the district in which such person is found, resides, or transacts business, shall, upon application of the Commission, or the Attorney General in a case involving a government, governmental agency or political subdivision, have jurisdiction to issue to such person an order requiring him to comply.

TITLE 29, CHAPTER XIV CODE OF FEDERAL REGULATIONS

NOTE: A few aspects of the following regulations will need to be revised to conform with the EEO-1 Report to be used beginning with the 2007 reporting period.

Subpart B—Employer Information Report

§1602.7 Requirement for filing of report.

On or before September 30 of each year, every employer that is subject to Title VII of the Civil Rights Act of 1964, as amended,

and that has 100 or more employees, shall file with the Commission or its delegate executed copies of Standard Form 100, as revised (otherwise known as "Employer Information Report EEO-1"), in conformity with the directions set forth in the form and accompanying instructions. Notwithstanding the provisions of §1602.14, every such employer shall retain at all times at each reporting unit, or at company or divisional headquarters, a copy of the most recent report filed for each such unit and shall make the same available if requested by an officer, agent, or employee of the Commission under the authority of section 710 of Title VII. Appropriate copies of Standard Form 100 in blank will be supplied to every employer known to the Commission to be subject to the reporting requirements, but it is the responsibility of all such employers to obtain necessary supplies of the form from the Commission or its delegate prior to the filing date.

§1602.8 Penalty for making of willfully false statements on report.

The making of willfully false statements on Report EEO-1 is a violation of the United States Code, Title 18, section 1001, and is punishable by fine or imprisonment as set forth therein.

§ 1602.9 Commission's remedy for employer's failure to file report.

Any employer failing or refusing to file Report EEO-1 when required to do so may be compelled to file by order of a U.S. District Court, upon application of the Commission.

§ 1602.10 Employer's exemption from reporting requirements.

If an employer claims that the preparation or filing of the report would create undue hardship, the employer may apply to the Commission for an exemption from the requirements set forth in this part, according to instruction 5. If an employer is engaged in activities for which the reporting unit criteria described in section 5 of the instructions are not readily adaptable, special reporting procedures may be required. If an employer seeks to change the date for filing its Standard Form 100 or seeks to change the period for which data are reported, an alternative reporting date or period may be permitted. In such instances, the employer should so advise the Commission by submitting to the Commission or its delegate a specific written proposal for an alternative reporting system prior to the date on which the report is due.

§ 1602.11 Additional reporting requirements.

The Commission reserves the right to require reports, other than that designated as the Employer Information Report EEO-1, about the employment practices of individual employers or groups of employers whenever, in its judgment, special or supplemental reports are necessary to accomplish the purposes of Title VII or the Americans with Disabilities Act (ADA). Any system for the requirement of such reports will be established in accordance with the procedures referred to in section 709(c) of Title VII or section 107 of the ADA and as otherwise prescribed by law.

Subpart C—Recordkeeping by Employers

§ 1602.12 Records to be made or kept.

The Commission has not adopted any requirement, generally applicable to employers, that records be made or kept. It reserves the right to impose recordkeeping requirements upon individual employers or groups of employers subject to its jurisdiction whenever, in its judgment, such records (a) are necessary for the effective operation of the EEO-1 reporting system or of any special or supplemental reporting system as described above; or (b) are further required to accomplish the purposes of Title VII or the ADA. Such recordkeeping requirements will be adopted in accordance with the procedures referred to in section 709(c) of Title VII, or section 107 of the ADA, and otherwise prescribed by law.

§ 1602.13 Records as to racial or ethnic identity of employees.

Employers may acquire the information necessary for completion of items 5 and 6 of Report EEO-1 either by visual surveys of the work force, or at their option, by the maintenance of post-employment records as to the identity of employees where the same is permitted by State law. In the latter case, however, the Commission recommends the maintenance of a permanent record as to the racial or ethnic identity of an individual for purpose of completing the report form only where the employer keeps such records separately from the employee's basic personnel form or other records available to those responsible for personnel decisions, e.g., as part of an automatic data processing system in the payroll department.

§ 1602.14 Preservation of records made or kept.

Any personnel or employment record made or kept by an employer (including but not necessarily limited to requests for reasonable accommodation, application forms submitted by applicants and other records having to do with hiring, promotion, demotion, transfer, lay-off or termination, rates of pay or other terms of compensation, and selection for training or apprenticeship) shall be preserved by the employer for a period of one year from the date of the making of the record or the personnel action involved, whichever occurs later. In the case of involuntary termination of an employee, the personnel records of the individual terminated shall be kept for a period of one year from the date of termination. Where a charge of discrimination has been filed, or an action brought by the Commission or the Attorney General, against an employer under Title VII or the ADA, the respondent employer shall preserve all personnel records relevant to the charge or action until final disposition of the charge or the action. The term "personnel records relevant to the charge," for example, would include personnel or employment records relating to the aggrieved person and to all other employees holding positions similar to that held or sought by the aggrieved person and application forms or test papers completed by an unsuccessful applicant and by all other candidates for the same position as that for which the aggrieved person applied and was rejected. The date of *final disposition of the charge or the action* means the date of expiration of the statutory period within which the aggrieved person may bring an action in a U. S. District Court or, where an action is brought against an employer either by the aggrieved person, the Commission, or by the Attorney General, the date on which such litigation is terminated.

Joint Reporting Committee
- Equal Employment Opportunity Commission
- Office of Federal Contract Compliance Programs (Labor)

EQUAL EMPLOYMENT OPPORTUNITY

EMPLOYER INFORMATION REPORT EEO—1

Standard Form 100
REV. 01/2006

O.M.B. No. 3048-0007
EXPIRES 01/2009
100-214

Section A—TYPE OF REPORT

Refer to instructions for number and types of reports to be filed.

1. Indicate by marking in the appropriate box the type of reporting unit for which this copy of the form is submitted (MARK ONLY ONE BOX).

(1) ☐ Single-establishment Employer Report

Multi-establishment Employer:
(2) ☐ Consolidated Report (Required)
(3) ☐ Headquarters Unit Report (Required)
(4) ☐ Individual Establishment Report (submit one for each establishment with 50 or more employees)
(5) ☐ Special Report

2. Total number of reports being filed by this Company (Answer on Consolidated Report only) _____

Section B—COMPANY IDENTIFICATION *(To be answered by all employers)*

OFFICE USE ONLY

1. Parent Company

a. Name of parent company (owns or controls establishment in item 2) omit if same as label — a.

Address (Number and street) — b.

City or town	State	ZIP code	c.

2. Establishment for which this report is filed. (Omit if same as label)

a. Name of establishment — d.

Address (Number and street)	City or Town	County	State	ZIP code	e.

b. Employer identification No. (IRS 9-DIGIT TAX NUMBER) | | | | | | | | | | f.

c. Was an EEO–1 report filed for this establishment last year? ☐ Yes ☐ No

Section C—EMPLOYERS WHO ARE REQUIRED TO FILE *(To be answered by all employers)*

☐ Yes ☐ No 1. Does the entire company have at least 100 employees in the payroll period for which you are reporting?

☐ Yes ☐ No 2. Is your company affiliated through common ownership and/or centralized management with other entities in an enterprise with a total employment of 100 or more?

☐ Yes ☐ No 3. Does the company or any of its establishments (a) have 50 or more employees AND (b) is not exempt as provided by 41 CFR 60–1.5, AND either (1) is a prime government contractor or first-tier subcontactor, and has a contract, subcontract, or purchase order amounting to $50,000 or more, or (2) serves as a depository of Government funds in any amount or is a financial institution which is an issuing and paying agent for U.S. Savings Bonds and Savings Notes?

If the response to question C–3 is yes, please enter your Dun and Bradstreet identification number (if you have one): ☐☐☐☐☐☐☐☐☐

NOTE: If the answer is yes to questions 1, 2, or 3, complete the entire form, otherwise skip to Section G.

Section D-EMPLOYMENT DATA

Employment at this establishment – Report all permanent full- and part-time employees including apprentices and on-the-job trainees unless specifically excluded as set forth in the instructions. Enter the appropriate figures on all lines and in all columns. Blank spaces will be considered as zeros.

Job Categories	Number of Employees (Report employees in only one category)														
	Race/Ethnicity														
	Hispanic or Latino		Not-Hispanic or Latino												Total Col A - N
			Male						Female						
	Male	Female	White	Black or African American	Native Hawaiian or Other Pacific Islander	Asian	American Indian or Alaska Native	Two or more races	White	Black or African American	Native Hawaiian or Other Pacific Islander	Asian	American Indian or Alaska Native	Two or more races	
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Executive/Senior Level Officials and Managers 1.1															
First/Mid-Level Officials and Managers 1.2															
Professionals 2															
Technicians 3															
Sales Workers 4															
Administrative Support Workers 5															
Craft Workers 6															
Operatives 7															
Laborers and Helpers 8															
Service Workers 9															
TOTAL 10															
PREVIOUS YEAR TOTAL 11															

1. Date(s) of payroll period used: _____ (Omit on the Consolidated Report.)

Section E - ESTABLISHMENT INFORMATION (Omit on the Consolidated Report.)

1. What is the major activity of this establishment? (Be specific, i.e., manufacturing steel castings, retail grocer, wholesale plumbing supplies, title insurance, etc. Include the specific type of product or type of service provided, as well as the principal business or industrial activity.)

Section F - REMARKS

Use this item to give any identification data appearing on the last EEO-1 report which differs from that given above, explain major changes in composition of reporting units and other pertinent information.

Section G - CERTIFICATION

Check one
1 ☐ All reports are accurate and were prepared in accordance with the instructions. (Check on Consolidated Report only.)
2 ☐ This report is accurate and was prepared in accordance with the instructions.

Name of Certifying Official	Title	Signature	Date
Name of person to contact regarding this report	Title	Address (Number and Street)	
City and State	Zip Code	Telephone No. (including Area Code and Extension)	Email Address

All reports and information obtained from individual reports will be kept confidential as required by Section 709(e) of Title VII.
WILLFULLY FALSE STATEMENTS ON THIS REPORT ARE PUNISHABLE BY LAW, U.S. CODE, TITLE 18, SECTION 1001

Federal Sector

Overview

Federal Employees & Applicants

Federal EEO Coordination

Federal Agency EEO Directors

Laws, Regulations & Guidance

Management Directives & Federal Sector Guidance

Federal Sector Alternative Dispute Resolution

Federal Sector Reports

Appellate Decisions

Digest of EEO Law

Form 462 Reporting

Federal Training & Outreach

Home > Federal Agencies > Management Directives

+ Share

Frequently Asked Questions About Management Directive-715

Management Directive 715 (MD-715) is the policy guidance which the Equal Employment Opportunity Commission (EEOC) provides to federal agencies for their use in establishing and maintaining effective programs of equal employment opportunity under Section 717 of Title VII of the Civil Rights Act of 1964 (Title VII), as amended, 42 U.S.C. § 2000e *et seq.*, and Section 501 of the Rehabilitation Act of 1973 (Rehabilitation Act), as amended, 29 U.S.C. § 791 *et seq*. MD-715 provides a roadmap for creating effective equal employment opportunity (EEO) programs for all federal employees as required by Title VII and the Rehabilitation Act. MD-715 took effect on October 1, 2003.

The Instructions to Federal Agencies for Equal Employment Opportunity Management Directive 715 (Instructions) set forth general reporting requirements for federal agencies.

A copy of MD-715 and the Instructions are available on the EEOC's web site: http://www.eeoc.gov/federal/directives/index.cfm. Also available are PARTS A through J of EEOC FORM 715-01 (in HTML, PDF, and MS WORD), the Workforce Data Tables (in HTML, MS WORD and EXCEL), the Department or Agency List with Second Level Reporting Components, Guidance on Completing the EEOC Form 715-01 Workforce Data Tables and links to the OPM/Census Occupation Cross-Classification Table and the Census EEO 2000 Data Tool.

The following questions are those which have been most frequently asked by persons who have read MD-715 and the Instructions.

GENERAL QUESTIONS

1. What format may I use to submit the MD-715 report and the applicable Workforce Data Tables? Access? Text?

At the present time, your MD-715 report (FORM 715-01, all supporting documentation, and all the Workforce Data Tables) must be submitted to the EEOC in hard copy format. All data must be identified and arranged in the same manner as shown in the Workforce Data Tables.

2. How do I know if I am a 2nd level, 3rd level or 4th level reporting component?

Most federal agencies have subordinate components, but not every subordinate component is a subordinate **reporting** component for purposes of filing under MD-715. A subordinate

reporting component, *i.e.*, a second, third or fourth level **reporting** component, is one that enjoys a certain amount of autonomy from its parent agency. In other words, does the subordinate component have its own personnel system, finance department, recruitment structure, culture, etc? Or is the component simply a regional office that operates more as an extension of the parent? If the component is closer to being independent, then it is considered a subordinate **reporting** component.

For example, the Department of Justice (DoJ) is a parent agency with several subordinate components. Some of those subordinate components, like the Federal Bureau of Investigation (FBI), Drug Enforcement Agency, etc., operate independently (albeit under the umbrella of DoJ); they have their own recruitment programs, personnel systems, culture, etc. Thus, the FBI is a 2nd level **reporting** component. Compare the FBI to the Baltimore District Office of the EEOC. The Baltimore District Office is not an independent entity, but rather a spoke on the wheel, with EEOC headquarters at the center.

The majority of federal agencies do not have 2nd level **reporting** components, and even fewer will have a 3rd or 4th level **reporting** component, because very few agencies have independent and autonomous entities under their second level components. One example of a 3rd level **reporting** component would be the National Weather Service (NWS). The parent agency is the Department of Commerce. Under Commerce is the National Oceanic and Atmospheric Administration (NOAA), which meets the definition of a second level **reporting** component. NWS comes under NOAA and meets the same definition.

Contrast NWS with FBI's New York District Office (NYDO). The Department of Justice is a parent agency with several subordinate components. The Federal Bureau of Investigation is one such component that is greatly autonomous from Justice. Thus, it is a 2nd level **reporting** component. Under FBI, there are several regional offices, including the New York District Office. The FBI-NYDO is not a subordinate **reporting** component. It has no filing requirements under MD-715. Note, however, that this does not mean the FBI-NYDO has no responsibility under MD-715! See FAQ No. 9, below.

The EEOC has developed a Department or Agency List with Second Level Reporting Components, which may be accessed through the following link: http://www.eeoc.gov/federal/agencylist.cfm

Please contact Lori Grant at 202 663-4616 or lori.grant@eeoc.gov if you believe that your agency or department has a Second Level Reporting Component which should have been included on this list or if you believe such a component has been included erroneously.

3. What about very large regional offices that are not considered subordinate *reporting* components? Does the above definition mean that those subordinate components do not have any responsibilities under MD-715?

Absolutely not. **All entities that make up a federal agency have responsibilities under MD-715.** A federal agency needs to work closely with all of its subordinate entities in order to ensure that the agency itself can perform a Model EEO self-assessment and undertake a comprehensive barrier analysis to identify barriers and execute plans for eliminating them **throughout its workforce**, as well as to maintain an effective, **agency-wide** special recruitment program which establishes specific goals for the employment and advancement of individuals with targeted disabilities.

Continuing the example from above, the Baltimore District Office of the EEOC is required to conduct a self-assessment of its EEO program and a barrier analysis of its workplace. Deficiencies identified in the self-assessment and barriers uncovered must be addressed and corrective plans must be developed and instituted. All this information (the self-assessment, the corrective plans, etc.) will then be rolled up to EEOC headquarters to be used in completing the ***overall*** EEOC MD-715 report. EEOC headquarters can't possibly report on the entire Commission without the input of all subordinate entities (regional, district and field offices).

Similarly, the FBI-NYDO will have to engage in the Model EEO self-assessment and perform a thorough barrier

analysis. Plans to address identified deficiencies and barriers will need to be developed and instituted. These plans will be rolled up to FBI headquarters for inclusion in its Bureau-wide report. Additionally, FBI headquarters will roll up its information to Justice for inclusion in the department-wide report. The important distinction to understand is that, **regardless of whether a subordinate entity has to file a report with the EEOC, all of the activities required by MD 715 have to be done either by or for all of an agency's entities - whether those entities are termed major commands, post offices, small air bases, regional centers, etc.**

4. I have subordinate components that are reporting components. Who and where do they report to, and what are they reporting?

Second Level Reporting Components which have 1,000 or more employees in permanent full or part time appointments must submit MD-715 reports (FORM 715-01, PARTS A-F and H-J and all Workforce Data Tables) to their agency headquarters for inclusion in the agency-wide report and for submission by the parent to the EEOC. Second Level Reporting Components with 500 or more (but fewer than 1,000) employees in permanent full or part time appointments must file MD-715 reports with PARTS A-F and H-I and Workforce Data Tables A/B 1-7 with their agency headquarters for inclusion in the agency-wide report and maintain a copy.

See The Quick Guide in Section III of the Instructions, available at the following link: http://www.eeoc.gov/federal/715instruct/section3.html.

5. My agency has several Second Level Reporting Components. Must the agency's MD-715 report include all of the PART Hs, Is and Js prepared by its Second Level Reporting Components?

No. The agency's overall MD-715 Report may incorporate these by reference. However, the MD-715 report filed by the parent agency (i.e., the agency-wide report) should include the PART Hs, Is and Js to be addressed at the headquarters level. Please note that ultimately, it is the agency itself which is responsible for ensuring that a Model EEO self-assessment and a comprehensive barrier analysis to identify barriers and execute plans for eliminating them have been conducted **throughout its workforce**, and for ensuring that the agency maintains an effective, **agency-wide** special recruitment program which establishes specific goals for the employment and advancement of individuals with targeted disabilities.

6. Should a Second Level Reporting Component file its MD-715 report directly with the Commission or should it first submit its MD-715 report to its parent agency?

As previously noted, a federal agency needs to work closely with all of its subordinate entities in order to ensure that the agency itself can perform a Model EEO self-assessment and undertake a comprehensive barrier analysis to identify barriers and execute plans for eliminating them **throughout its workforce**, as well as to maintain an effective, **agency-wide** special recruitment program which establishes specific goals for the employment and advancement of individuals with targeted disabilities. Thus, an agency's EEO Director ultimately is responsible for ensuring equal opportunity throughout the entire agency.

Accordingly, all Second Level Reporting Components should first submit their MD-715 reports to their parent agency's EEO Director for review and coordination. The parent agency should submit a complete package of MD-715 reports to the EEOC. Therefore, those agencies which have Second Level Reporting Components need to seriously consider the date by which these entities must gather and analyze all necessary data and information and to perform the required MD 715 exercises, in order to complete the review and coordination process well in advance of the January 31 due date. Practically speaking, since subordinate components, whether they are reporting components or not, make up the report of the parent entity, the parent entity will need its subordinate's MD-715 report well in advance of January 31. Parent agencies should keep this in mind when setting internal deadlines for subordinate components, and take care to have in place a procedure which will ensure that the review of a subordinate component's MD-715 report will be concluded in sufficient time to allow required MD-715 reports to be filed by January 31.

MODEL EEO PROGRAMS AND BARRIER QUESTIONS

7. What should be done under MD-715 when a particular group has a low participation rate?

A low participation rate should be taken as a "trigger," a situation which alerts the agency to the possible existence of a barrier to equal opportunity. An agency should identify the likely factor (or combination of factors) which has adversely affected the employment opportunities of the group in question. Depending on the nature of the potential problem, an agency could consider a variety of questions. For example, if a particular group has a low participation rate in a particular occupation, the agency should determine whether recruitment efforts are resulting in a diverse pool of applicants. In this regard, it should be noted that actions designed to increase the number of applications for employment from a particular group are unaffected by *Adarand*. See DoJ Memorandum at pp. 3-4.

If the applicant pool includes a cross-section of qualified applicants, the agency should explore whether there is a significant disparity between a group's proportionate representation in the applicant pool and the pool of selectees. If so, the agency needs to explore why. Are there selection criteria that tend to screen out the group in question?

If there is a situation where the participation rate for a group occupying a higher level position is lower than the corresponding participation rate in the lower level feeder pool for that position, the agency should review its merit promotion processes and may also need to review related processes, such as career development programs, appraisal systems and/or awards programs, for barriers affecting the group's advancement to the next level.

Numerous other examples of questions which should be addressed during a thorough investigation of a potential barrier in an assortment of employment processes are found in Section II of the Instructions to Federal Agencies for Equal Employment Opportunity Management Directive 715.

8. My agency has identified many areas where our EEO Programs are deficient and numerous areas which should be explored for barriers. How can we be expected to file so many PART Hs and PART Is?

We suggest that your agency first determine whether any of the program deficiencies are interrelated and could, therefore, be addressed in a comprehensive manner which can be set forth in a single PART H. In addition, an agency may need to prioritize its needs. If an agency will be unable to address the deficiency during the Fiscal Year in question (whether due to budget, lack of personnel or other reasons), the deficiency should be identified in a PART H together with at least a general indication of the agency's current plans to address the deficiency in an identified, subsequent Fiscal Year.

Similarly, a through and systematic analysis may identify certain barriers which are interrelated and could, therefore, be addressed in a comprehensive manner which can be set forth in a single PART I. In addition, if an agency is unable to explore data, an employment process, or other sources for possible barriers during the Fiscal Year in question (whether due to budget, lack of personnel or other reasons), the barrier should be identified in a PART I together with a general indication of the agency's current plans to perform an analysis to determine the cause of the condition and develop measurable objectives to correct the undesired condition address the barrier in an identified, subsequent Fiscal Year.

9. Do you have any suggestions as to how the data gathered in my agency's Form 462 Report could be utilized in conducting a barrier analysis under MD-715?

Yes. An agency is required to examine any policy, principle or practice that limits or tends to limit employment opportunities for members of a particular sex, race or ethnic background, or based on an individual's disability status. An analysis of the Form 462 data relating to the nature and disposition of EEO complaints can provide useful insight into the extent to which an agency is meeting its obligations under Title VII and the Rehabilitation Act and, thus, may help an agency to identify areas where barriers may be operating to limit certain groups.

For example, an analysis may reveal that there are certain trends in the types of complaints being filed or

problem areas within the agency. Does the data reveal an increase in complaints about employee development or training? How about promotions? Awards? Disciplinary actions? If the answer to any of these questions is 'yes,' then an agency should study the data further to determine if there is an identifiable trend - is a particular group making a significant percentage of the complaints? Is the increase attributable to a certain facility, office, region, etc.? Do complaints about promotion, for example, tend to involve a particular stage of the promotion process or procedures? Do complaints involving reasonable accommodation issues also involve failures to comply with the agency's reasonable accommodation procedures? Has a union, ombudsman, employee advocacy group, special emphasis group or other group also raised concerns about the area in question?

In addition, note that the 462 data also is invaluable in assessing whether your agency's EEO program is meeting the 6 essential elements of a model EEO program. If the data reveals that complaints are not being processed within the regulatory time frame, the 462 will allow you to determine what stage of the process needs attention: Is counseling completed in a timely manner? Does the problem lie with timely completion of investigations? If your agency does both, is there a significant difference in timeliness between in-house and contract investigations? Is the agency's information collection system accurate and adequate for purposes of completing the Form 462? Any deficiencies in these areas also need to be addressed in the 715 report.

10. Please discuss the impact of the Supreme Court's decision in *Adarand* and its applicability to agencies' affirmative employment programs.

In *Adarand Constructors, Inc. v. Pena*, 515 U.S. 200 (1995), the U.S. Supreme Court held that all racial classifications imposed by a federal, state, or local government must be analyzed by a reviewing court under "strict scrutiny," meaning that such classifications are constitutional only if they are narrowly tailored measures that further compelling government interests. The *Adarand* case arose under the Equal Protection clause of the U.S. Constitution regarding a federal program that provided financial incentives for contractors to hire subcontractors controlled by socially and economically disadvantaged groups, which included various racial and ethnic groups.

EEOC is tasked by Congress to enforce laws prohibiting employment discrimination, including Title VII of the Civil Rights Act. *Adarand* does not affect an agency's responsibilities under MD-715. Neither EEOC policy nor MD-715 requires agencies to establish racial or ethnic preferences or quotas. Indeed, federal anti-discrimination laws and EEOC's policies require that agencies prohibit discrimination, including "reverse" discrimination. MD-715 requires agencies to take proactive steps to ensure equal employment opportunity for all their employees and applicants for employment by regularly evaluating their employment practices to identify and eliminate barriers that hamper the advancement of any racial or ethnic group in federal agencies.

In July 1995, the Department of Justice issued a memorandum entitled "Post-*Adarand* Guidance on Affirmative Action in Federal Employment" ("DoJ Memorandum"). The DoJ Memorandum provides guidance to all federal agencies on how to interpret *Adarand* in the context of federal employment and agencies seeking guidance in this area should review the DoJ Memorandum. It should be noted that the DoJ Memorandum re-emphasizes the federal commitment to affirmative employment in the federal government.

11. But MD-715 requires agencies to collect and analyze data which show the representation of groups by ethnicity and race (as well as by sex and disability status) in numerous profiles, such as grade distribution, major occupations, promotions, career development, etc. Thus, agencies must identify personnel by their membership in protected groups. Aren't such classifications unlawful?

No, an agency's collection and analysis of data by protected group is not unlawful. Neither *Adarand* nor any other controlling authority prohibits such collection and analysis. As is specifically noted in the DoJ Memorandum, "*Adarand* … does not preclude tracking participation [by protected class] in the agency's workforce through the collection and maintenance of statistics or the filing of reports with the Equal Employment Opportunity Commission." DoJ Memorandum, p. 4. The purpose of the data collection is to allow the evaluation of policies,

practices or procedures which may be impacting the employment opportunities of any protected group. Of course, agencies must ensure that the data collected are used appropriately for the purpose of developing and monitoring affirmative employment programs.

12. Are federal agencies prohibited from adopting goals based on race or ethnicity?

If a federal agency desires to develop numerical objectives or goals, the agency's General Counsel should carefully review the DoJ Memorandum before establishing any goals.

13. Are federal agencies prohibited from adopting preferences based on race or ethnicity?

Before a federal agency uses ethnicity or race as a basis for an employment decision, the agency must satisfy strict scrutiny to ensure that the decision promotes "compelling" government interests and that it is "narrowly tailored" to serve those interests. Again, the agency's General Counsel should carefully review the DoJ Memorandum before establishing any preferences.

TABLE QUESTIONS

14. Why did the EEOC revise the categories under which the agencies are to report the race and ethnicity of employees and applicants?

The Instructions call for federal agencies to report statistical information on the racial and ethnic categories of employees and applicants as prescribed by the Office of Management and Budget (OMB) in Statistical Policy Directive No. 15, Race and Ethnic Standards for Federal Statistics and Administrative Reporting (OMB Directive 15), which all federal agencies were required to adopt no later than January 1, 2003. OMB Directive 15 is available at: http://www.whitehouse.gov/omb/fedreg/ombdir15.html.

Under OMB Directive 15:

"The minimum categories for data on race and ethnicity for Federal statistics, program administrative reporting, and civil rights compliance reporting are defined as follows:

- **American Indian or Alaska Native.** A person having origins in any of the original peoples of North and South America (including Central America), and who maintains tribal affiliation or community attachment.
- **Asian.** A person having origins in any of the original peoples of the Far East, Southeast Asia, or the Indian subcontinent including, for example, Cambodia, China, India, Japan, Korea, Malaysia, Pakistan, the Philippine Islands, Thailand, and Vietnam.
- **Black or African American.** A person having origins in any of the black racial groups of Africa. Terms such as "Haitian" or "Negro" can be used in addition to "Black or African American."
- **Hispanic or Latino.** A person of Cuban, Mexican, Puerto Rican, Cuban, South or Central American, or other Spanish culture or origin, regardless of race. The term, "Spanish origin," can be used in addition to "Hispanic or Latino."
- **Native Hawaiian or Other Pacific Islander.** A person having origins in any of the original peoples of Hawaii, Guam, Samoa, or other Pacific Islands.
- **White.** A person having origins in any of the original peoples of Europe, the Middle East, or North Africa.

Respondents shall be offered the option of selecting one or more racial designations. Recommended forms for the instruction accompanying the multiple response question are 'Mark one or more' and 'Select one or more.'" (Emphasis added.)

15. Why doesn't the EEOC require agencies to report on the race of Hispanic employees and applicants?

Agency's reports to the EEOC use the minimum categories prescribed by OMB Directive 15 because we have determined that these categories provide the most useful statistics for federal oversight purposes. Also, inasmuch as the prior Management Directive 714 also did not require agencies to report the race of Hispanic employees or applicants, the use of the minimum categories allows for comparison of historical data.

However, nothing in MD-715 or the Instructions prohibit federal agencies from capturing more detailed racial and ethnic information, including the race of its Hispanic employees and applicants or the specific races selected by employees and applicants who select more than one race. Indeed, agencies are encouraged to capture such information to ensure that their data base is as comprehensive as possible. However, for reporting purposes, such detailed data must be aggregated into the minimum categories provided for in the Workforce Data Tables.

In addition, please note that when capturing racial and ethnic data, agencies should use a form that allows employees or applicants to select more than one race. Agencies should not use a form that has a box labeled "two or more races."

16. Why does the EEOC only require agencies to re-survey their Asian employees and those who have not been previously identified? Shouldn't all employees be afforded the opportunity to self-identify under the categories prescribed by OMB Directive 15?

In order to ensure that agencies would be able to timely submit their initial MD-715 report by January 31, 2005, the EEOC limited the requirement to re-survey existing employees to those who are identified as Asian because these employees must be placed accurately into either the category of "Asian" or "Native Hawaiian or Other Pacific Islander." Similarly, those employees who have not been previously identified need to be surveyed as reporting such employees as "Other" or "Non-category" does not comport with OMB Directive 15 or EEOC regulations. *See also* 29 C.F.R. § 1614.601(b).

The EEOC nonetheless encourages agencies to resurvey their employees for accurate race and national origin identification under OMB Directive 15. In addition, some agencies have concerns about the accuracy of their existing data and in such cases, re-surveying the workforce under the current categories would be a good idea. Finally, agencies are always strongly encouraged to periodically resurvey their employees to accurately capture current disability status.

17. My agency has not finished re-surveying its workforce nor has my agency begun tracking applicants. Should we still file the MD-715 report?

Yes. You should annotate your agency's Workforce Data Tables to indicate any data deviations or other assumptions made in the course of completing the Tables. You should also file as many PART Hs (EEO Plan To Attain the Essential Elements of a Model EEO Program) as may be necessary to address these deficiencies in your agency's EEO program. The Office of Personnel Management has revised Standard Form 181 to reflect OMB Directive 15. See http://www.opm.gov/forms/html/sf.asp .

18. My agency does not appear to be reaching persons who identify themselves as two or more races. How does an agency target persons who are of two or more races?

Broad targeting of recruitment efforts to a wide range of diverse sources of applicants generally should be sufficient to reach all races including those who select more than one racial identification.

19. When re-surveying, does an agency's EEO Office or its Human Resources Office have the responsibility to request the data and conduct the survey?

The EEOC has emphasized that coordination and cooperation between an agency's EEO Office and its Human Resources Office is necessary for MD-715 to be a success. Indeed, the cooperation of all offices (General Counsel, Information Technology, Budget and Finance, etc.,) is critical if an agency is to successfully remove workplace barriers or attempt to develop and maintain a Model EEO Program. Cooperation and coordination is a

must. Thus, it would be beneficial for both offices to work together to accomplish the re-survey.

20. How do I determine the appropriate Civilian Labor Force (CLF) Data to use on the various Workforce Data Tables? Where do I find the CLF data?

The CLF data is available at: http://www.census.gov/eeo2000. The national CLF, as shown, should be used on Tables A1 and A2; however, no CLF data should be shown for occupational groups on Table A3.

For Tables A6 through A8, the appropriate or relevant CLF availability data generally depends on the employer's area of recruitment. If a job is recruited nationally, then it may be appropriate to use the national CLF for that occupation, particularly if individuals apply form all parts of the country and the location from which they apply is not a factor in the hiring decision.

On the other hand, if an agency's announcement is limited to a particular geographic area (e.g. region, state, county or city) or, although the agency advertised nationally for a low-graded position, the only applications received are from the city or county in which the position is located, then it may be more appropriate to consider the local area CLF.

An agency must have a justification for whichever CLF data it uses for comparison purposes in the Workforce Data Tables filed under MD-715. If the agency has questions about what CLF data to use, it should contact EEOC's Affirmative Employment Division at (202) 663-4555.

21. How are foreign nationals reported?

Foreign nationals are not reported in the Workforce Data Tables, whether or not the foreign national works overseas or in the United States. See Instructions, Section III, page 1, column 2. "All non-intermittent or non-seasonal employees except foreign nationals, will be reported". Employees who are U.S. citizens are included in the Workforce Data Tables, whether they are employed within the United States (including Puerto Rico) or abroad.

22. What is the "Federal High" used on Table B1?

This is the participation rate of the agency (with 500 or more permanent employees) which had the greatest participation rate of employees with targeted disabilities during the prior fiscal year. For 2005, that agency was the Equal Employment Opportunity Commission, where 2.16% of employees had a targeted disability.

23. I am aware that my agency has employees with targeted disabilities who have not self-identified. May I visually identify these employees for purposes of reporting them in the agency's MD-715 Report?

No. The collection of data on disability status is governed by 29 C.F.R. § 1614.601(f). This regulation provides that data on disability status is collected by voluntary self-identification. Agencies are to explain the importance of the data to employees and actively encourage them to self-identify. Only if the employee is a Schedule A appointee and refuses to self-identify, may the agency identify the employee's disability using the records supporting the appointment. For all other employees, if the employee still refuses to self-identify even with encouragement, the agency should report the employee's disability status as "unknown." Note that the fact that such a non-Schedule A, non-self-identifying employee may have requested an accommodation and provided records supporting the request which establish a disability is irrelevant; the records used for purposes of the accommodation request cannot be used by the agency to unilaterally identify the employee. Thus, visual identification may not be used for the collection of disability data.

24. Tables A1 and B1 ask agencies to report on employees who are paid with non-appropriated funds, in addition to reporting on permanent and temporary employees. Can you please explain this category?

Under previous management directives, agency affirmative employment reports to the Commission only contained workforce data statistics that were otherwise contained in OPM's Central Personnel Data File (CPDF).

The CPDF excludes large portions of non-appropriated fund employees, meaning these employees often went unreported. Thus, an accurate snapshot of the agency workforce was never seen and reviewed. Agency resources, planned activities, etc., were also not evaluated with an accurate picture of the workforce in mind. MD-715 requires that all employees be reported. Therefore, by including a category where non-appropriated fund employees can be reported, this gap between what's in the CPDF and an agency's actual workforce total can be bridged. Hence, the data to be included in this category should include individuals excluded from the CPDF and otherwise not traditionally reported in affirmative employment reports.

25. In Tables A3 and B3, why is the EEOC using 9 occupational categories instead of the PATCOB categories used in the past? It is burdensome to have to use the 9 occupational categories for reports to the EEOC and PATCOB for reports to the Office of Personnel Management (OPM).

Since the 1960s, private employees have reported information to the EEOC on one of the more well-known reports collected by the Commission, the EEO-1 report. The EEO-1 report provides a breakout of the employer's workforce by gender and race/ethnicity in nine job categories. The EEOC's experience in analyzing EEO-1 reports for many years has led us to determine that use of similar occupational categories in the federal sector will provide more useful information. Moreover, use of similar occupational categories will allow comparisons between the federal and private sectors. In particular, use of the Officials and Managers category, further divided into hierarchical subcategories, allows for the collection of data about racial and gender stratification that can help to identify the existence of a "glass ceiling." We view this as a positive development in our mission to eradicate discrimination from the federal workplace and move toward the ultimate goal of making the federal government a model employer.

Although OPM may decide to continue its historical use of PATCOB, OPM's data needs differ significantly from the EEOC's data needs in its role as the enforcer of the civil rights laws governing employment. The EEOC determined that the PATCOB categories are outdated, overly broad and too imprecise to allow the level of analysis desired. To the extent that certain agencies may object to grouping their data into the nine occupational categories as burdensome, the EEOC notes that other agencies have represented that their information technology departments have not found this to be a difficult task. Nevertheless, EEOC staff have met with OPM staff and discussed the nine categories used under MD-715 as OPM proceeds in the development of the new Enterprise Human Resources Integration (EHRI) system. We also conveyed to OPM the need for the system to be equally compatible with PATCOB and the nine occupational categories used for reporting under MD-715. We expect to continue to meet with OPM staff to further coordinate our mutual needs.

26. Isn't this just obtaining information for the sake of having information? If the PATCOB is good enough for OPM, why isn't it good enough for EEOC?

As previously noted, EEOC's data needs differ substantially from those of OPM. While OPM's role is human resource management, EEOC is the enforcer of civil rights laws governing employment. We have concluded that the PATCOB categories are both outdated and too imprecise to provide the level of analysis needed in our mission to identify and eliminate impediments to equal opportunity. Moreover, PATCOB data does not give any information on the composition of an agency's managers or otherwise allow for the identification of 'glass ceilings.'

The information obtained in the MD-715 reports is vital to our - that is, the Commission's and the agencies' - understanding of the Federal workforce.

Many new Federal employees are drawn from the private sector. Clearly, the ability to cross-reference and analyze both Federal and private data moves all of us toward achieving our goal of making the Federal government a model employer. Organizations that want to recruit and retain an inclusive workforce - one that reflects the American public - must use all available sources of candidates in these increasingly competitive times. Any agency that fails to benchmark itself against the full spectrum of the labor market will not achieve the

mission and business of the agency. As more Federal employees become eligible for retirement, succession planning provides an opportunity to engage in a deliberate and systematic effort to ensure that critical skills positions attract and hire persons from all groups. A system of measurement which allows for comparison to the private workforce allows agencies to more successfully monitor the effectiveness of their efforts.

27. How do I know in which of the 9 occupational groups an employee should be placed?

The EEOC's website contains a link to the OPM/Census Occupation Cross-Classification Table (Crosswalk). This Crosswalk is intended as general guidance in cross-classifying OPM occupation codes to the nine occupational categories. Agencies are encouraged to contact EEOC with specific questions about what category might be appropriate for their particular occupations.

The link to the Crosswalk is: http://www.eeoc.gov/federal/715instruct/00-09opmcode.html

Please remember that when an employee is classified as a supervisor or manager, that employee should be placed in the ***Officials and Managers*** category rather than in the category in the crosswalk that they would otherwise be placed in based on their OPM occupation codes. Those employees classified as supervisors or managers who are at the GS-12 level or below should be placed in the First-Level subcategory of ***Officials and Managers***, those at the GS-13 or 14 should be in the **Mid-Level** subcategory, and those at the GS-15 or in the SES should be placed in the **Executive/Senior-Level** subcategory. An agency may also choose to place employees who have significant policy-making responsibilities, but do not supervise other employees, in these three subcategories.

The fourth subcategory, called "**Other**," contains employees in a number of different occupations that are primarily business, financial and administrative in nature, and do not have supervisory or significant policy responsibility. For example, Administrative Officers (OPM Code 0341) are appropriately placed in the "**Other**" subcategory.

28. May I utilize the codes used in the Federal Personnel Payroll System (FPPS) to identify my agency's supervisors or managers? These are the codes I would like to use: 02 - Supervisor or Manager, 04 - Supervisor, 05 - Management Official, 06 - Leader, and 07 - Team Leader.

You may use whatever method you deem appropriate to properly account for and categorize employees reflected in the Workforce Data Tables. The EEOC has no objection to an agency's use of FPPS codes or other agency-specific codes to assist in identifying the supervisors and managers who should be placed in one of the first three subcategories of the Officials and Managers category. However, please note that the EEOC does not consider Team Leaders to be supervisors or managers within the definition of the occupational group "Officials and Managers." Therefore, FPPS codes 06 and 07 may not be used to identify supervisors and managers.

29. What about Wage Grade employees who are supervisors or managers?

Wage Grade employees who are supervisors or managers should be included in the Officials and Managers category. An agency will have to determine which of the first three subcategories is the appropriate one for placement of the employee. Should an agency have specific questions in this area, they are welcome to consult with the EEOC.

30. I have employees in series that are not in the Crosswalk. Where do I place these employees?

When questions are raised about a series not being included on the Crosswalk, it generally has been because the series no longer exists. For example, some agencies' data systems still show employees in the former GS-334 series, which is now the GS-2210, Information Technology Management Series. Similarly, the former GS-204, 205, 221, 233, and 235 series were all placed into the GS-201, Human Resource Management Series and the former GS-345 series is now part of the GS-301 series. Note that these changes include series both in the General Schedule and the Wage Grade areas. Also, another wrong or missing code example could

occasionally be a violation of the "single agency code" rule. Specifically, when a GS code and title exists and is authorized only for one designated agency, sometimes others decide unilaterally to use it.

When these discrepancies are discovered, we suggest that Human Resources and EEO Offices coordinate on that matter, as the Human Resources office may need to reclassify the affected employees, using relevant OPM Position Classification Standards (PCS) that specify the "new" series relative to the "discontinued" series.

31. Why does the Commission ask for data on the Occupational Categories (Tables A3-1, A3-2, B3-1 and B3-2), Participation Rates in General Schedule Grades (Tables A4-1, A4-2, B4-1 and B4-2) and Participation Rates in Wage Grades (Tables A5-1, A5-2, B5-1 and B5-2) to be displayed in two ways?

These Tables display the data by either showing (1) participation rates, i.e. the percentage of a particular group participating in an occupational category or a grade or (2) distribution rates, i.e. the distribution of a particular group throughout all of the occupational categories or grades.

In order to show the percentage of a particular group participating in an occupational category or a grade, in Tables A/B 3-1, 4-1, and 5-1, the data is computed across the rows, with the sum of the row equaling 100%. Thus, these Tables show what percentage of all employees in that occupational category or grade is represented by a particular group.

For example, an agency's Table A4-1 reflects that the agency has 788 GS-13 employees, of which 18, or 2.3%, are Hispanic females. The Table also shows that the agency has 361 GS-14 employees, of which 3, or 0.8%, are Hispanic females.

The participation rate of a particular group in an occupational category or grade should be compared to that group's participation rate in the agency's total workforce. If the group's participation rate is not comparable to its participation rate in the total workforce, an agency should explore whether members of the group are encountering obstacles to full participation in an occupational category or grade.

In Tables A/B 3-2, 4-2 and 5-2, the data is computed **down** the columns, with the sum of the column equaling 100%. Thus, these Tables show the distribution of a particular group among the occupational categories or grades.

For the agency in the above example, its Table A4-2 reflects that the agency has 90 Hispanic female employees, of which 18, or 20% of all Hispanic female employees, are at the GS-13 level. The Table also shows that 3 of the Hispanic female employees, or 3.3% of all Hispanic female employees, are at the GS-14 level.

The distribution rate of a particular group should be compared to that group's participation rate in the agency's total workforce. If the group's distribution rate is not comparable to its participation rate in the total workforce, an agency should explore to what extent members of the group are clustered in a particular occupational category or grade and whether members of the group are encountering obstacles to participation in other occupational categories or in advancing to higher grades.

Thus, in the examples given above, the two Tables together suggest that the agency should explore whether there is any barrier or "glass ceiling" facing Hispanic females. In investigating the "triggers" reflected in these Tables, the agency will want to consider the data on Hispanic females presented in the remainder of the Tables. For example, the agency should explore the representation rates for Hispanic females employed in the agency's major occupations (Tables A4-1 and A4-2), data on the agency's new hires of Hispanic females (Table A8), data on the agency's selections for internal competitive promotions for major occupations (Table A9), the participation rate of Hispanic females in career development programs (Table A12), the participation rate of Hispanic females in awards (Table A13) and data on the separation rates for Hispanic females (Table A14). The agency may wish to gather more refined data; e.g. the agency may wish to explore whether Hispanic females at the GS-13 level are separating from the agency at rates higher than would be expected and/or gather data on the performance ratings of Hispanic females at the GS-13 level.

32. My agency has pay bands. May I modify the Workforce Data Tables, particularly Tables A/B 4 and 5, to reflect pay bands instead of GS grades?

In its MD-715 report, an agency may not provide the data required by Tables A/B 4 and 5 solely by modifying the Tables to use pay bands. Glass ceilings can occur within a pay band, and this method does not allow the agency to identify the specific pay level where a group may be experiencing barriers. In addition, government-wide data is reported by use of the GS grades, which remain the most common pay schedule. Agencies must use payroll data to break down these employees into the equivalent GS-grades for purposes of completing Tables A/B 4 and 5. We suggest that the agency's EEO office, in conjunction with its Human Resource office, determine the precise metrics for breaking down of the payroll data to ensure consistency throughout the agency. An agency may, of course, elect to perform additional analyses using pay band data.

33. My agency has several different Wage Grade structures governing different employees and the actual pay for each grade level differs significantly from structure to structure. How do I fill out a single Workforce Data Table 5, as it will be difficult to reconcile the data from all the structures into one overall comparative Table?

An agency may fill out more than one Workforce Data Table in this instance or similar instances where the result is the provision of more precise and useful information. The agency should indicate the basis for providing the additional tables.

34. Workforce Data Tables A13 and B13 (Employee Recognition and Awards) require agencies to report on "Cash Awards - $100-$500" and Cash Awards - $501+." A large percentage of my agency's workforce received well over $500 in awards, with a substantial number receiving awards between $3,000 and $5,000, and others received over $5,000. May I modify these Workforce Data Tables to include additional levels of awards?

Yes. This is another instance where the result is the provision of more precise and useful information.

35. Whom should I contact for further information?

For further information or questions on MD-715, please contact Lori Grant on (202) 663-4616 (voice) or (202) 663-4593 (TTY).

United States Equal Employment Opportunity Commission

OFFICE OF FEDERAL OPERATIONS

Annual Report on the Federal Work Force Part I
EEO Complaints Processing

Fiscal Year 2012

Table of Contents

PREFACE

The United States Equal Employment Opportunity Commission (EEOC or Commission) was established by *Title VII of* the *Civil Rights Act of 1964*, (*Title VII*), *as amended*, with the original mission of eradicating discrimination in employment on the bases of race, color, religion, sex, and national origin. Since 1964, EEOC's role has expanded beyond Title VII. In the federal sector, the agency currently has responsibilities under the following nondiscrimination laws as well:

- the *Equal Pay Act of 1963 (EPA)*, *as amended*, which prohibits employment discrimination on the basis of gender in compensation for substantially similar work performed under similar conditions;
- the *Age Discrimination in Employment Act of 1967 (ADEA)*, *as amended*, which prohibits employment discrimination on the basis of age (40 years of age and older);
- the *Rehabilitation Act of 1973 (Rehabilitation Act)*, *as amended*, which prohibits employment discrimination against federal employees and applicants with disabilities, and requires that reasonable accommodations be provided; and
- the *Genetic Information Nondiscrimination Act of 2008 (GINA)*, which prohibits employment discrimination on the basis of genetic information.

EEOC's Office of Federal Operations (OFO) adjudicates discrimination complaint appeals in the federal sector and monitors federal agency compliance with equal employment opportunity (EEO) laws and procedures. OFO also reviews and assesses the effect of federal agencies' compliance with requirements to maintain continuing affirmative employment programs to promote equal employment opportunity, and to identify and eliminate barriers to equality of employment opportunity.

Equal Employment Opportunity Management Directive 715 (MD-715), issued in October 1, 2003, established standards for ensuring that agencies develop and maintain model EEO programs. These standards are used to measure and report on the status of the federal government's efforts to become a model employer. As detailed in *MD-715,* the six elements of a model EEO program are:

- Demonstrated commitment from agency leadership,
- Integration of EEO into the agency's strategic mission,
- Management and program accountability,
- Proactive prevention of unlawful discrimination,
- Efficiency, and
- Responsiveness and legal compliance.

Part I of the report covers the period from October 1, 2011, through September 30, 2012 and contains selected measures of agencies' progress toward achieving the following elements of

model EEO programs: the integration of EEO into the agency's strategic mission, efficiency, and responsiveness and legal compliance elements of model EEO programs.[1]

Part II of the report, will be published at a later date, and will contain selected measures of progress made by agencies in FY 2011 and 2012 toward the demonstrated commitment from agency leadership, integration of EEO into the agency's strategic mission, management and program accountability, proactive prevention of unlawful discrimination, and responsiveness and legal compliance elements of model EEO programs.[2] Working within our mission to provide oversight and guidance, EEOC strives to create partnerships within the federal community.

The fiscal year (FY) 2012 *Annual Report on the Federal Work Force Part I*, submitted to the President and Congress, presents a summary of selected EEO program activities of 71 federal agencies. The report provides valuable information to all agencies as they strive to become model employers.

In preparing this report, EEOC relied on the following: 1) EEO complaint processing data submitted and certified as accurate by 357 federal agencies and subcomponents in their FY 2012 Federal Equal Employment Opportunity Statistical Report of Discrimination Complaints (EEO Form 462 reports) - note the Election Assistance Commission (EAC) and the Federal Retirement Thrift Investment Board (FRTIB) did not file a FY 2012 EEO Form 462 report; and 2) hearings and appeals data obtained from EEOC's internal databases.[3]

The Commission would like to extend its thanks to those agencies that timely submitted accurate and verifiable EEO complaint processing data. Agencies are encouraged to submit all reports to the Commission in a timely and accurate manner to ensure that the state of EEO in the federal work force is reflected correctly.

As in the past, agencies were provided an opportunity to review the draft of this report. The Commission thanks those agencies that responded with useful comments and suggestions.

---

[1] All measures under EEOC's regulations and management directives are equally important, and the inclusion of particular measures in this Report does not indicate a higher degree of importance.

[2] *Id.*

[3] Certain agencies do not provide total work force numbers for national security reasons.

EXECUTIVE SUMMARY

STATE OF EEO COMPLAINT PROCESSING IN THE FEDERAL GOVERNMENT

- ❑ In FY 2012, 71% of agencies (with 100 or more employees) required to file a FY 2012 Form 462 reported compliance with MD-715's requirement that the EEO Director reports directly to the Head of the agency.

- ❑ 96% of agencies (with 100 or more employees) required to file a FY 2012 Form 462 reported they provided some of their EEO staff with the required training in FY 2012.

- ❑ Pre-complaint EEO counseling and alternative dispute resolution (ADR) programs addressed many employee concerns before they resulted in formal EEO complaints. Of the 34,521 instances of counseling in FY 2012, 54.2% did not result in a formal complaint, due either to settlement by the parties or withdrawal from the EEO process.

- ❑ In FY 2012, 15,026 individuals filed 15,837 complaints alleging employment discrimination against the federal government.

- ❑ The number of complaints filed decreased by 6.7% over the previous year and there was a 4.9% decrease in the number of individuals who filed complaints over the same period. In FY 2012, 5.1% of the complaints were filed by individuals who had filed at least one other complaint during the year, down from the 6.9% in FY 2011.

- ❑ Government-wide, a total of 10,226 investigations were completed in an average of 187 days in FY 2012. There were 74.9%, of the investigations (7,660) timely completed, up slightly from FY 2011's 74.7% timely completion rate. Without the United States Postal Service's (USPS) investigations, the government-wide average was 66.4%, which is an increase from the 65.3% timely completion rate in FY 2011.

- ❑ Agencies issued 4,118 merit decisions without a decision by an EEOC Administrative Judge, and 48.6% were timely issued (2,003), down from 56.5% timely issued in FY 2011. Without the USPS' merit decisions, the government-wide average dropped to 31.1%.

- ❑ EEOC's hearing receipts decreased from 8,113 in FY 2011 to 7,728 in FY 2012, down by 4.7%. The average processing time for a hearing was 370 days, a 7.2% increase from FY 2011's average of 345 days.

- ❑ EEOC's appeal receipts decreased from 5,176 in FY 2011 to 4,350 in FY 2012, down by 15.9%. The average processing time for appeals in FY 2012 was 361 days, a 4.5% decrease from the 378 days in FY 2011.

- ❏ As a result of final agency decisions, settlement agreements, and final agency actions fully implementing EEOC Administrative Judges' decisions, agencies paid monetary benefits to EEO complainants totaling $51.4 million in FY 2012, up 18.2% from the $43.5 million paid in FY 2011. An additional $10.8 million was paid out in response to appellate decisions, a 17.4% increase from the $9.2 million paid out in FY 2011.

- ❏ In FY 2012, EEOC's training and outreach program reached 2,440 federal employees through 95 sessions.

- ❏ In FY 2012, EEOC Form 462 reports were timely filed by 92% of the agencies (with 100 or more employees) that were required to submit an EEOC Form 462 report (90 of 98).

I. SUMMARY OF EEO STATISTICS IN THE FEDERAL GOVERNMENT

Section A - Integration of EEO Into Agencies' Strategic Mission

In order to achieve its strategic mission, an agency must integrate equality of opportunity into attracting, hiring, developing, and retaining the most qualified work force. The success of an agency's EEO program ultimately depends upon decisions made by individual agency managers. Therefore, agency managers constitute an integral part of the agency's EEO program. The EEO office serves as a resource to these managers by providing direction, guidance, and monitoring of key activities to achieve a diverse workplace free of barriers to equal opportunity.

As part of integrating EEO into the strategic mission, Section II(B) of MD-715 instructs agencies to ensure that: (1) the EEO Director has access to the agency head; (2) the EEO office coordinates with Human Resources; (3) sufficient resources are allocated to the EEO program; (4) the EEO office retains a competent staff; (5) all managers receive management training; (6) all managers and employees are involved in implementing the EEO program; and (7) all employees are informed of the EEO program. Two aspects of this Section are highlighted below.

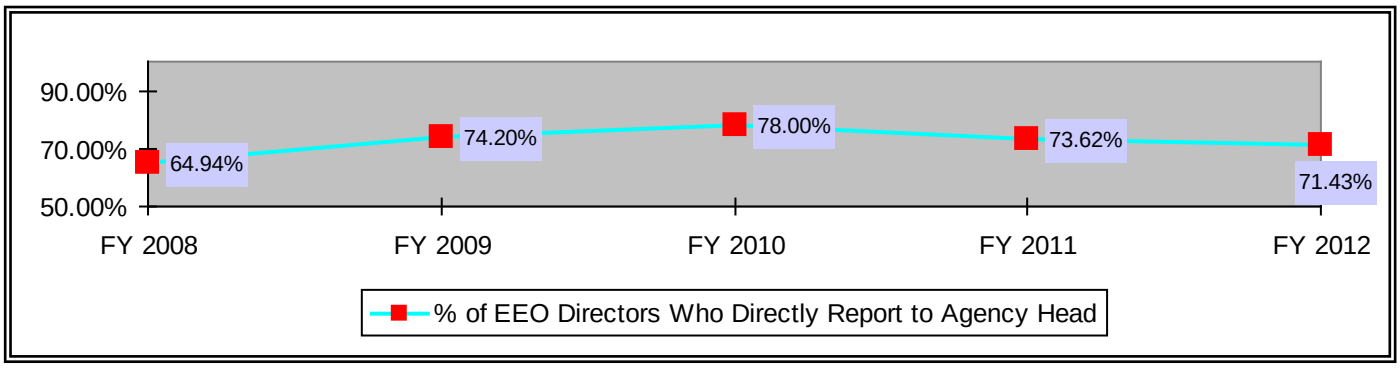
1. 71% of Agency EEO Directors Report to Agency Head

EEOC's regulations governing agency programs to promote equal employment opportunity require each agency to "maintain a continuing affirmative program to promote equal opportunity and to identify and eliminate discriminatory practices and policies." 29 C.F.R. §1614.102(a). To implement its program, each agency must designate a Director of Equal Employment Opportunity who shall be under the immediate supervision of the agency head. 29 C.F.R. §1614.102(b)(4).

When the EEO Director is under the authority of others within the agency, the agency creates a potential conflict of interest where the person to whom the EEO Director reports is involved in or would be affected by the actions of the EEO Director. By placing the EEO Director in a direct reporting relationship to the agency head, the agency underscores the importance of EEO to the agency's mission and ensures that the EEO Director is able to act with the greatest degree of independence.

Of the 98 agencies with 100 or more employees that were required to submit an EEOC Form 462 report in FY 2012, 71.4% (70) indicated that their EEO Director reports to the agency head, down from the 73.6% reported in FY 2011 and up from the 64.9% reported in FY 2008. Figure 1 below shows a five-year trend. See Appendix III for a detailed list of agencies' status.

Figure 1 - Percentage of EEO Directors Who Report Directly to the Agency Head FY 2008 - FY 2012



2. 96% of Agencies Provided Some of Their EEO Staff with Required Training

Section II(B) of MD-715 requires that agencies attract, develop and retain EEO staff with the strategic competencies necessary to accomplish the agency's EEO mission. In order to ensure staff competency within its EEO complaint program, agencies must comply with the mandatory training requirements for EEO counselors and investigators as set forth in Management Directive 110 for 29 C.F.R. Part 1614, as revised November 9, 1999 (MD-110). Agencies using contract staff to perform these functions must also ensure that these requirements are met.

Chapter 2, Section II of MD-110, requires that new EEO counselors receive thirty-two hours of EEO counselor training and thereafter eight hours of training each year. Likewise, new EEO investigators are required to have thirty-two hours of EEO investigator training and thereafter eight hours of training each year as set forth in Chapter 6, Section II of MD-110.

Of the 98 agencies with 100 or more employees that were required to file an EEOC Form 462 report in FY 2012, 96% ensured that some of their EEO staff received the required regulatory training, less than the 97.8% that reported in FY 2011. See Appendix III for a detailed list of agencies' status. Agencies ensured or provided training for 1,324 new EEO counselors and 433 new EEO investigators. Agencies also ensured or provided the required eight hour annual refresher training to 3,185 EEO counselors and 1,732 EEO investigators. Additionally, agencies reported ensuring or

providing 88 EEO counselor/investigators with thirty-two hour training and 327 with eight hour training.

Section B - Efficiency in the Federal EEO Process

EEOC's regulations provide that each agency shall ensure that individual complaints are fairly and thoroughly investigated and that final action is taken in a timely manner. 29 C.F.R. §1614.102(c)(5). Section II(E) of MD-715 establishes that a model EEO program must have an efficient and fair dispute resolution process and effective systems for evaluating the impact and effectiveness of its EEO programs. In this regard, Section II(E) recommends that agencies "benchmark against EEOC regulations at 29 C.F.R. Part 1614 and other federal agencies of similar size which are ranked in EEOC's Annual Report on the federal sector complaints process."

1. Federal A gency EEO Programs: Complaints Decrease and Processing Times Continue to Exceed Regulatory Deadlines

Agencies process EEO complaints from applicants' for federal employment and federal employees under EEOC's regulations at 29 C.F.R. Part 1614. Individuals unable to resolve their concerns through counseling can file a complaint with their agency.[4] The agency will either dismiss[5] or accept the complaint. If the complaint is accepted, the agency must conduct an investigation and, in most instances, issue the investigative report within 180 days from the date the complaint was filed.[6]

After the employee receives the investigative report, s/he may: (1) request a hearing before an EEOC Administrative Judge, who issues a decision that the employee or the agency may appeal to the OFO; or (2) forgo a hearing and request a final agency decision. An employee who is dissatisfied with a final agency decision or the agency's decision to dismiss the complaint may appeal to OFO. The complainant or agency may also request reconsideration of a decision on the appeal. At various points in the process, the complainant has the right to file a civil action in a federal court.

---

[4] Matters involving both claims of discrimination and agency actions appealable to the U. S. Merit Systems Protection Board follow one of the processes set forth at 29 C.F.R. §1614.302.

[5] There are several reasons an agency may dismiss a complaint, including the complainant's failure to state a claim, untimely contact with an EEO counselor, or that alleges a preliminary step to taking a personnel action is discriminatory. *See* 29 C.F.R. §1614.107(a).

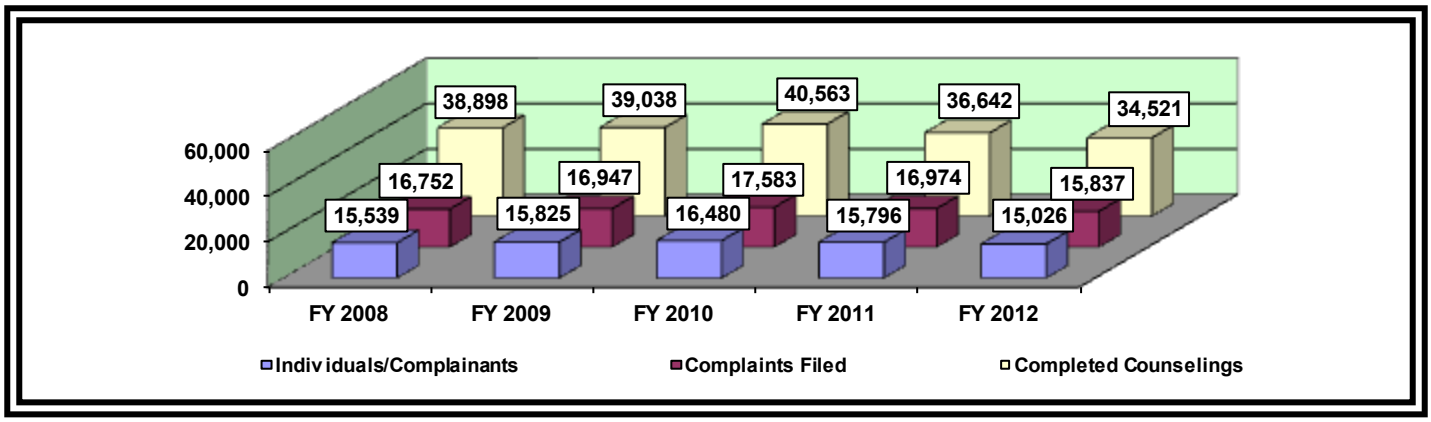
[6] The 180-day period may be extended by 90 days if both parties agree. *See* 29 C.F.R. §1614.108(e). The regulations also extend the 180-day time limit for consolidated and amended complaints to the earlier of 180 days from the date of the most recent consolidated or amended complaint, or 360 days from the date of the earliest pending complaint. *See* 29 C.F.R. § 1614.108(f).

As the EEO complaint process has become increasingly more adversarial, and lengthy, EEOC has encouraged agencies to promote and expand the use of alternative dispute resolution (ADR) as a means of avoiding the formal adjudicatory processes. Used properly, ADR can provide fast and cost-effective results while improving workplace communication and morale.[7]

a. Pre-Complaint Counselings and Complaints Decrease

From FY 2011 to FY 2012, the number of completed counselings decreased by 5.8% and by almost 11.3% since FY 2008. Formal complaints decreased by 6.7% from FY 2011 to FY 2012 and by 5.5% since FY 2008. Among the 34,521 completed counselings, 15,026 individuals filed 15,837 formal complaints in FY 2012.[8] The number of formal complaints filed represents 45.9% of all pre-complaint counseling activities in FY 2012. As Figure 2 shows, over the past five fiscal years, the number of pre-complaint counseling activities decreased from 38,898 in FY 2008 to 34,521 in FY 2012; and the number of complaints filed by individuals has declined over the past two-year period. During the same five-year period, the number of formal complaints filed continued to represent less than 50% of all pre-complaint counseling activities. See Figure 2. Significantly, while the United States Postal Service constituted 21.3% of the work force[9], it accounted for 38.1% of all EEO counselings, 28.6% of all complaints filed, 26.0% of all completed investigations and 29.2% of all complaints closed in FY 2012. See Tables B-1, B-9 and B-10 in Appendix IV at http://www.eeoc.gov/.

Figure 2 – Completed Counseling to Formal Complaints Filed/Complainants FY 2008 - FY 2012



[7] *See* Marc Van Nuys, *Return on Investment From Use of Alternative Dispute Resolution in Workplace Disputes*, 1-14 (Army ADR Program).

[8] Counseling may be provided via EEO Counselor or ADR Intake Officer.

[9] Work force numbers as reported by the agency in its FY 2012 Form 462 report.

Table 1 below shows that among the cabinet/large (15,000 or more employees) agencies in FY 2012, the U.S. Postal Service again reported the highest percentage (1.9%) of its work force that completed counseling, while the government-wide average was 1.1%. Among the medium sized agencies (1,000 to 14,999 employees), Government Printing Office reported the highest percentage (2.8%) of its work force completed counseling. Agencies that had fewer than 25 completed/ended counselings were not included in the ranking. Small and Micro agencies (1-999 employees) typically have fewer than 25 completed/ended counselings and, therefore, are not ranked. Table B-1 in Appendix IV lists this information for all agencies and is located at http://www.eeoc.gov/.

Table 1 – Agencies with the Highest Counseling Rate in FY 2012

Agency	Total Work Force*	Percentage of Individuals Who Completed Counseling
Cabinet or Large (15,000 or more employees)		
U.S. Postal Service	625,701	1.9%
Department of Veterans Affairs	323,154	1.3%
Social Security Administration	65,474	1.3%
Medium Agencies (1,000 to 14,999 employees)		
Government Printing Office	1,879	2.8%
Broadcasting Board of Governors	1,675	2.7%
Defense JTF National Capital Region Medical	4,417	1.8%

* Work force numbers as reported by the agency in its FY 2012 462 report.

As shown in Table 2 below, in FY 2012, among the cabinet/large agencies (15,000 or more employees), the Department of Labor reported the highest complainant rate of 0.8%, while the government-wide average was 0.5%. Among the medium sized agencies (1,000 to 14,999 employees), the Government Printing Office again reported the highest complainant rate of 1.2%. Agencies that had fewer than 25 complaints filed were not included in the ranking. Table B-1 in Appendix IV contains this information for all agencies and is located at http://www.eeoc.gov/.

Table 2 - Agencies with the Highest Complainant Rate in FY 2012

Agency	Total Work Force*	Complainants as % of Total Work Force
Cabinet or Large (15,000 or more employees)		
Department of Labor	16,819	0.77%
Social Security Administration	65,474	0.69%
U.S. Postal Service	625,701	0.68%
Medium Agencies (1,000 to 14,999 employees)		
Government Printing Office	1,879	1.22%
Defense Commissary Agency	14,382	0.97%
Equal Employment Opportunity Commission	2,291	0.96%

* Work force numbers as reported by the agency in its FY 2012 462 report.

b. Pre-Complaint ADR Usage – Rates Rise in Two Major Categories

Beginning in FY 2006, ADR offer and participation rates were measured in completed/ended counselings at the end of the fiscal year to ensure greater uniformity, consistency, and quality in the reporting and utilization of ADR data. Therefore, comparison of FY 2006 through FY 2012 data with prior years' data is not possible.

In FY 2012, the government-wide offer rate was 85.7% based upon 29,577 ADR offers made in 34,522 completed/ended counselings, up from the 78% reported in FY 2011. The participation rate was 51.1%, based upon the 17,643 counselings accepted into agencies' ADR programs of the total completed/ended counselings, exceeding the 48.6% reported in FY 2011.

Thirty-four agencies had 100% offer rates in FY 2012. The agencies were the American Battle Monuments Commission, Broadcasting Board of Governors, Chemical Safety and Hazard Investigation Board, Commodity Futures Trading Commission, Consumer Product Safety Commission, Defense Army and Air Force Exchange, Defense Information Systems Agency, Defense Joint Task Force National Capital Region Medical, Defense National Security, Defense Office of Inspector General, Defense Technical Information Center, Defense Threat Reduction Agency, Department of Housing and Urban Development, Department of Labor, Export-Import Bank of the US, Farm Credit Administration, Federal Election Commission, Federal Labor Relations Authority, Federal Maritime Commission, Federal Reserve System-Board of Governors, Federal Trade Commission, Government Printing Office, International Boundary and Water Commission, International Trade Commission, John F. Kennedy Center for the Performing Arts, Merit Systems Protection Board, National Credit Union Administration,

National Gallery of Art, National Indian Gaming Commission, Nuclear Regulatory Commission, Office of Government Ethics, Peace Corps, Pension Benefit Guaranty Corporation, and the Smithsonian Institution.

The U.S. Postal Service Again Had the Highest ADR Participation Rate

In FY 2012, the U.S. Postal Service again reported the highest ADR participation rate in the pre-complaint process (69.9%) among the cabinet/large agencies, while the government-wide average was 51.1%. Among the medium sized agencies, the Smithsonian Institution reported the highest pre-complaint ADR participation rate (86.8%). The government-wide average falls to 39.9% without the U.S. Postal Service. See Table 3. Agencies that had fewer than 25 completed/ended counseling were not included in the ranking. See Tables B-1 and B-4 in Appendix IV for information on all agencies, which is located at http://www.eeoc.gov/.

Table 3 - Highest ADR Participation Rate in the Pre-Complaint Process FY 2012

Agency	Total Work Force*	Completed/ Ended Counselings	Participation in ADR	Participation Rate
Cabinet or Large (15,000 or more employees)				
U.S. Postal Service	625,701	13,143	9,180	69.85%
Defense Logistics Agency	25,229	312	191	61.22%
Department of Veterans' Affairs	323,154	4,484	2,580	57.54%
Medium Agencies (1,000 to 14,999 employees)				
Smithsonian Institution	6,057	38	33	86.84%
Defense Finance and Accounting Service	11,982	92	55	59.78%
Defense Commissary Agency	14,382	227	122	53.74%

* Work force numbers as reported by the agency in its FY 2012 462 report.

c. Agencies Meet Counseling Deadlines in 92.9% of Cases

On average in FY 2012, agencies met timeliness requirements for EEO counseling in 92.9% of all completed/ended counselings, which was a slight increase from 92.8% in FY 2011 and from the 91.2% in FY 2008. Agencies are required to complete counseling in 30 days except when there is a 60-day extension due to an ADR election or the complainant agrees in writing to an extension.

d. Agencies Pre-Complaint Resolution Rate Up Slightly in FY 2012

During counseling and ADR in the pre-complaint stage, EEO disputes can be resolved by either a settlement or a decision not to file a formal complaint. In FY 2012, the government-wide resolution rate average was 53.4%, up slightly from 53.1% in FY 2011.

The National Archives and Records Administration Holds the Highest Pre-Complaint Resolution Rate

In FY 2012, the National Archives and Records Administration, a medium sized agency, reported the highest pre-complaint resolution rate (87.9%) among all agencies with more than 25 completed/ended counselings. Among cabinet/large agencies, Defense National Guard Bureau reported the highest pre-complaint resolution rate (71.7%). See Table 4. Agencies that had fewer than 25 completed/ended counselings were not included in the ranking. However, nine agencies, Defense Technical Information Center, Farm Credit Administration, Federal Election Commission, Federal Trade Commission, International Boundary and Water Commission, National Indian Gaming Commission, Office of Government Ethics, Overseas Private Investment Corporation and the Postal Regulatory Commission, in this category had 100% resolution rates. Table B-3 in Appendix IV contains this information for all agencies and is located at http://www.eeoc.gov/.

Table 4 – Highest Pre-Complaint Resolution Rates FY 2012

Agency	Total Work Force*	Completed Counselings	Total Resolved	Resolution Rate
Cabinet or Large (15,000 or more employees)				
Defense National Guard Bureau	57,511	113	81	71.7%
Defense Army and Air Force Exchange Service	34,273	336	230	68.5%
U.S. Postal Service	625,701	13,143	8,602	65.5%
Medium Agencies (1,000 to 14,999 employees)				
National Archives and Records Administration	3,381	33	29	87.9%
Federal Reserve System-Board of Governors	2,412	54	42	77.8%
Broadcasting Board of Governors	1,675	53	41	77.4%

* Work force numbers as reported by the agency in its FY 2012 462 report.

The Defense National Guard Bureau Had the Highest ADR Resolution Rate in FY 2012

In FY 2012, the Defense National Guard Bureau reported the highest ADR resolution rate in the pre-complaint process (91.5%) among those agencies with 25 or more ADR closures, whereas the government-wide average was 63%. Among the medium sized agencies, the Defense Finance and Accounting Service reported the highest pre-complaint ADR resolution rate (65.5%). See Table 5. The government-wide ADR resolution rate decreased to 49.7% for FY 2012, when the U.S. Postal Service resolution rate (75.2%) is excluded from the government-wide average, which was down from the 50.9% in FY 2011. Agencies that had fewer than 25 ADR closures were not included in the ranking. Table B-5 in Appendix IV contains this information for all agencies and is located at www.eeoc.gov/.

Table 5 – Highest Pre-Complaint ADR Resolution Rates FY 2012

Agency	Total Work Force*	ADR Closures	ADR Resolutions	ADR Resolution Rate
Cabinet or Large (15,000 or more employees)				
Defense National Guard Bureau	57,511	47	43	91.5%
U.S. Postal Service	625,701	9,180	6,905	75.2%
Defense Logistics Agency	25,229	191	138	72.3%
Medium Agencies (1,000 to 14,999 employees)				
Defense Finance and Accounting Service	11,982	55	36	65.5%
Defense Contact Management Agency	10,452	36	19	52.8%
General Services Administration	12,416	66	27	40.9%

* Work force numbers as reported by the agency in its FY 2012 462 report.

e. Average Monetary Benefits in Pre-Complaint Phase Declined

Monetary benefit amounts awarded in settlements during the pre-complaint phase, shown in Table 6, declined in FY 2012 from the FY 2008 amounts while the number of settlements with monetary benefits increased in FY 2012. The data showed a decrease in the average amount of monetary benefits from $4,853 in FY 2011 to $4,652 in FY 2012.

Table 6 – Monetary Benefits Awarded In Settlements During the Pre-Complaint Stage of the EEO Process FY 2008 – FY 2012

FY	Completed Counselings	Total Resolutions #	%	Total Settlements #	%	Total Settlements with Monetary Benefits #	%	Settlement Monetary Benefits	Average Award per Resolution with Monetary Benefits
2008	38,898	21,431	55.1	7,573	19.5	659	8.7	$4,027,772	$6,112
2009	39,038	21,666	55.5	6,735	17.3	703	10.4	$3,715,972	$5,286
2010	40,563	22,094	54.5	6,332	15.6	577	9.1	$3,148,563	$5,457
2011	36,642	19,460	53.1	5,799	15.8	627	10.8	$3,042,646	$4,853
2012	34,521	18,449	53.4	5,353	15.5	740	13.8	$3,442,719	$4,652

f. The Most Frequently Alleged Basis and Issue Remain Unchanged

Of the 15,837 complaints filed in FY 2012, the basis most frequently alleged was reprisal/retaliation (7,457) and the issue most frequently alleged was non-sexual harassment (5,991). As shown in Tables 7 and 8, this has remained unchanged for the past five fiscal years. FY 2012 also saw a continuance of a five-year trend in complaints alleging both reprisal and age discrimination. Also in FY 2012, the number of complaints filed with allegations of race (Black/African American) once again exceeded those complaints filed with allegations of disability (physical).

An agency may not take an adverse action or otherwise "retaliate" against applicants or employees because they engaged in a protected activity. See EEOC's Facts About Retaliation for examples of adverse actions, protected activities and other guidance on retaliation.

Table 7 – Top 3 Bases in Complaint Allegations Filed for FY 2008 – FY 2012

Basis	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012
Reprisal/Retaliation	7,489	7,510	7,712	7,553	7,457
Age	4,977	5,058	5,314	5,105	4,915
Race – Black/African American	4,299		4,232	4,389	4,042
Disability (Physical)		4,006			

In FY 2012, allegations of race discrimination were made in 37.5% of all complaints, equal to the 37.5% of all complaints filed in FY 2011. In FY 2012, there was a 5.5% decrease in the number of complaints filed since FY 2008, and the percentage of complaints alleging discrimination based on race also decreased by 5.3%. During that

same period, the percentage of complaints filed alleging discrimination based on color increased 11.6%, from 1,653 in FY 2008 to 1,844 in FY 2012.[10]

Table 8 – Top 3 Issues in Complaint Allegations Filed for FY 2008 – FY 2012

Issue	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012
Harassment – Non-Sexual	4,999	5,599	5,907	5,863	5,991
Promotion/Non-Selection	2,882	2,574	2,530	2,683	2,250
Terms/Conditions	2,142	2,592	2,546	2,492	2,506

In April 2006, EEOC issued Section 15 of the new Compliance Manual on "Race and Color Discrimination." It includes numerous examples and guidance in proactive prevention and "best practices." This Manual Section is located at Compliance Manual Section 15: Race and Color Discrimination.

g. The Number of Timely Investigations Falls and Agencies Continue to Exceed Time Limits for Issuing Final Agency Decisions

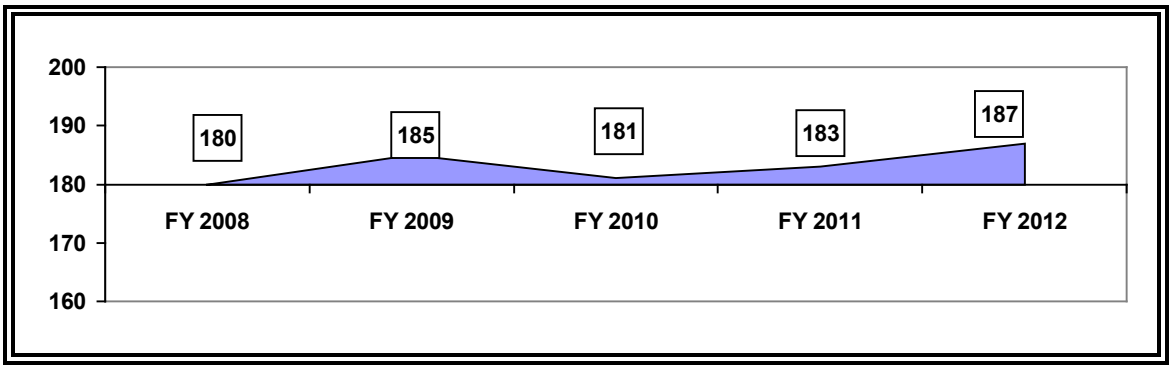
Investigations

Investigations into claims of discrimination are a key component of the formal EEO complaint process. Delays may impede the primary goal of gathering sufficient evidence to permit a determination as to whether discrimination occurred. EEOC regulation 29 C.F.R. §1614.106(e)(2) requires agencies to conduct an investigation and issue a report to the complainant within 180 days of the filing of a complaint unless: 1) the parties agreed to an extension of no more than 90 days (may not exceed 270 days); or 2) the complaint was amended or consolidated, which can add another 180 days to the period but may not exceed a total of 360 days.

In FY 2012, agencies timely completed investigations 74.9% of the time, up from 74.7% in FY 2011 (including written agreements to extend the investigation and consolidated or amended complaints). When the U.S. Postal Service is not included, the percentage of timely completed investigations also increased to 66.4% government-wide from the 65.3% timely completed in FY 2011. Agencies' average time to complete investigations increased from 183 days in FY 2011 to 187 days in FY 2012, leaving the FY 2007 reported average of 176 days as the best time for the previous twenty years.[11] See Figure 3 below.

[10] Complaints may contain multiple bases and issues.
[11] In 1993, agencies reported an average of 171 days to complete investigations.

Figure 3 – Average Processing Days for Investigations for FY 2008 – FY 2012



Of those investigations required to be completed within the 180-day time limit, agency in-house investigators averaged 220 days to complete the investigation in FY 2012, while contract investigators averaged 170 days. Several years ago, in a review of the investigatory practices of selected agencies, EEOC identified several reasons for untimely investigations: poorly staffed EEO offices, unnecessary and time-consuming procedures,[12] delays in obtaining affidavits, and inadequate tracking and monitoring systems. For more information, see EEOC's *Federal Sector Investigations – Time and Cost*, issued June 2004 and *Attaining a Model Agency Program: Efficiency.*

Four Agencies Timely Completed 100% of Investigations[13]

Among the agencies which completed 25 or more investigations in FY 2012, the Department of Education, Federal Deposit Insurance Corporation, Office of Personnel Management and the Tennessee Valley Authority all timely completed 100% of their investigations. See Table 9 below. Among cabinet or large agencies, the US Postal Service timely completed 99.0% of its 2,660 investigations in FY 2012. Agencies that had completed fewer than 25 investigations were not included in the ranking. Table B-9 in Appendix IV contains this information for all agencies and is located at http://www.eeoc.gov/.

[12] To include lengthy approval of investigative plans, or cumbersome procurement processes.
[13] An additional 21 agencies which completed less than 25 investigations, timely completed 100% of their investigations.

Table 9 – Highest Percentage of Timely Completed Investigations for FY 2012

Agencies	Total Work Force	# Completed Investigations	# Timely Completed	% Timely
Cabinet or Large (15,000 or more employees)				
U.S. Postal Service	625,701	2,660	2,636	99.1%
Department of Transportation	57,187	216	214	99.0%
Department of Labor	16,819	85	83	97.6%
Medium Agencies (1,000 to 14,999 employees)				
Department of Education	4,373	26	26	100%
Federal Deposit Insurance Corporation	7,846	29	29	100%
Office of Personnel Management	5,843	25	25	100%

In FY 2012, the government-wide average cost for contracting out complaint investigations was calculated at $2,811.07, a 5.3% decrease from the FY 2011 average cost of $2,968.99. Likewise, the FY 2012 average cost of agency (in-house) investigations ($7,156.72) decreased 8.1% from the FY 2011 average cost of $7,789.23. Average costs to contract out investigations in FY 2012 were approximately 60.7% less than the average costs of agency (in-house) investigations, which represent a decrease from 61.9% in FY 2011.

Final Agency Actions

EEOC regulations require an agency to take a final action on each formal complaint filed. Table 10 below provides a breakdown, with processing times, for all final agency actions. Agencies may issue a decision dismissing a complaint on procedural grounds such as untimely EEO counselor contact or failure to state a claim. In FY 2012, the government-wide average processing time for issuing a decision dismissing a complaint on procedural grounds was 92.5 days, an increase from FY 2011's 72.7 days but less than FY 2010's 100.2 day average processing times. EEOC maintains that, in general, acceptance letters/dismissal decisions should be issued well in advance of the 180 day time limit for completing an investigation, and has suggested a more practical time would be within 60 days of the filing of the formal complaint.

Table 10 – EEO Complaint Closures by Type with Government-Wide Average Processing Times in Days (APD) in FY 2008 – FY 2012

FY	Complaint Closures		Merit Final Agency Actions With AJ Decisions		Merit Final Agency Decisions Without AJ Decisions				Procedural Dismissals With & Without AJ Decisions		Settlements		Withdrawals	
	Total	APD	Total	APD from Comp. Filed	Total	APD	APD from Date Required	% Timely	Total	APD	Total	APD	Total	APD
2008	16,654	336	2,962	589	4,576	420	126	63.5%	4,298	88	3,249	371	1,569	219
2009	16,134	344	2,755	621	4,150	451	175	54.8%	4,370	83	3,394	378	1,465	222
2010	17,124	361	2,771	685	4,282	481	201	51.5%	5,091	100	3,623	388	1,357	220
2011	17,436	346	2,998	673	4,428	429	128	56.5%	4,853	73	3,785	382	1,372	234
2012	15,706	388	2,640	713	4,118	462	144	48.6%	3,515	92	4,076	409	1,357	232

An agency may also issue a decision after an investigation, either finding discrimination or finding no discrimination. In FY 2012, agencies timely issued 48.6% of their final agency merit decisions, a decrease from the 56.5% timely completed in FY 2011. Commission regulations require agencies to issue final decisions within 60 days of a complainant's request for such a decision or Administrative Judge's remand for a final agency decision. In addition, regulations require agencies to issue a final agency decision within 90 days after completion of an investigation if the complainant has not requested either a final decision or an EEOC hearing. In FY 2012, agencies issued merit final agency decisions without an Administrative Judge's decision in an average of 144 days, up from 128 days in FY 2011.

The Department of the Navy Issued the Highest Percentage of Timely Merit Decisions Without an Administrative Judge Decision

In FY 2012, the Department of the Navy reported it had issued 100% of its merit decisions without an EEOC Administrative Judge decision in a timely manner. The FY 2012 government-wide average for timely issued merit decision percentage was 48.6% with the U.S. Postal Service and dropped to 31.1% without the U.S. Postal Service. See Table 11 below.[14] Agencies that issued fewer than 25 merit decisions without a hearing were not included in the ranking. For information on all agencies, see Table B-14 in Appendix IV located at http://www.eeoc.gov/.

[14] We note that twenty other agencies issued 100.0% of their merit decisions in a timely fashion but issued fewer than 25 total merit decisions.

Table 11 – Agencies with the Highest Percentage of Timely Issued Merit Decisions (Without an Administrative Judge Decision) in FY 2012

Agencies	Total Work Force	Merit Decisions without an AJ Decision #	Timely	%
Cabinet or Large (15,000 or more employees)				
Department of the Navy	245,574	117	117	100%
U.S. Postal Service	625,701	1,088	1,062	97.6%
Department of the Treasury	115,292	123	108	87.8%
Medium Agencies (1,000 to 14,999 employees)				
Defense Commissary Agency	14,382	27	26	96.3%
Department of Labor	16,819	44	38	86.4%

Finally, when an EEOC Administrative Judge has issued a decision, the agency must issue a final order either implementing the Administrative Judge's decision or not implementing the decision and simultaneously appealing to EEOC. In FY 2012, agencies issued 2,708 final orders implementing and 35 orders not implementing the Administrative Judges' procedural and merit decisions. Commission regulations require agencies to issue an order within 40 calendar days of receiving the Administrative Judge's decision or the decision becomes the agency's final decision. In FY 2012, agencies issued orders on Administrative Judge merit decisions in an average of 713 days after the complaint was filed, an increase from 674 days in FY 2011 and from the 590 days in FY 2008.

h. Percentage of Findings of Discrimination and Average Monetary Benefits Decrease

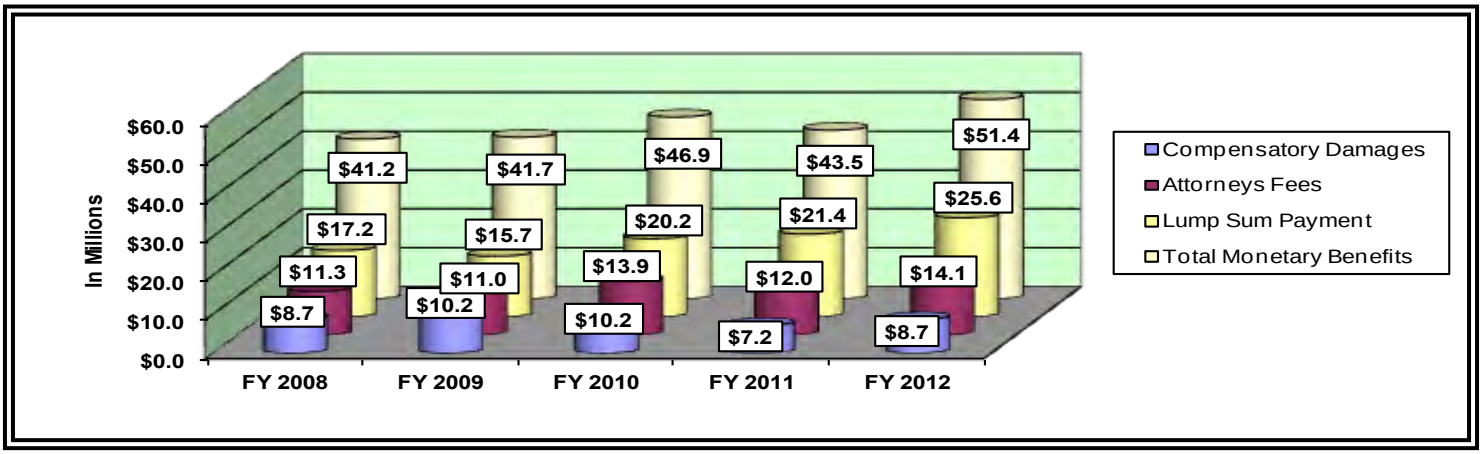
In FY 2012, the percentage of findings of discrimination increased to 3.1% from the 2.9% in FY 2011. Table 12, however, shows that the total number of merit decisions decreased while the number of settlements increased in FY 2012.

Table 12 – Amounts Awarded in Resolution of Formal EEO Complaints Before Appeals FY 2008 – FY 2012

Total Complaint Closures			Findings of Discrimination		Settlements		Monetary Benefits			
FY	#	Total Merit Decisions	#	% of Merits Decisions	#	% of Total Closures	# Total Complaint Closures with Benefits	% of Total Complaint Closures with Benefits	Total (in millions)	Per Capita
2008	16,654	7,538	191	2.5%	3,249	19.5%	3,383	20.3%	$41.2	$12,193
2009	16,134	6,905	206	3.0%	3,394	21.0%	3,555	22.0%	$41.7	$11,734
2010	17,124	7,053	233	3.3%	3,623	21.2%	3,803	22.2%	$46.9	$12,335
2011	17,436	7,426	212	2.9%	3,785	21.7%	3,953	22.7%	$43.5	$11,000
2012	15,706	6,758	214	3.1%	4,076	25.9%	4,257	27.1%	$51.4	$12,084

Average monetary benefits awarded in resolution of formal EEO complaints increased by 9.9% between FY 2011 and FY 2012, but decreased by 0.9% since FY 2008. Table 12 above shows the total monetary benefits awarded during the formal complaint process for the past five fiscal years, while Figure 4 below indicates the portion of these benefits awarded for compensatory damages, attorney's fees and lump sum payments, respectively.

Figure 4 – Monetary Benefits Awarded in the Formal Complaint Stage FY 2008 – FY 2012



i. Affirmation Rate of Final Agency Decisions on Appeal Fell

As demonstrated by Table 13 below, 63.9% of final agency decisions (FADs), excluding those in which an Administrative Judge issued a decision, were affirmed on appeal in FY 2012. This represents a 10.5% decrease from the FY 2011 affirmation rate and a 13.5% decrease from the FY 2008 affirmation rate.

Table 13 – Affirmation Rate of Final Agency Decisions on Appeal FY 2008 – FY2012

Fiscal Year	FADs Decided on Appeal	FADs Affirmed on Appeal	Percentage of FADs Affirmed on Appeal
FY 2008	2,473	1,828	73.9%
FY 2009	2,184	1,556	71.2%
FY 2010	2,543	1,759	69.2%
FY 2011	2,274	1,624	71.4%
FY 2012	2,471	1,578	63.9%

Some of the totals have been corrected from totals reported in previous Annual Reports.

2. EEOC Hearings and Appeals: Processing Times Increase for Hearings and Appeals

By federal regulation, EEOC becomes involved in the handling of an EEO complaint from an applicant for federal employment or a federal employee after the case initially has been processed by the employing agency and a hearing has been requested before an EEOC Administrative Judge or an appeal from a final agency action has been filed.

If a complainant requests a hearing, an EEOC Administrative Judge may oversee discovery between the parties and hold a hearing or issue a decision on the record. If a hearing is held, the Administrative Judge will hear the testimony of witnesses, review relevant evidence, and make findings of fact and conclusions of law in a decision issued to the parties. In appropriate cases, an Administrative Judge may, in lieu of holding a hearing, procedurally dismiss a case or issue a decision by summary judgment.

EEOC is also responsible for adjudicating appeals from final actions issued by federal agencies on complaints of employment discrimination. These final actions may involve an agency's decision to dismiss procedurally a complaint, a final decision on the merits of a complaint when the complainant has not requested a hearing, or a decision on whether or not to implement fully the decision of an EEOC Administrative Judge. Once appellate decisions are issued, EEOC monitors agency compliance with all orders and takes appropriate action to enforce them. EEOC's adjudicatory responsibilities also include resolving allegations of a breach of a settlement agreement involving a federal sector EEO complaint, as well as deciding petitions for review of decisions made by the Merit Systems Protection Board involving claims of discrimination and petitions for review of final grievance decisions when claims of discrimination are permitted to be raised in the grievance procedure.

In addition to, and equally important to its adjudicatory role, is EEOC's engagement in assisting federal agencies in the proactive prevention of discrimination. EEOC's Office of Federal Operations (OFO) provides outreach, technical assistance, and oversight to federal agencies, which includes conducting program reviews throughout the federal government to evaluate agencies' efforts to develop and maintain model EEO programs. OFO also monitors and evaluates agencies' activities to identify and correct barriers to equal opportunity, reasonable accommodation procedures for individuals with disabilities, and ADR programs. OFO also gathers and analyzes data provided by federal agencies on employment trends and EEO complaint processing; issues periodic reports which are publicly available; and works with individual agencies to identify both positive and negative trends in their EEO programs. In addition, through EEOC's Revolving Fund, OFO develops training and with staff from various EEOC offices

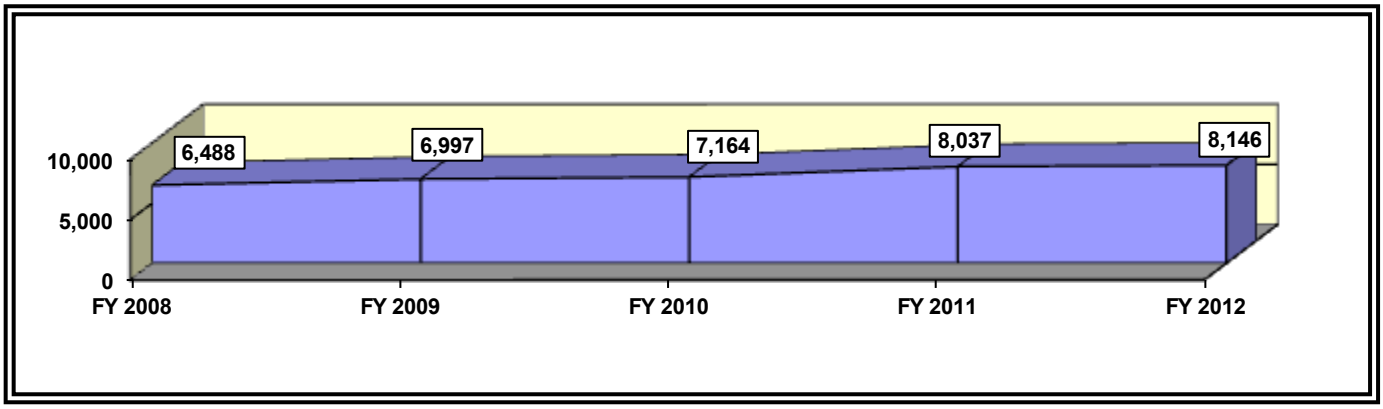
throughout the country, delivers these courses to federal agencies and other interested parties on a wide variety of federal-sector EEO topics.

a. HEARINGS

i. Hearings Inventory Continues to Rise

The year-end hearings inventory grew from 8,036 in FY 2011 to 8,146 in FY 2012, which represents an increase of 1.4%. Since FY 2008, the hearings inventory has increased 25.6%.

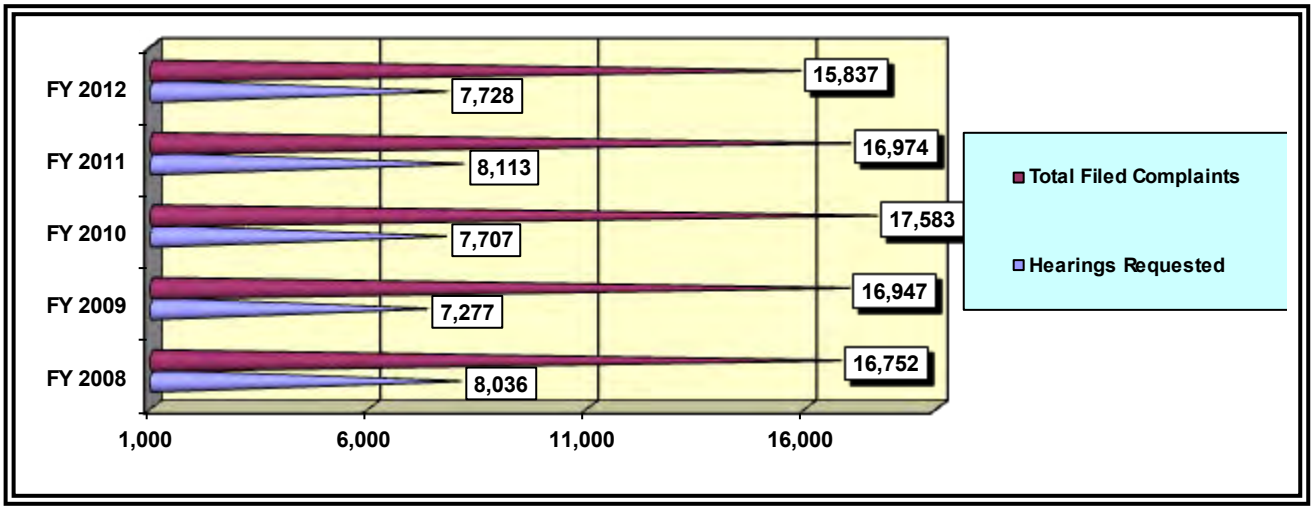
Figure 5 – Hearings Inventory FY 2008 – FY 2012



ii. Hearing Requests Decrease

Hearing requests decreased by 4.7% from 8,113 in FY 2011 to 7,728 in FY 2012, and decreased by 3.8% since FY 2008. For comparison purposes, the 7,728 hearings requested comprised 48.8% of the total complaints filed in FY 2012.

Figure 6 – Comparison of Requests for EEOC Hearings to Complaints Filed FY 2008 – FY 2012



iii. Hearing Closures

During FY 2012, EEOC's Hearings Program resolved 7,538 cases (including 28 class actions), which represents a 1.7% decrease from the 7,672 cases resolved in FY 2011 and a 5.6% increase from the 7,138 cases closed in FY 2008. Excluding the class actions, the 7,510 individual cases in FY 2012 were closed in the following manner: 9.6% were by decision following a hearing; 28.1% were by decisions on the record; 31.2% were closed by settlements; 12.3% were by procedural dismissal; and 18.9% were withdrawals. See Table 14 for a comparison of FY 2008 – FY 2012.

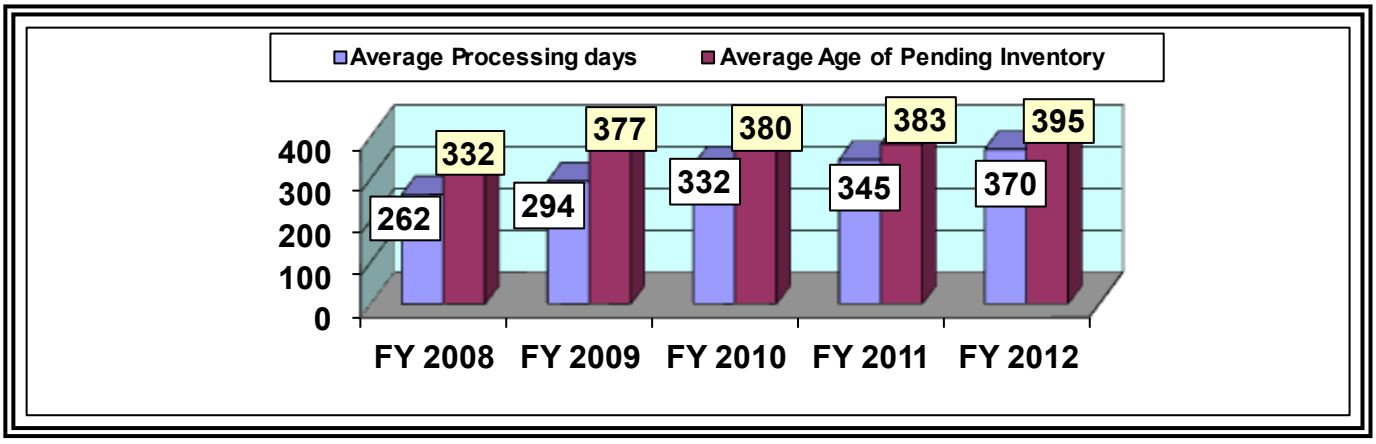
Table 14 – Hearings Program Individual Case Closures: FY 2008 – FY 2012

Closure Type	FY 2008		FY 2009		FY 2010		FY 2011		FY 2012	
	#	%	#	%	#	%	#	%	#	%
Decisions Following a Hearing	867	12.2	822	12.2	806	11.2	817	10.7	718	9.6
Decisions On the Record	1,958	27.7	1,919	28.6	2,102	29.3	2,108	27.6	2,108	28.1
Settlements	1,803	25.5	1,892	28.2	2,120	29.6	2,321	30.4	2,340	31.2
Procedural Dismissals	1,042	14.7	859	12.8	924	12.9	1,057	13.8	925	12.3
Withdrawals	1,408	19.9	1,220	18.2	1,217	16.9	1,339	17.5	1,419	18.9
Total Individual Case Closures	7,078		6,712		7,169		7,642		7,510	

iv. Average Processing Time for Hearings

The average processing time for hearing closures increased from 345 days in FY 2011 to 370 days in FY 2012, and also represents an increase from the 262 days in FY 2008. The average age of the pending inventory increased to 395 days in FY 2012 from 383 days in FY 2011, and also exceeded the 332 days in FY 2008.

Figure 7 - Average Processing Days for Hearings
FY 2008 - FY 2012



v. Agencies Challenge Findings of Discrimination

In FY 2012, EEOC Administrative Judges issued 148 decisions finding discrimination, which was 5.2% of all decisions on the merits of complaints. In comparison to the 164 decisions finding discrimination that Administrative Judges issued in FY 2011, the 148 decisions in FY 2012 represents a 9.8% decrease. Agencies may either fully implement the Administrative Judge's decision or not fully implement and simultaneously appeal the Administrative Judge's decision to the OFO. In FY 2012, agencies appealed only 1.3% of all Administrative Judge decisions. However, they appealed 20.0% of the cases where an Administrative Judge found discrimination.

Table 15 - Agency Actions on Administrative Judge Decisions FY 2008 - FY 2012

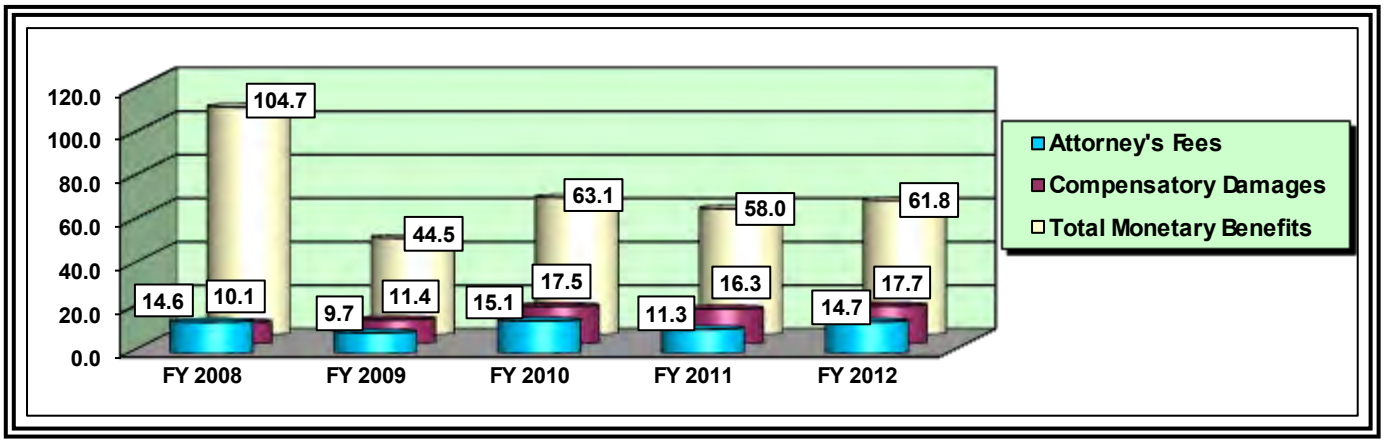
FY	Finding Discrimination[15]				Finding No Discrimination				Totals			
	Implemented		Appealed		Implemented		Appealed		Implemented		Appealed	
	#	%	#	%	#	%	#	%	#	%	#	%
2008	107	65.2%	57	34.8%	2,794	99.9%	4	0.1%	2,901	97.9%	61	2.1%
2009	103	69.6%	45	30.4%	2,606	99.9%	1	0.04%	2,709	98.3%	46	1.7%
2010	119	69.2%	53	30.8%	2,596	99.9%	3	0.12%	2,715	98.0%	56	2.0%
2011	116	72.5%	44	27.5%	2,833	94.7%	5	0.18%	2,954	98.5%	49	1.6%
2012	124	80.0%	31	20.0%	2,481	99.8%	4	0.16%	2,605	98.7%	35	1.3%

vi. Monetary Benefits Decrease at Hearings

In FY 2012, Administrative Judges' decisions and settlements at the hearings stage awarded $61.8 million in benefits, as compared to the $58 million in FY 2011 and the $104.7 million awarded in FY 2008. Note that benefits awarded by decisions of Administrative Judges at the hearings stage are preliminary, pending a decision on implementation by the agency or on appeal.

[15] These numbers do not parallel Administrative Judge findings of discrimination because agencies may not take final action in the same fiscal year as the decision was issued. Also, agencies may settle a complaint where the Administrative Judge has found discrimination.

Figure 8 - Monetary Benefits Awarded from Hearings (In Millions of Dollars) FY 2008 - FY 2012



The total FY 2008 award included a large class action complaint settlement.

vii. Affirmation Rate of AJ Decisions on Appeal Drops Slightly

As demonstrated by the table below, 89.3% of Administrative Judges' decisions were affirmed on appeal in FY 2012.[16] The number of appealed Administrative Judges' decisions decreased 35.4% over the five year period between FY 2008 to FY 2012; the affirmation rate also fell by 38.8% during this time period.

Table 16 – Affirmation Rate of AJ Decisions on Appeal FY 2008 - FY 2012

Fiscal Year	AJ Decisions Appealed			AJ Decisions Affirmed on Appeal			% of AJ Decisions Affirmed on Appeal		
	Total	Appeal By Agency[17]	Appeal By Appellant	Total	Appeal By Agency	Appeal By Appellant	Total	Appeal By Agency	Appeal By Appellant
2008	1,284	81	1,203	1,211	64	1,147	94.3%	79.0%	94.7%
2009	972	50	922	928	38	890	95.5%	76.0%	96.5%
2010	972	55	917	916	47	869	94.2%	85.5%	94.7%
2011	1,065	39	1,026	989	34	955	92.9%	87.2%	93.1%
2012	830	46	784	741	33	708	89.3%	71.7%	90.3%

[16] Administrative Judge's decisions reported here do not include Petitions for Enforcement or procedural cases.

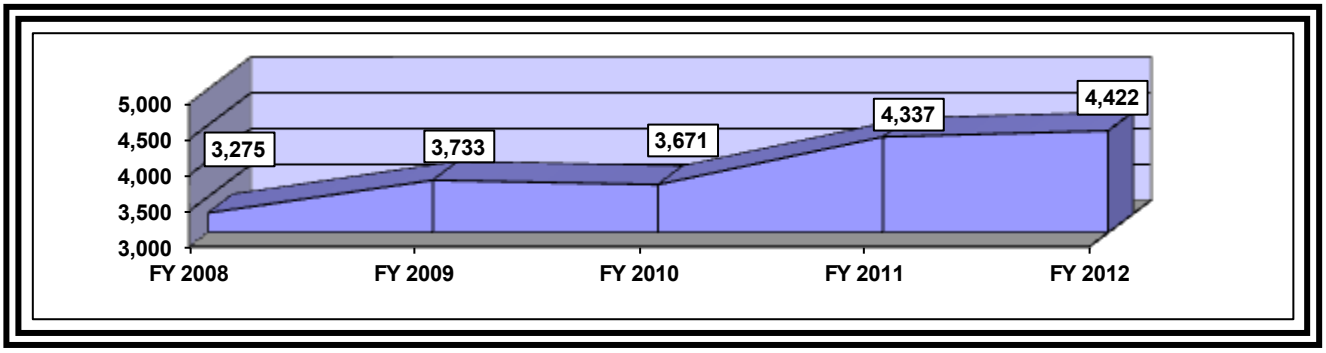
[17] "Appeal By Agency" occurs when the agency does not fully implement the Administrative Judge's decision.

b. APPEALS

i. Appeals Inventory Increases

OFO's appellate inventory, at the close of FY 2012 rose to 4,422, which represents a 1.9% increase from the 4,337 case inventory at the close of FY 2011 and a 35% increase from the 3,275 case inventory at the close of FY 2008.

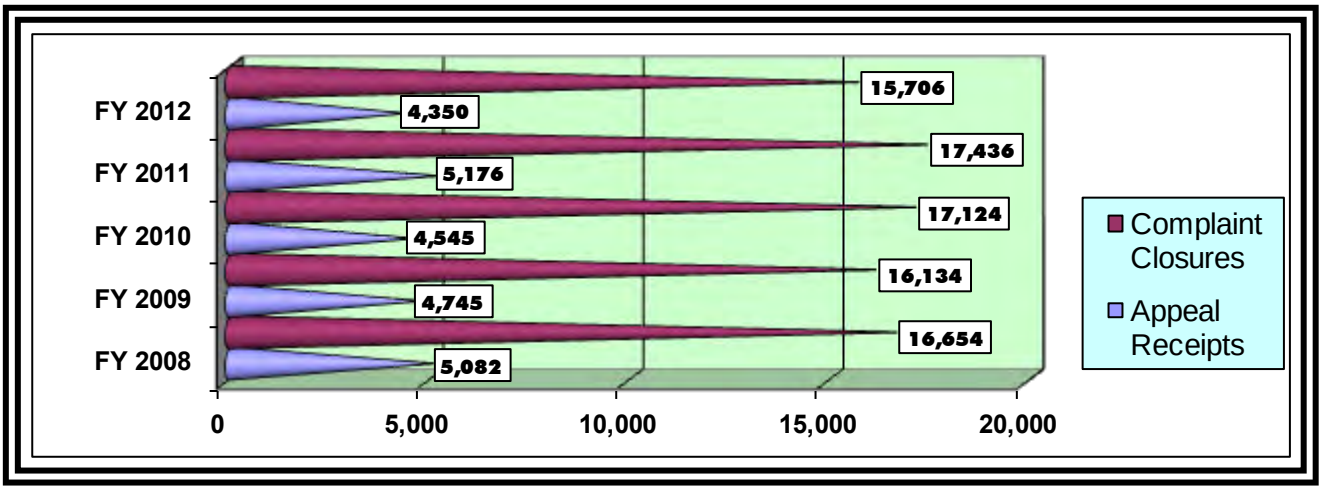
Figure 9 - Appellate Inventory FY 2008 - FY 2012



ii. Appeal Receipts On the Decline

OFO received 4,350 appeals in FY 2012, representing a 15.9% decrease from the 5,176 appeals filed in FY 2011. FY 2012 appeal receipts represented a 14.4% decrease from the 5,082 appeals received in FY 2008. In FY 2012, 27.7% of closed complaints were appealed, which was less than the 30.5% in FY 2008.

Figure 10 – Comparison of Appeals Receipts to Complaint Closures FY 2008 - FY 2012



iii. Appeal Closures Down

OFO closed a total of 4,265 appellate cases in FY 2012, slightly fewer than the 4,510 appellate cases closed in FY 2011. Of the FY 2012 closed cases, 2,830 (66.4%) alleged violations of Title VII; 1,077 (25.3%) involved the Rehabilitation Act; 1,052 (24.7%) alleged violations of the ADEA; and 17 (0.4%) involved the Equal Pay Act of 1963. In FY 2011, OFO closed a total of 4,510 appellate cases, of which 2,793 were Title VII cases (61.9%); 1,212 involved the Rehabilitation Act (26.9%); 1,084 alleged violations of the ADEA (24.0%); and 16 involved the Equal Pay Act of 1963 (0.4%).[18] See Figure 11 for the appeal closures from FY 2008 to FY 2012.

Figure 11 - Appeal Closures FY 2008 - FY 2012

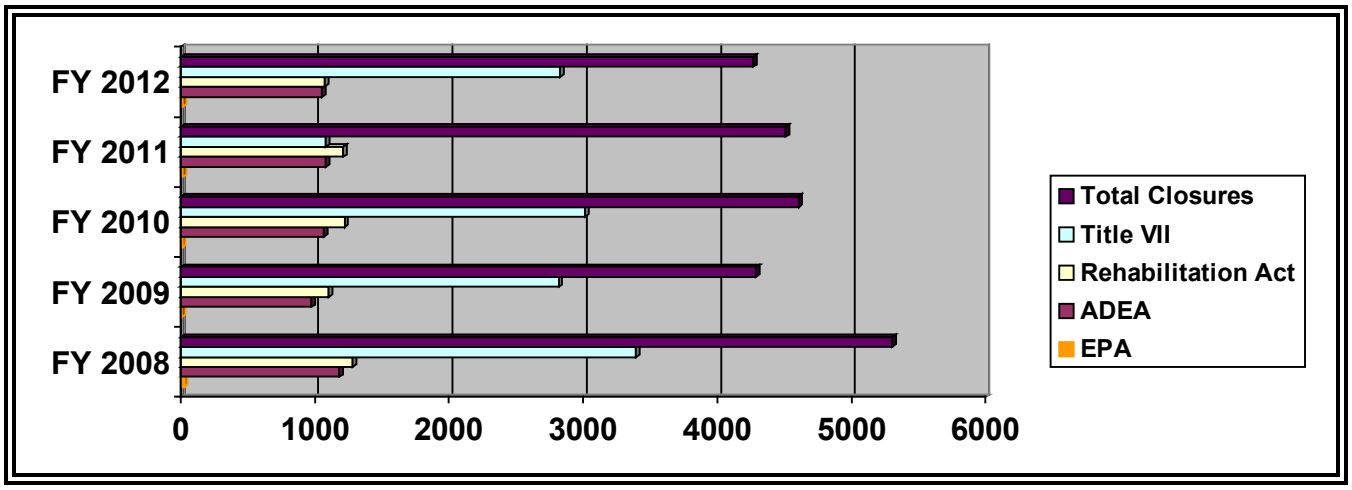


Table 17 below provides a breakdown by appeal type of all FY 2012 appellate receipts and closures.

Table 17 - Types of Receipts and Appeals FY 2012

Types of Appeals	Receipts		Closures	
	#	% of Total	#	% of Total
Total	4,350		4,265	
Initial Appeals from Complainants	3,577	82.2	3,613	84.7
Initial Appeals from Agencies	41	0.9	52	1.2
Petitions to Review MSPB Decisions	69	1.6	52	1.2
Appeals from a Grievance/Arbitration of FLRA Decisions	7	0.2	10	0.2
Petitions for Enforcement	13	0.3	10	0.2
Requests for Reconsiderations	643	14.8	528	12.4

[18] The number and percentage of resolutions by statute is greater than the number of cases closed, because one or more statutory bases may be alleged in each appeal.

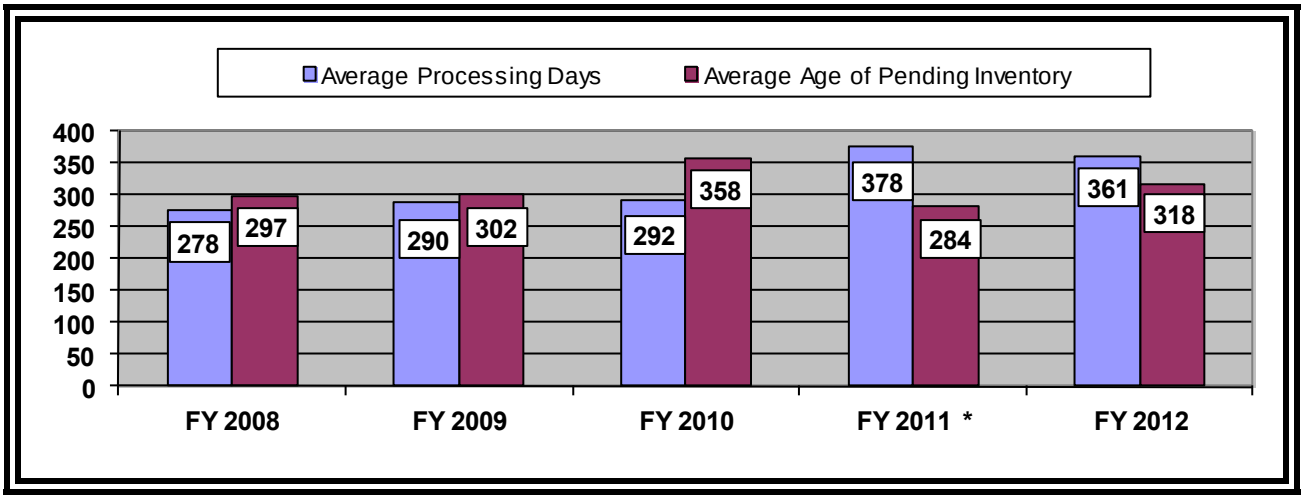
In FY 2012, OFO closed 1,735 appeals addressing the merits of the underlying discrimination claims, and made a total of 109 findings of discrimination, which represents 6.3% of the total. By comparison, in FY 2011, OFO closed 1,960 appeals addressing the merits of the underlying discrimination claims, and made a total of 87 findings of discrimination, which represented 4.4% of the total. In FY 2012, OFO reversed 31.5% of the 2,209 appeals of procedural dismissals.

iv. Average Processing Time of Appeal Closures

The average processing time for appeal closures fell to 361 days in FY 2012, representing a 4.5% decrease from 378 days in FY 2011 and a 29.9% increase from 278 days in FY 2008.

OFO resolved 2,258 (52.9%) of the 4,265 appeals closed in FY 2012 within 180 days. The average age of the pending inventory at the end of FY 2012 was 318 days, a 11.9% increase from the 284 day average age at the end of FY 2011 and a 7.1% increase from the 297 day average age of the open inventory at the end of FY 2008.

Figure 12 - Average Processing Days on Appeal
FY 2008 - FY 2012



*During FY 2011 OFO closed substantially more aged appeals than in recent fiscal years, resulting in the increase to average processing time and a corresponding decrease in the average age of the pending inventory.

v. Three Most Prevalent Bases and Issues on Appeal

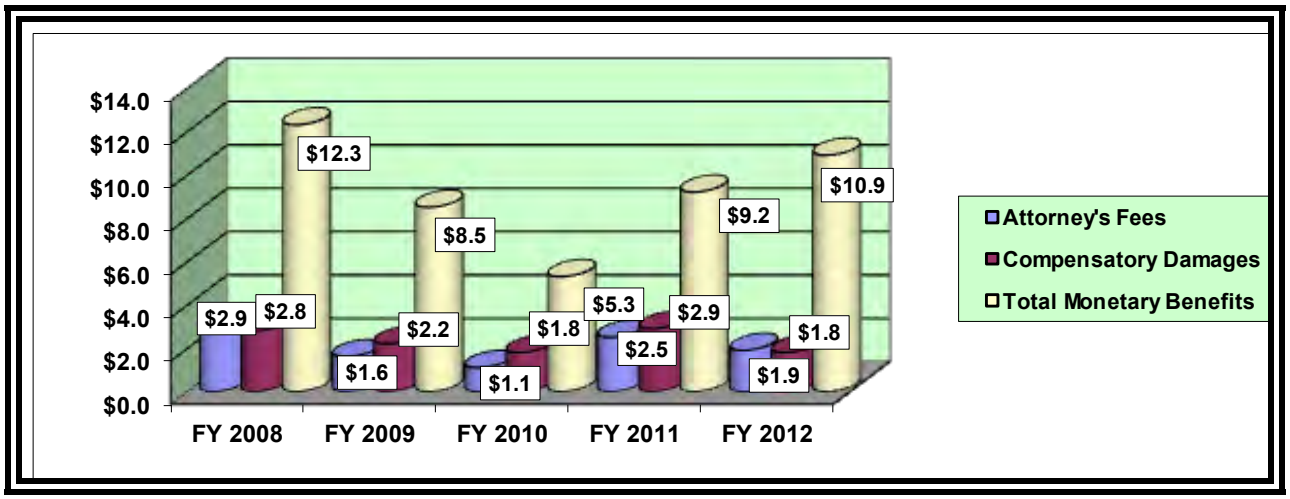
Since FY 2007, reprisal has been the top basis of discrimination alleged in closed appeals. In FY 2012, sex was the second most alleged basis, with race as the third most prevalent basis of discrimination alleged in closed appeals. Harassment,

promotion, and removal were the three most prevalent issues of discrimination alleged in closed appeals.

vi. $10.9 Million Awarded on Appeal

In FY 2012, the $10.9 million in monetary benefits awarded in compliance with appellate decisions (including settlement agreements resolving appeals) increased by 18.5% from the $9.2 million awarded in FY 2011 and a 11.4% decrease from the $12.3 million awarded in FY 2008.

Figure 13 - Monetary Benefits Awarded from Appeals[19] FY 2008 - FY 2012 (In Millions of Dollars)



vii. Training and Outreach Conducted By EEOC

In FY 2012, EEOC staff members informed a large number of federal employees of their rights and responsibilities under the EEO process, affirmative employment programs, and laws that the Commission enforces. EEOC's proactive prevention activities targeted multiple agencies, and provided agency managers and supervisors with a better understanding of how to prevent employment discrimination within their workplace. OFO staff members, as well as staff from various EEOC offices throughout the country provided these training sessions.

Specifically, staff members conducted 95 training sessions reaching 2,440 federal employees, including 154 new EEO counselors, 150 new EEO investigators, and 249 EEO professionals in affirmative employment programs.

[19] It should be noted that Hearings Benefits should not be added to Appeals Benefits for a grand total, as Hearings Benefits are only preliminary.

In an ongoing effort to provide the federal sector EEO community and stakeholders with timely and accurate information, OFO staff members responded to more than 8,168 calls concerning the federal sector EEO complaint process.

The Commission's training and outreach information can be found at http://www.eeoc.gov/federal/training/index.cfm.

Section C - Responsiveness and Legal Compliance

The sixth MD-715 element, "Responsiveness and Legal Compliance," encompasses agencies' timely filing of required reports with EEOC and timely compliance with EEOC's issued orders.

1. 92% of Submitted EEOC Form 462 Reports Were Timely

EEOC regulation 29 C.F.R. § 1614.602(a) requires agencies to report to the EEOC information concerning pre-complaint counseling, ADR, and the status, processing, and disposition of complaints at such times and in such manner as the Commission prescribes.

The requirement to file an EEOC Form 462 Report applies to all federal agencies and departments covered by 29 C.F.R. Part 1614, as defined in 29 C.F.R. § 1614.103(b). This includes Executive agencies as defined in 5 U.S.C. 105, military departments as defined in 5 U.S.C. 102, the Government Printing Office, the Postal Regulatory Commission, the Smithsonian Institution, the Tennessee Valley Authority, the United States Postal Service, and those units of the judicial branch of the federal government having positions in the competitive service. All covered agencies must file Form 462 Reports with the Commission. EEOC Form 462 Reports are due on or before October 31st of each year.

In FY 2012, 90 or 91.8% of the 98 agencies (with 100 or more employees) timely submitted the EEOC Form 462 Report, up from the 90.1% timely submitted in FY 2011. In FY 2008 EEOC made the report submission paperless for agencies by assigning a unique personal identification number (PIN) to agency EEO Directors for use as their signatures. The PIN needed to be entered on the secure web site by the November 5nd deadline to be considered timely.[20] See Appendix III for the list of agencies' FY 2012 report submission times.

[20] The deadline set by the Commission is October 31st, however due to severe weather the deadline was extended to November 5th, 2012.

II. PROFILES FOR SELECTED FEDERAL AGENCIES

What follows are individual profiles of federal agencies with a total work force of 500 or more employees. These profiles of selected indicators were created from data submitted by agencies in annual EEOC Form 462 reports.

The profiles contain a number of measures related to the agencies' EEO complaint activities, including the number of complaints filed, complainants, closed complaints, merit decisions, findings of discrimination, and settlements. Also included are timeliness measures for various stages of EEO complaint processing and some of the costs associated with the process. EEOC relies on each agency to provide accurate and reliable data for its complaint processing program. Although the EEOC reviews and analyzes the data submitted, each agency remains ultimately responsible for the accuracy of its own data.

Finally, each profile offers data concerning an agency's success in implementing ADR activities at the pre-complaint and formal complaint stages of the discrimination complaint process. EEOC is firmly committed to using ADR to resolve workplace disputes. Used properly and in appropriate circumstances, ADR can provide faster and less expensive results while at the same time improving workplace communication and morale.

List of Agencies Included in the Agency Profile Section

In addition to the government-wide profile, the following agencies have profiles listed alphabetically in this part:

Government-Wide (The Government) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	16,878		17,643		34,521	
Settlements	549	3.3%	4,804	27.2%	5,353	15.5%
Withdrawals or No Complaints Filed	6,786	40.2%	6,310	35.8%	13,096	37.9%
Complaints Filed*					15,211	44.1%
Decision to File Complaint Pending at End of FY					862	2.5%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	34,521	85.7%	51.1%
Complaint Closures	15,706	20.3%	8.1%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Age	Race (Black or African American)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	34,486	32,043	92.9%				
All Investigations	10,226	7,660	74.9%	183	187	2.2%	187
All Complaint Closures	15,706			346	388	12.1%	388
Merit Decisions (no AJ)	4,118	2,003	48.6%	430	462	7.4%	462
Dismissal Decisions (no AJ)	3,412			62	92	48.4%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	15,837							
Total Closures	15,706							
Settlements	4,076	26%						
Withdrawals	1,357	8.6%						
Total Final Agency Actions	10,273	65.4%	7,530	73.3%	2,708	26.4%	35	0.3%
Dismissals	3,515	34.2%	3,412	97.1%	103	2.9%	0	0%
Merit Decisions	6,758	65.8%	4,118	60.9%	2,605	38.5%	35	0.5%
Finding Discrimination	214	3.2%	59	27.6%	124	57.9%	31	14.5%
Finding No Discrimination	6,544	96.8%	4,059	62%	2,481	37.9%	4	0.1%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	740	$3,442,718	$4,652
ADR Settlements w/ Monetary Benefits	621	$2,399,280	$3,863
Investigation Costs	10,226	$44,029,679	$4,305
Complaint Closures with Monetary Benefits	2,758	$51,443,329	$18,652
ADR Settlements w/ Monetary Benefits	415	$5,288,912	$12,744

Agency for International Development (AID) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	29		5		34	
Settlements	0	0%	1	20%	1	2.9%
Withdrawals or No Complaints Filed	14	48.3%	3	60%	17	50%
Complaints Filed*					14	41.2%
Decision to File Complaint Pending at End of FY					2	5.9%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	34	85.3%	14.7%
Complaint Closures	16	6.3%	0%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Age	National Origin (Other)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	34	23	67.7%				
All Investigations	13	1	7.7%	294	282	-4.1%	187
All Complaint Closures	16			484	399	-17.6%	388
Merit Decisions (no AJ)	1	0	0%	389	830	113.4%	462
Dismissal Decisions (no AJ)	7			70	92	31.4%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	14							
Total Closures	16							
Settlements	4	25%						
Withdrawals	3	18.8%						
Total Final Agency Actions	9	56.3%	8	88.9%	1	11.1%	0	0%
Dismissals	7	77.8%	7	100%	0	0%	0	0%
Merit Decisions	2	22.2%	1	50%	1	50%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	2	100%	1	50%	1	50%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	1	$6,000	$6,000
ADR Settlements w/ Monetary Benefits	1	$6,000	$6,000
Investigation Costs	13	$30,971	$2,382
Complaint Closures with Monetary Benefits	4	$253,024	$63,256
ADR Settlements w/ Monetary Benefits	0	$0	$0

Department of Agriculture (USDA) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	720		255		975	
Settlements	42	5.8%	55	21.6%	97	10%
Withdrawals or No Complaints Filed	277	38.5%	78	30.6%	355	36.4%
Complaints Filed*					496	50.9%
Decision to File Complaint Pending at End of FY					27	2.8%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	975	76.8%	26.2%
Complaint Closures	453	32.5%	16.8%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Sex (Female)	Age

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	975	713	73.1%				
All Investigations	437	217	49.7%	270	242	-10.4%	187
All Complaint Closures	453			496	633	27.6%	388
Merit Decisions (no AJ)	151	42	27.8%	638	638	0%	462
Dismissal Decisions (no AJ)	48			133	112	-15.8%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	524							
Total Closures	453							
Settlements	170	37.5%						
Withdrawals	29	6.4%						
Total Final Agency Actions	254	56.1%	199	78.3%	55	21.7%	0	0%
Dismissals	48	18.9%	48	100%	0	0%	0	0%
Merit Decisions	206	81.1%	151	73.3%	55	26.7%	0	0%
Finding Discrimination	11	5.3%	10	90.9%	1	9.1%	0	0%
Finding No Discrimination	195	94.7%	141	72.3%	54	27.7%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	29	$341,933	$11,790
ADR Settlements w/ Monetary Benefits	10	$153,963	$15,396
Investigation Costs	437	$1,535,339	$3,513
Complaint Closures with Monetary Benefits	138	$2,894,572	$20,975
ADR Settlements w/ Monetary Benefits	24	$846,614	$35,275

Department of the Air Force (USAF) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	563		439		1,002	
Settlements	24	4.3%	162	36.9%	186	18.6%
Withdrawals or No Complaints Filed	284	50.4%	59	13.4%	343	34.2%
Complaints Filed*					458	45.7%
Decision to File Complaint Pending at End of FY					15	1.5%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	1,002	74.2%	43.8%
Complaint Closures	500	48.8%	17.2%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Age	Race (Black or African American)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	996	897	90.1%				
All Investigations	305	53	17.4%	206	263	27.7%	187
All Complaint Closures	500			395	483	22.3%	388
Merit Decisions (no AJ)	96	12	12.5%	630	839	33.2%	462
Dismissal Decisions (no AJ)	67			61	98	60.7%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	473							
Total Closures	500							
Settlements	174	34.8%						
Withdrawals	57	11.4%						
Total Final Agency Actions	269	53.8%	163	60.6%	105	39%	1	0.4%
Dismissals	76	28.3%	67	88.2%	9	11.8%	0	0%
Merit Decisions	193	71.7%	96	49.7%	96	49.7%	1	0.5%
Finding Discrimination	7	3.6%	0	0%	7	100%	0	0%
Finding No Discrimination	186	96.4%	96	51.6%	89	47.8%	1	0.5%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	18	$172,541	$9,585
ADR Settlements w/ Monetary Benefits	16	$167,740	$10,483
Investigation Costs	305	$1,353,190	$4,436
Complaint Closures with Monetary Benefits	99	$2,075,106	$20,960
ADR Settlements w/ Monetary Benefits	28	$514,458	$18,373

Department of the Army (ARMY) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	1,748		553		2,301	
Settlements	89	5.1%	175	31.7%	264	11.5%
Withdrawals or No Complaints Filed	608	34.8%	177	32%	785	34.1%
Complaints Filed*					1,179	51.2%
Decision to File Complaint Pending at End of FY					73	3.2%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	2,301	43.2%	24%
Complaint Closures	1,116	22.8%	15.1%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Race (Black or African American)	Sex (Female)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	2,299	2,008	87.3%				
All Investigations	484	114	23.6%	235	258	9.8%	187
All Complaint Closures	1,116			260	325	25%	388
Merit Decisions (no AJ)	181	21	11.6%	440	528	20%	462
Dismissal Decisions (no AJ)	234			37	44	18.9%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	1,226							
Total Closures	1,116							
Settlements	476	42.7%						
Withdrawals	100	9%						
Total Final Agency Actions	540	48.4%	415	76.9%	121	22.4%	4	0.7%
Dismissals	237	43.9%	234	98.7%	3	1.3%	0	0%
Merit Decisions	303	56.1%	181	59.7%	118	38.9%	4	1.3%
Finding Discrimination	10	3.3%	2	20%	5	50%	3	30%
Finding No Discrimination	293	96.7%	179	61.1%	113	38.6%	1	0.3%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	41	$208,167	$5,077
ADR Settlements w/ Monetary Benefits	25	$39,063	$1,562
Investigation Costs	484	$3,014,704	$6,228
Complaint Closures with Monetary Benefits	244	$4,538,819	$18,601
ADR Settlements w/ Monetary Benefits	40	$323,748	$8,093

Defense Army and Air Force Exchange (AAFES) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	260		76		336	
Settlements	8	3.1%	18	23.7%	26	7.7%
Withdrawals or No Complaints Filed	171	65.8%	33	43.4%	204	60.7%
Complaints Filed*					98	29.2%
Decision to File Complaint Pending at End of FY					8	2.4%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	336	100%	22.6%
Complaint Closures	89	89.9%	15.7%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Disability (Physical)	Age

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	336	255	75.9%				
All Investigations	38	5	13.2%	195	235	20.5%	187
All Complaint Closures	89			313	318	1.6%	388
Merit Decisions (no AJ)	14	13	92.9%	360	346	-3.9%	462
Dismissal Decisions (no AJ)	20			112	75	-33%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	101							
Total Closures	89							
Settlements	26	29.2%						
Withdrawals	16	18%						
Total Final Agency Actions	47	52.8%	34	72.3%	13	27.7%	0	0%
Dismissals	20	42.6%	20	100%	0	0%	0	0%
Merit Decisions	27	57.4%	14	51.9%	13	48.1%	0	0%
Finding Discrimination	1	3.7%	1	100%	0	0%	0	0%
Finding No Discrimination	26	96.3%	13	50%	13	50%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	3	$2,569	$856
ADR Settlements w/ Monetary Benefits	3	$2,569	$856
Investigation Costs	38	$446,869	$11,759
Complaint Closures with Monetary Benefits	16	$120,914	$7,557
ADR Settlements w/ Monetary Benefits	4	$25,455	$6,363

Broadcasting Board of Governors (BBG) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	51		2		53	
Settlements	5	9.8%	0	0%	5	9.4%
Withdrawals or No Complaints Filed	34	66.7%	2	100%	36	67.9%
Complaints Filed*					12	22.6%
Decision to File Complaint Pending at End of FY					0	0%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	53	100%	3.8%
Complaint Closures	14	100%	0%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Race (Black or African American)	Race (Two or More Races)	Sex (Female)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	53	51	96.2%				
All Investigations	5	5	100%	133	161	21.1%	187
All Complaint Closures	14			358	356	-0.6%	388
Merit Decisions (no AJ)	2	2	100%	296	326	10.1%	462
Dismissal Decisions (no AJ)	5			37	236	537.8%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	12							
Total Closures	14							
Settlements	6	42.9%						
Withdrawals	0	0%						
Total Final Agency Actions	8	57.1%	7	87.5%	1	12.5%	0	0%
Dismissals	5	62.5%	5	100%	0	0%	0	0%
Merit Decisions	3	37.5%	2	66.7%	1	33.3%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	3	100%	2	66.7%	1	33.3%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	1	$1,000	$1,000
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	5	$27,000	$5,400
Complaint Closures with Monetary Benefits	1	$35,000	$35,000
ADR Settlements w/ Monetary Benefits	0	$0	$0

Department of Commerce (DOC) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	288		37		325	
Settlements	4	1.4%	7	18.9%	11	3.4%
Withdrawals or No Complaints Filed	73	25.3%	12	32.4%	85	26.2%
Complaints Filed*					222	68.3%
Decision to File Complaint Pending at End of FY					7	2.2%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	325	28.3%	11.4%
Complaint Closures	432	3%	3%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Age	Race (Black or African American)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	325	275	84.6%				
All Investigations	183	166	90.7%	227	188	-17.2%	187
All Complaint Closures	432			289	465	60.9%	388
Merit Decisions (no AJ)	189	26	13.8%	451	569	26.2%	462
Dismissal Decisions (no AJ)	49			102	66	-35.3%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	222							
Total Closures	432							
Settlements	74	17.1%						
Withdrawals	12	2.8%						
Total Final Agency Actions	346	80.1%	238	68.8%	106	30.6%	2	0.6%
Dismissals	57	16.5%	49	86%	8	14%	0	0%
Merit Decisions	289	83.5%	189	65.4%	98	33.9%	2	0.7%
Finding Discrimination	8	2.8%	1	12.5%	6	75%	1	12.5%
Finding No Discrimination	281	97.2%	188	66.9%	92	32.7%	1	0.4%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	1	$25,000	$25,000
ADR Settlements w/ Monetary Benefits	1	$25,000	$25,000
Investigation Costs	183	$1,045,662	$5,714
Complaint Closures with Monetary Benefits	61	$1,054,737	$17,290
ADR Settlements w/ Monetary Benefits	1	$15,000	$15,000

Commodity Futures Trading Commission (CFTC) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	1		0		1	
Settlements	0	0%	0	0%	0	0%
Withdrawals or No Complaints Filed	0	0%	0	0%	0	0%
Complaints Filed*					1	100%
Decision to File Complaint Pending at End of FY					0	0%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	1	100%	0%
Complaint Closures	2	0%	0%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Sex (Female)	National Origin (Other)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	1	1	100%				
All Investigations	1	1	100%	330	110	-66.7%	187
All Complaint Closures	2			0	314	NA%	388
Merit Decisions (no AJ)	2	1	50%	0	314	NA%	462
Dismissal Decisions (no AJ)	0			0	0	NA%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	1							
Total Closures	2							
Settlements	0	0%						
Withdrawals	0	0%						
Total Final Agency Actions	2	100%	2	100%	0	0%	0	0%
Dismissals	0	NA%	0	NA%	0	0%	0	0%
Merit Decisions	2	100%	2	100%	0	0%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	2	100%	2	100%	0	0%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	1	$6,750	$6,750
Complaint Closures with Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0

Consumer Financial Protection Bureau (CFPB) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	8		7		15	
Settlements	0	0%	2	28.6%	2	13.3%
Withdrawals or No Complaints Filed	1	12.5%	1	14.3%	2	13.3%
Complaints Filed*					11	73.3%
Decision to File Complaint Pending at End of FY					0	0%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	15	86.7%	46.7%
Complaint Closures	7	85.7%	14.3%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Age	Reprisal	National Origin (Hispanic)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	15	11	73.3%				
All Investigations	3	3	100%	0	209	NA%	187
All Complaint Closures	7			0	181	NA%	388
Merit Decisions (no AJ)	3	3	100%	0	301	NA%	462
Dismissal Decisions (no AJ)	0			0	0	NA%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	11							
Total Closures	7							
Settlements	3	42.9%						
Withdrawals	1	14.3%						
Total Final Agency Actions	3	42.9%	3	100%	0	0%	0	0%
Dismissals	0	NA%	0	NA%	0	0%	0	0%
Merit Decisions	3	100%	3	100%	0	0%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	3	100%	3	100%	0	0%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	3	$23,469	$7,823
Complaint Closures with Monetary Benefits	2	$40,000	$20,000
ADR Settlements w/ Monetary Benefits	0	$0	$0

Consumer Product Safety Commission (CPSC) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	2		1		3	
Settlements	0	0%	0	0%	0	0%
Withdrawals or No Complaints Filed	0	0%	0	0%	0	0%
Complaints Filed*					2	66.7%
Decision to File Complaint Pending at End of FY					1	33.3%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	3	100%	33.3%
Complaint Closures	2	0%	0%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Race (American Indian or Alaska Native)	Sex (Female)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	3	2	66.7%				
All Investigations	4	4	100%	122	142	16.4%	187
All Complaint Closures	2			365	380	4.1%	388
Merit Decisions (no AJ)	1	1	100%	672	416	-38.1%	462
Dismissal Decisions (no AJ)	0			115	0	-100%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	2							
Total Closures	2							
Settlements	1	50%						
Withdrawals	0	0%						
Total Final Agency Actions	1	50%	1	100%	0	0%	0	0%
Dismissals	0	NA%	0	NA%	0	0%	0	0%
Merit Decisions	1	100%	1	100%	0	0%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	1	100%	1	100%	0	0%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	4	$19,616	$4,904
Complaint Closures with Monetary Benefits	1	$500	$500
ADR Settlements w/ Monetary Benefits	0	$0	$0

Corporation for National and Community Service (CNCS) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	7		0		7	
Settlements	0	0%	0	0%	0	0%
Withdrawals or No Complaints Filed	3	42.9%	0	0%	3	42.9%
Complaints Filed*					4	57.1%
Decision to File Complaint Pending at End of FY					0	0%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	7	0%	0%
Complaint Closures	3	0%	0%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Race (Black or African American)	Reprisal	Sex (Female)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	7	3	42.9%				
All Investigations	6	6	100%	51	109	113.7%	187
All Complaint Closures	3			613	432	-29.5%	388
Merit Decisions (no AJ)	3	0	0%	0	432	NA%	462
Dismissal Decisions (no AJ)	0			0	0	NA%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	5							
Total Closures	3							
Settlements	0	0%						
Withdrawals	0	0%						
Total Final Agency Actions	3	100%	3	100%	0	0%	0	0%
Dismissals	0	NA%	0	NA%	0	0%	0	0%
Merit Decisions	3	100%	3	100%	0	0%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	3	100%	3	100%	0	0%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	6	$27,107	$4,517
Complaint Closures with Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0

Court Services and Offender Supervision Agency for the District of Columbia (CSOSA) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	20		4		24	
Settlements	1	5%	2	50%	3	12.5%
Withdrawals or No Complaints Filed	9	45%	2	50%	11	45.8%
Complaints Filed*					10	41.7%
Decision to File Complaint Pending at End of FY					0	0%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	24	37.5%	16.7%
Complaint Closures	15	0%	0%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Sex (Female)	Disability (Mental)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	24	13	54.2%				
All Investigations	6	4	66.7%	187	165	-11.8%	187
All Complaint Closures	15			343	757	120.7%	388
Merit Decisions (no AJ)	2	2	100%	237	393	65.8%	462
Dismissal Decisions (no AJ)	2			0	85	NA%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	10							
Total Closures	15							
Settlements	5	33.3%						
Withdrawals	1	6.7%						
Total Final Agency Actions	9	60%	4	44.4%	5	55.6%	0	0%
Dismissals	2	22.2%	2	100%	0	0%	0	0%
Merit Decisions	7	77.8%	2	28.6%	5	71.4%	0	0%
Finding Discrimination	1	14.3%	0	0%	1	100%	0	0%
Finding No Discrimination	6	85.7%	2	33.3%	4	66.7%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	6	$22,512	$3,752
Complaint Closures with Monetary Benefits	5	$62,740	$12,548
ADR Settlements w/ Monetary Benefits	0	$0	$0

Defense Commissary Agency (DeCA) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	105		122		227	
Settlements	1	1%	9	7.4%	10	4.4%
Withdrawals or No Complaints Filed	42	40%	33	27.1%	75	33%
Complaints Filed*					138	60.8%
Decision to File Complaint Pending at End of FY					4	1.8%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	227	81.1%	53.7%
Complaint Closures	120	18.3%	15.8%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Sex (Female)	Race (Black or African American)	Reprisal

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	227	198	87.2%				
All Investigations	58	14	24.1%	198	257	29.8%	187
All Complaint Closures	120			250	319	27.6%	388
Merit Decisions (no AJ)	27	26	96.3%	325	349	7.4%	462
Dismissal Decisions (no AJ)	22			25	13	-48%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	140							
Total Closures	120							
Settlements	36	30%						
Withdrawals	17	14.2%						
Total Final Agency Actions	67	55.8%	49	73.1%	18	26.9%	0	0%
Dismissals	22	32.8%	22	100%	0	0%	0	0%
Merit Decisions	45	67.2%	27	60%	18	40%	0	0%
Finding Discrimination	1	2.2%	0	0%	1	100%	0	0%
Finding No Discrimination	44	97.8%	27	61.4%	17	38.6%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	58	$257,328	$4,436
Complaint Closures with Monetary Benefits	19	$818,779	$43,093
ADR Settlements w/ Monetary Benefits	4	$21,887	$5,471

Defense Contract Audit Agency (DCAA) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	40		5		45	
Settlements	0	0%	4	80%	4	8.9%
Withdrawals or No Complaints Filed	9	22.5%	1	20%	10	22.2%
Complaints Filed*					28	62.2%
Decision to File Complaint Pending at End of FY					3	6.7%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	45	15.6%	11.1%
Complaint Closures	32	28.1%	28.1%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Age	Reprisal	Race (Black or African American)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	45	26	57.8%				
All Investigations	12	3	25%	175	264	50.9%	187
All Complaint Closures	32			321	252	-21.5%	388
Merit Decisions (no AJ)	7	5	71.4%	273	358	31.1%	462
Dismissal Decisions (no AJ)	4			0	41	NA%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	28							
Total Closures	32							
Settlements	12	37.5%						
Withdrawals	6	18.8%						
Total Final Agency Actions	14	43.8%	11	78.6%	3	21.4%	0	0%
Dismissals	4	28.6%	4	100%	0	0%	0	0%
Merit Decisions	10	71.4%	7	70%	3	30%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	10	100%	7	70%	3	30%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	12	$53,240	$4,436
Complaint Closures with Monetary Benefits	7	$21,850	$3,121
ADR Settlements w/ Monetary Benefits	6	$21,450	$3,575

Defense Contract Management Agency (DCMA) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	49		36		85	
Settlements	2	4.1%	4	11.1%	6	7.1%
Withdrawals or No Complaints Filed	21	42.9%	15	41.7%	36	42.4%
Complaints Filed*					41	48.2%
Decision to File Complaint Pending at End of FY					2	2.4%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	85	44.7%	42.4%
Complaint Closures	38	18.4%	18.4%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Age	Race (Black or African American)	Sex (Female)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	85	85	100%				
All Investigations	3	0	0%	202	329	62.9%	187
All Complaint Closures	38			446	345	-22.6%	388
Merit Decisions (no AJ)	8	8	100%	708	497	-29.8%	462
Dismissal Decisions (no AJ)	16			54	120	122.2%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	45							
Total Closures	38							
Settlements	9	23.7%						
Withdrawals	5	13.2%						
Total Final Agency Actions	24	63.2%	24	100%	0	0%	0	0%
Dismissals	16	66.7%	16	100%	0	0%	0	0%
Merit Decisions	8	33.3%	8	100%	0	0%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	8	100%	8	100%	0	0%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	2	$11,900	$5,950
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	3	$13,310	$4,436
Complaint Closures with Monetary Benefits	4	$68,239	$17,059
ADR Settlements w/ Monetary Benefits	0	$0	$0

Department of Defense Education Activity (DODEA) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	107		29		136	
Settlements	3	2.8%	7	24.1%	10	7.4%
Withdrawals or No Complaints Filed	43	40.2%	9	31%	52	38.2%
Complaints Filed*					72	52.9%
Decision to File Complaint Pending at End of FY					2	1.5%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	136	38.2%	21.3%
Complaint Closures	55	16.4%	9.1%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Age	Sex (Female)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	136	134	98.5%				
All Investigations	54	50	92.6%	178	176	-1.1%	187
All Complaint Closures	55			287	406	41.5%	388
Merit Decisions (no AJ)	12	7	58.3%	299	386	29.1%	462
Dismissal Decisions (no AJ)	10			91	54	-40.7%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	79							
Total Closures	55							
Settlements	23	41.8%						
Withdrawals	4	7.3%						
Total Final Agency Actions	28	50.9%	22	78.6%	6	21.4%	0	0%
Dismissals	10	35.7%	10	100%	0	0%	0	0%
Merit Decisions	18	64.3%	12	66.7%	6	33.3%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	18	100%	12	66.7%	6	33.3%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	1	$1,380	$1,380
ADR Settlements w/ Monetary Benefits	1	$1,380	$1,380
Investigation Costs	54	$186,303	$3,450
Complaint Closures with Monetary Benefits	17	$390,604	$22,976
ADR Settlements w/ Monetary Benefits	1	$21,804	$21,804

Defense Finance and Accounting Service (DFAS) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	37		55		92	
Settlements	1	2.7%	22	40%	23	25%
Withdrawals or No Complaints Filed	15	40.5%	14	25.5%	29	31.5%
Complaints Filed*					36	39.1%
Decision to File Complaint Pending at End of FY					4	4.4%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	92	77.2%	59.8%
Complaint Closures	39	0%	0%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Disability (Physical)	Age

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	92	92	100%				
All Investigations	20	11	55%	196	245	25%	187
All Complaint Closures	39			262	353	34.7%	388
Merit Decisions (no AJ)	8	8	100%	247	309	25.1%	462
Dismissal Decisions (no AJ)	9			7	12	71.4%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	38							
Total Closures	39							
Settlements	13	33.3%						
Withdrawals	3	7.7%						
Total Final Agency Actions	23	59%	17	73.9%	6	26.1%	0	0%
Dismissals	9	39.1%	9	100%	0	0%	0	0%
Merit Decisions	14	60.9%	8	57.1%	6	42.9%	0	0%
Finding Discrimination	1	7.1%	1	100%	0	0%	0	0%
Finding No Discrimination	13	92.9%	7	53.8%	6	46.2%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	1	$340	$340
ADR Settlements w/ Monetary Benefits	1	$340	$340
Investigation Costs	20	$88,733	$4,436
Complaint Closures with Monetary Benefits	11	$189,976	$17,270
ADR Settlements w/ Monetary Benefits	0	$0	$0

Defense Human Resources Activity (DHRA) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	2		6		8	
Settlements	0	0%	1	16.7%	1	12.5%
Withdrawals or No Complaints Filed	1	50%	3	50%	4	50%
Complaints Filed*					3	37.5%
Decision to File Complaint Pending at End of FY					0	0%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	8	87.5%	75%
Complaint Closures	5	100%	80%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Sex (Male)	Age	Race (Black or African American)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	8	6	75%				
All Investigations	0	0	NA%	284	0	-100%	187
All Complaint Closures	5			507	149	-70.6%	388
Merit Decisions (no AJ)	0	0	0%	507	0	-100%	462
Dismissal Decisions (no AJ)	1			0	32	NA%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	4							
Total Closures	5							
Settlements	1	20%						
Withdrawals	3	60%						
Total Final Agency Actions	1	20%	1	100%	0	0%	0	0%
Dismissals	1	100%	1	100%	0	0%	0	0%
Merit Decisions	0	NA%	0	NA%	0	NA%	0	NA%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	0	NA%	0	NA%	0	NA%	0	NA%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	0	$0	$0
Complaint Closures with Monetary Benefits	1	$20,000	$20,000
ADR Settlements w/ Monetary Benefits	1	$20,000	$20,000

Defense Information Systems Agency (DISA) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	29		1		30	
Settlements	0	0%	0	0%	0	0%
Withdrawals or No Complaints Filed	12	41.4%	1	100%	13	43.3%
Complaints Filed*					17	56.7%
Decision to File Complaint Pending at End of FY					0	0%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	30	100%	3.3%
Complaint Closures	8	0%	0%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Age	Disability (Physical)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	29	29	100%				
All Investigations	4	0	0%	306	261	-14.7%	187
All Complaint Closures	8			680	687	1%	388
Merit Decisions (no AJ)	0	0	0%	696	0	-100%	462
Dismissal Decisions (no AJ)	5			0	996	NA%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	17							
Total Closures	8							
Settlements	2	25%						
Withdrawals	1	12.5%						
Total Final Agency Actions	5	62.5%	5	100%	0	0%	0	0%
Dismissals	5	100%	5	100%	0	0%	0	0%
Merit Decisions	0	NA%	0	NA%	0	NA%	0	NA%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	0	NA%	0	NA%	0	NA%	0	NA%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	4	$28,003	$7,000
Complaint Closures with Monetary Benefits	1	$25,000	$25,000
ADR Settlements w/ Monetary Benefits	0	$0	$0

Defense Office of the Inspector General (DOIG) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	7		2		9	
Settlements	1	14.3%	1	50%	2	22.2%
Withdrawals or No Complaints Filed	0	0%	0	0%	0	0%
Complaints Filed*					6	66.7%
Decision to File Complaint Pending at End of FY					1	11.1%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	9	100%	22.2%
Complaint Closures	3	0%	0%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Race (Black or African American)	Sex (Female)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	9	9	100%				
All Investigations	1	1	100%	208	255	22.6%	187
All Complaint Closures	3			210	469	123.3%	388
Merit Decisions (no AJ)	0	0	0%	296	0	-100%	462
Dismissal Decisions (no AJ)	1			49	8	-83.7%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	6							
Total Closures	3							
Settlements	2	66.7%						
Withdrawals	0	0%						
Total Final Agency Actions	1	33.3%	1	100%	0	0%	0	0%
Dismissals	1	100%	1	100%	0	0%	0	0%
Merit Decisions	0	NA%	0	NA%	0	NA%	0	NA%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	0	NA%	0	NA%	0	NA%	0	NA%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	1	$15,000	$15,000
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	1	$9,895	$9,895
Complaint Closures with Monetary Benefits	2	$97,500	$48,750
ADR Settlements w/ Monetary Benefits	0	$0	$0

Defense Joint Task Force National Capital Region Medical (DJTFNCRM) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	67		17		84	
Settlements	0	0%	6	35.3%	6	7.1%
Withdrawals or No Complaints Filed	43	64.2%	2	11.8%	45	53.6%
Complaints Filed*					33	39.3%
Decision to File Complaint Pending at End of FY					0	0%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	84	100%	20.2%
Complaint Closures	7	85.7%	85.7%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Sex (Female)	Disability (Physical)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	84	53	63.1%				
All Investigations	1	0	0%	0	315	NA%	187
All Complaint Closures	7			0	92	NA%	388
Merit Decisions (no AJ)	0	0	0%	0	0	NA%	462
Dismissal Decisions (no AJ)	5			0	53	NA%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	33							
Total Closures	7							
Settlements	0	0%						
Withdrawals	2	28.6%						
Total Final Agency Actions	5	71.4%	5	100%	0	0%	0	0%
Dismissals	5	100%	5	100%	0	0%	0	0%
Merit Decisions	0	NA%	0	NA%	0	NA%	0	NA%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	0	NA%	0	NA%	0	NA%	0	NA%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	1	$3,025	$3,025
Complaint Closures with Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0

Defense Logistics Agency (DLA) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	121		191		312	
Settlements	2	1.7%	58	30.4%	60	19.2%
Withdrawals or No Complaints Filed	52	43%	80	41.9%	132	42.3%
Complaints Filed*					114	36.5%
Decision to File Complaint Pending at End of FY					6	1.9%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	312	95.2%	61.2%
Complaint Closures	136	25.7%	21.3%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Race (Black or African American)	Age

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	312	276	88.5%				
All Investigations	52	12	23.1%	270	272	0.7%	187
All Complaint Closures	136			458	463	1.1%	388
Merit Decisions (no AJ)	38	3	7.9%	591	494	-16.4%	462
Dismissal Decisions (no AJ)	14			46	82	78.3%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	121							
Total Closures	136							
Settlements	49	36%						
Withdrawals	12	8.8%						
Total Final Agency Actions	75	55.2%	52	69.3%	23	30.7%	0	0%
Dismissals	14	18.7%	14	100%	0	0%	0	0%
Merit Decisions	61	81.3%	38	62.3%	23	37.7%	0	0%
Finding Discrimination	2	3.3%	2	100%	0	0%	0	0%
Finding No Discrimination	59	96.7%	36	61%	23	39%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	5	$9,052	$1,810
ADR Settlements w/ Monetary Benefits	4	$7,334	$1,833
Investigation Costs	52	$464,213	$8,927
Complaint Closures with Monetary Benefits	26	$498,486	$19,172
ADR Settlements w/ Monetary Benefits	5	$106,808	$21,361

Defense Media Activity (DMA) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	3		0		3	
Settlements	0	0%	0	0%	0	0%
Withdrawals or No Complaints Filed	2	66.7%	0	0%	2	66.7%
Complaints Filed*					1	33.3%
Decision to File Complaint Pending at End of FY					0	0%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	3	66.7%	0%
Complaint Closures	3	66.7%	66.7%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Sex (Female)	Age

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	3	3	100%				
All Investigations	0	0	NA%	66	0	-100%	187
All Complaint Closures	3			66	453	586.4%	388
Merit Decisions (no AJ)	0	0	0%	0	0	NA%	462
Dismissal Decisions (no AJ)	0			66	0	-100%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	1							
Total Closures	3							
Settlements	2	66.7%						
Withdrawals	1	33.3%						
Total Final Agency Actions	0	0%	0	NA%	0	NA%	0	NA%
Dismissals	0	NA%	0	NA%	0	0%	0	0%
Merit Decisions	0	NA%	0	NA%	0	NA%	0	NA%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	0	NA%	0	NA%	0	NA%	0	NA%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	0	$0	$0
Complaint Closures with Monetary Benefits	1	$54,000	$54,000
ADR Settlements w/ Monetary Benefits	2	$54,000	$27,000

Defense Missile Defense Agency (DMDA) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	10		1		11	
Settlements	1	10%	0	0%	1	9.1%
Withdrawals or No Complaints Filed	2	20%	1	100%	3	27.3%
Complaints Filed*					4	36.4%
Decision to File Complaint Pending at End of FY					3	27.3%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	11	36.4%	9.1%
Complaint Closures	0	0%	0%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Sex (Female)	Age

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	11	3	27.3%				
All Investigations	1	0	0%	224	237	5.8%	187
All Complaint Closures	0			30	0	-100%	388
Merit Decisions (no AJ)	0	0	0%	0	0	NA%	462
Dismissal Decisions (no AJ)	0			30	0	-100%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	5							
Total Closures	0							
Settlements	0	0%						
Withdrawals	0	0%						
Total Final Agency Actions	0	0%	0	NA%	0	NA%	0	NA%
Dismissals	0	NA%	0	NA%	0	0%	0	0%
Merit Decisions	0	NA%	0	NA%	0	NA%	0	NA%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	0	NA%	0	NA%	0	NA%	0	NA%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	1	$4,437	$4,437
Complaint Closures with Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0

Defense National Guard Bureau (DNGB) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	66		47		113	
Settlements	10	15.2%	37	78.7%	47	41.6%
Withdrawals or No Complaints Filed	28	42.4%	6	12.8%	34	30.1%
Complaints Filed*					26	23%
Decision to File Complaint Pending at End of FY					6	5.3%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	113	73.5%	41.6%
Complaint Closures	33	30.3%	15.2%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Sex (Female)	Age

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	113	97	85.8%				
All Investigations	0	0	NA%	0	0	NA%	187
All Complaint Closures	33			394	327	-17%	388
Merit Decisions (no AJ)	3	0	0%	0	362	NA%	462
Dismissal Decisions (no AJ)	23			0	355	NA%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	26							
Total Closures	33							
Settlements	6	18.2%						
Withdrawals	1	3%						
Total Final Agency Actions	26	78.8%	26	100%	0	0%	0	0%
Dismissals	23	88.5%	23	100%	0	0%	0	0%
Merit Decisions	3	11.5%	3	100%	0	0%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	3	100%	3	100%	0	0%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	0	$0	$0
Complaint Closures with Monetary Benefits	2	$559,011	$279,505
ADR Settlements w/ Monetary Benefits	2	$559,011	$279,505

Defense Office of the Secretary - Wash. Hqtrs. Services (OSD) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	36		9		45	
Settlements	0	0%	2	22.2%	2	4.4%
Withdrawals or No Complaints Filed	16	44.4%	2	22.2%	18	40%
Complaints Filed*					25	55.6%
Decision to File Complaint Pending at End of FY					0	0%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	45	20%	20%
Complaint Closures	45	4.4%	4.4%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Disability (Physical)	Race (Black or African American)	Sex (Female)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	45	45	100%				
All Investigations	19	15	78.9%	253	248	-2%	187
All Complaint Closures	45			464	570	22.8%	388
Merit Decisions (no AJ)	6	0	0%	443	664	49.9%	462
Dismissal Decisions (no AJ)	13			135	245	81.5%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	27							
Total Closures	45							
Settlements	12	26.7%						
Withdrawals	7	15.6%						
Total Final Agency Actions	26	57.8%	19	73.1%	7	26.9%	0	0%
Dismissals	13	50%	13	100%	0	0%	0	0%
Merit Decisions	13	50%	6	46.2%	7	53.8%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	13	100%	6	46.2%	7	53.8%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	19	$172,330	$9,070
Complaint Closures with Monetary Benefits	8	$288,118	$36,014
ADR Settlements w/ Monetary Benefits	1	$40,000	$40,000

Defense Security Service (DSS) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	16		2		18	
Settlements	0	0%	2	100%	2	11.1%
Withdrawals or No Complaints Filed	3	18.8%	0	0%	3	16.7%
Complaints Filed*					8	44.4%
Decision to File Complaint Pending at End of FY					5	27.8%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	18	38.9%	11.1%
Complaint Closures	6	0%	0%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Sex (Female)	Disability (Physical)	Reprisal

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	18	18	100%				
All Investigations	5	0	0%	233	193	-17.2%	187
All Complaint Closures	6			411	167	-59.4%	388
Merit Decisions (no AJ)	3	3	100%	428	200	-53.3%	462
Dismissal Decisions (no AJ)	2			36	100	177.8%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	8							
Total Closures	6							
Settlements	1	16.7%						
Withdrawals	0	0%						
Total Final Agency Actions	5	83.3%	5	100%	0	0%	0	0%
Dismissals	2	40%	2	100%	0	0%	0	0%
Merit Decisions	3	60%	3	100%	0	0%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	3	100%	3	100%	0	0%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	5	$22,185	$4,437
Complaint Closures with Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0

Defense Threat Reduction Agency (DTRA) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	12		7		19	
Settlements	0	0%	3	42.9%	3	15.8%
Withdrawals or No Complaints Filed	4	33.3%	3	42.9%	7	36.8%
Complaints Filed*					9	47.4%
Decision to File Complaint Pending at End of FY					0	0%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	19	100%	36.8%
Complaint Closures	8	0%	0%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Disability (Physical)	Race (Black or African American)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	19	18	94.7%				
All Investigations	0	0	NA%	209	0	-100%	187
All Complaint Closures	8			170	743	337.1%	388
Merit Decisions (no AJ)	0	0	0%	414	0	-100%	462
Dismissal Decisions (no AJ)	4			53	869	1,539.6%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	9							
Total Closures	8							
Settlements	4	50%						
Withdrawals	0	0%						
Total Final Agency Actions	4	50%	4	100%	0	0%	0	0%
Dismissals	4	100%	4	100%	0	0%	0	0%
Merit Decisions	0	NA%	0	NA%	0	NA%	0	NA%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	0	NA%	0	NA%	0	NA%	0	NA%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	1	$2,000	$2,000
ADR Settlements w/ Monetary Benefits	1	$2,000	$2,000
Investigation Costs	0	$0	$0
Complaint Closures with Monetary Benefits	3	$121,000	$40,333
ADR Settlements w/ Monetary Benefits	0	$0	$0

Defense TRICARE Management Activity (DTMA) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	17		1		18	
Settlements	0	0%	0	0%	0	0%
Withdrawals or No Complaints Filed	7	41.2%	1	100%	8	44.4%
Complaints Filed*					10	55.6%
Decision to File Complaint Pending at End of FY					0	0%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	18	83.3%	5.6%
Complaint Closures	7	71.4%	71.4%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Race (Black or African American)	Reprisal	Sex (Female)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	18	7	38.9%				
All Investigations	2	1	50%	0	368	NA%	187
All Complaint Closures	7			221	217	-1.8%	388
Merit Decisions (no AJ)	0	0	0%	0	0	NA%	462
Dismissal Decisions (no AJ)	5			0	108	NA%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	10							
Total Closures	7							
Settlements	1	14.3%						
Withdrawals	1	14.3%						
Total Final Agency Actions	5	71.4%	5	100%	0	0%	0	0%
Dismissals	5	100%	5	100%	0	0%	0	0%
Merit Decisions	0	NA%	0	NA%	0	NA%	0	NA%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	0	NA%	0	NA%	0	NA%	0	NA%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	2	$6,094	$3,047
Complaint Closures with Monetary Benefits	1	$35,000	$35,000
ADR Settlements w/ Monetary Benefits	1	$35,000	$35,000

Defense Uniformed Services University (DUSU) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	5		0		5	
Settlements	0	0%	0	0%	0	0%
Withdrawals or No Complaints Filed	3	60%	0	0%	3	60%
Complaints Filed*					2	40%
Decision to File Complaint Pending at End of FY					0	0%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	5	0%	0%
Complaint Closures	0	0%	0%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Sex (Male)	Age	Disability (Physical)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	5	5	100%				
All Investigations	0	0	NA%	0	0	NA%	187
All Complaint Closures	0			45	0	-100%	388
Merit Decisions (no AJ)	0	0	0%	0	0	NA%	462
Dismissal Decisions (no AJ)	0			0	0	NA%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	2							
Total Closures	0							
Settlements	0	0%						
Withdrawals	0	0%						
Total Final Agency Actions	0	0%	0	NA%	0	NA%	0	NA%
Dismissals	0	NA%	0	NA%	0	0%	0	0%
Merit Decisions	0	NA%	0	NA%	0	NA%	0	NA%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	0	NA%	0	NA%	0	NA%	0	NA%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	0	$0	$0
Complaint Closures with Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0

Department of Education (ED) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	38		10		48	
Settlements	1	2.6%	1	10%	2	4.2%
Withdrawals or No Complaints Filed	8	21.1%	5	50%	13	27.1%
Complaints Filed*					32	66.7%
Decision to File Complaint Pending at End of FY					1	2.1%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	48	89.6%	20.8%
Complaint Closures	46	45.7%	4.4%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Race (Black or African American)	Age

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	48	47	97.9%				
All Investigations	26	26	100%	192	179	-6.8%	187
All Complaint Closures	46			430	566	31.6%	388
Merit Decisions (no AJ)	17	17	100%	385	358	-7%	462
Dismissal Decisions (no AJ)	2			54	92	70.4%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	33							
Total Closures	46							
Settlements	10	21.7%						
Withdrawals	5	10.9%						
Total Final Agency Actions	31	67.4%	19	61.3%	12	38.7%	0	0%
Dismissals	2	6.5%	2	100%	0	0%	0	0%
Merit Decisions	29	93.5%	17	58.6%	12	41.4%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	29	100%	17	58.6%	12	41.4%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	26	$90,427	$3,477
Complaint Closures with Monetary Benefits	6	$36,800	$6,133
ADR Settlements w/ Monetary Benefits	0	$0	$0

Department of Energy (DOE) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	95		29		124	
Settlements	7	7.4%	5	17.2%	12	9.7%
Withdrawals or No Complaints Filed	33	34.7%	4	13.8%	37	29.8%
Complaints Filed*					72	58.1%
Decision to File Complaint Pending at End of FY					3	2.4%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	124	63.7%	23.4%
Complaint Closures	63	55.6%	14.3%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Age	Disability (Physical)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	124	66	53.2%				
All Investigations	51	42	82.4%	DNF	179	NA	187
All Complaint Closures	63			DNF	345	NA	388
Merit Decisions (no AJ)	18	5	27.8%	DNF	372	NA	462
Dismissal Decisions (no AJ)	6			DNF	242	NA	92

*APD =Average Processing Days DNF = Did Not File a FY 2011 report.

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	72							
Total Closures	63							
Settlements	27	42.9%						
Withdrawals	9	14.3%						
Total Final Agency Actions	27	42.9%	24	88.9%	3	11.1%	0	0%
Dismissals	6	22.2%	6	100%	0	0%	0	0%
Merit Decisions	21	77.8%	18	85.7%	3	14.3%	0	0%
Finding Discrimination	2	9.5%	2	100%	0	0%	0	0%
Finding No Discrimination	19	90.5%	16	84.2%	3	15.8%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	1	$5,418	$5,418
ADR Settlements w/ Monetary Benefits	1	$5,418	$5,418
Investigation Costs	51	$133,184	$2,611
Complaint Closures with Monetary Benefits	23	$919,109	$39,961
ADR Settlements w/ Monetary Benefits	4	$94,000	$23,500

Environmental Protection Agency (EPA) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	70		28		98	
Settlements	2	2.9%	2	7.1%	4	4.1%
Withdrawals or No Complaints Filed	17	24.3%	2	7.1%	19	19.4%
Complaints Filed*					70	71.4%
Decision to File Complaint Pending at End of FY					5	5.1%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	98	84.7%	28.6%
Complaint Closures	49	2%	2%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Age	Sex (Female)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	98	68	69.4%				
All Investigations	61	9	14.8%	247	355	43.7%	187
All Complaint Closures	49			697	712	2.2%	388
Merit Decisions (no AJ)	13	0	0%	741	899	21.3%	462
Dismissal Decisions (no AJ)	2			331	229	-30.8%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	78							
Total Closures	49							
Settlements	12	24.5%						
Withdrawals	11	22.5%						
Total Final Agency Actions	26	53.1%	15	57.7%	11	42.3%	0	0%
Dismissals	3	11.5%	2	66.7%	1	33.3%	0	0%
Merit Decisions	23	88.5%	13	56.5%	10	43.5%	0	0%
Finding Discrimination	1	4.4%	1	100%	0	0%	0	0%
Finding No Discrimination	22	95.7%	12	54.5%	10	45.5%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	61	$138,948	$2,277
Complaint Closures with Monetary Benefits	9	$635,892	$70,654
ADR Settlements w/ Monetary Benefits	0	$0	$0

Equal Employment Opportunity Commission (EEOC) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	24		17		41	
Settlements	1	4.2%	1	5.9%	2	4.9%
Withdrawals or No Complaints Filed	12	50%	4	23.5%	16	39%
Complaints Filed*					23	56.1%
Decision to File Complaint Pending at End of FY					0	0%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	41	92.7%	41.5%
Complaint Closures	20	10%	10%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Disability (Mental)	Disability (Physical)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	41	40	97.6%				
All Investigations	13	12	92.3%	150	240	60%	187
All Complaint Closures	20			322	329	2.2%	388
Merit Decisions (no AJ)	5	0	0%	464	530	14.2%	462
Dismissal Decisions (no AJ)	5			96	161	67.7%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	25							
Total Closures	20							
Settlements	6	30%						
Withdrawals	1	5%						
Total Final Agency Actions	13	65%	10	76.9%	3	23.1%	0	0%
Dismissals	5	38.5%	5	100%	0	0%	0	0%
Merit Decisions	8	61.5%	5	62.5%	3	37.5%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	8	100%	5	62.5%	3	37.5%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	13	$84,000	$6,461
Complaint Closures with Monetary Benefits	4	$19,650	$4,912
ADR Settlements w/ Monetary Benefits	1	$8,000	$8,000

Federal Communications Commission (FCC) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	15		0		15	
Settlements	0	0%	0	0%	0	0%
Withdrawals or No Complaints Filed	5	33.3%	0	0%	5	33.3%
Complaints Filed*					10	66.7%
Decision to File Complaint Pending at End of FY					0	0%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	15	0%	0%
Complaint Closures	2	0%	0%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Race (Black or African American)	Sex (Male)	Disability (Mental)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	15	10	66.7%				
All Investigations	10	10	100%	61	39	-36.1%	187
All Complaint Closures	2			30	90	200%	388
Merit Decisions (no AJ)	0	0	0%	0	0	NA%	462
Dismissal Decisions (no AJ)	2			0	90	NA%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	10							
Total Closures	2							
Settlements	0	0%						
Withdrawals	0	0%						
Total Final Agency Actions	2	100%	2	100%	0	0%	0	0%
Dismissals	2	100%	2	100%	0	0%	0	0%
Merit Decisions	0	NA%	0	NA%	0	NA%	0	NA%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	0	NA%	0	NA%	0	NA%	0	NA%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	10	$36,000	$3,600
Complaint Closures with Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0

Federal Deposit Insurance Corporation (FDIC) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	43		39		82	
Settlements	2	4.7%	9	23.1%	11	13.4%
Withdrawals or No Complaints Filed	17	39.5%	6	15.4%	23	28.1%
Complaints Filed*					44	53.7%
Decision to File Complaint Pending at End of FY					4	4.9%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	82	86.6%	47.6%
Complaint Closures	42	40.5%	19.1%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Race (Black or African American)	Age

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	82	80	97.6%				
All Investigations	29	29	100%	207	224	8.2%	187
All Complaint Closures	42			255	291	14.1%	388
Merit Decisions (no AJ)	12	12	100%	450	407	-9.6%	462
Dismissal Decisions (no AJ)	11			44	133	202.3%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	44							
Total Closures	42							
Settlements	14	33.3%						
Withdrawals	2	4.8%						
Total Final Agency Actions	26	61.9%	23	88.5%	3	11.5%	0	0%
Dismissals	12	46.2%	11	91.7%	1	8.3%	0	0%
Merit Decisions	14	53.8%	12	85.7%	2	14.3%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	14	100%	12	85.7%	2	14.3%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	1	$1,750	$1,750
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	29	$165,049	$5,691
Complaint Closures with Monetary Benefits	8	$343,256	$42,907
ADR Settlements w/ Monetary Benefits	2	$25,442	$12,721

Federal Energy Regulatory Commission (FERC) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	13		0		13	
Settlements	0	0%	0	0%	0	0%
Withdrawals or No Complaints Filed	7	53.8%	0	0%	7	53.9%
Complaints Filed*					6	46.2%
Decision to File Complaint Pending at End of FY					0	0%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	13	0%	0%
Complaint Closures	10	30%	30%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Race (Black or African American)	Sex (Female)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	13	13	100%				
All Investigations	6	6	100%	0	180	NA%	187
All Complaint Closures	10			180	152	-15.6%	388
Merit Decisions (no AJ)	6	6	100%	180	200	11.1%	462
Dismissal Decisions (no AJ)	2			180	60	-66.7%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	6							
Total Closures	10							
Settlements	1	10%						
Withdrawals	1	10%						
Total Final Agency Actions	8	80%	8	100%	0	0%	0	0%
Dismissals	2	25%	2	100%	0	0%	0	0%
Merit Decisions	6	75%	6	100%	0	0%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	6	100%	6	100%	0	0%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	6	$21,000	$3,500
Complaint Closures with Monetary Benefits	1	$25,000	$25,000
ADR Settlements w/ Monetary Benefits	1	$25,000	$25,000

Federal Housing Finance Agency (FHFA) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	4		13		17	
Settlements	0	0%	2	15.4%	2	11.8%
Withdrawals or No Complaints Filed	2	50%	4	30.8%	6	35.3%
Complaints Filed*					9	52.9%
Decision to File Complaint Pending at End of FY					0	0%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	17	94.1%	76.5%
Complaint Closures	6	83.3%	33.3%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Race (Black or African American)	Age	Reprisal

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	16	15	93.8%				
All Investigations	3	2	66.7%	0	225	NA%	187
All Complaint Closures	6			565	200	-64.6%	388
Merit Decisions (no AJ)	0	0	0%	865	0	-100%	462
Dismissal Decisions (no AJ)	1			0	170	NA%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	9							
Total Closures	6							
Settlements	5	83.3%						
Withdrawals	0	0%						
Total Final Agency Actions	1	16.7%	1	100%	0	0%	0	0%
Dismissals	1	100%	1	100%	0	0%	0	0%
Merit Decisions	0	NA%	0	NA%	0	NA%	0	NA%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	0	NA%	0	NA%	0	NA%	0	NA%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	1	$11,920	$11,920
ADR Settlements w/ Monetary Benefits	1	$11,920	$11,920
Investigation Costs	3	$14,509	$4,836
Complaint Closures with Monetary Benefits	4	$191,210	$47,802
ADR Settlements w/ Monetary Benefits	2	$181,934	$90,967

Federal Reserve System--Board of Governors (FRSBG) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	53		1		54	
Settlements	0	0%	0	0%	0	0%
Withdrawals or No Complaints Filed	42	79.2%	0	0%	42	77.8%
Complaints Filed*					12	22.2%
Decision to File Complaint Pending at End of FY					0	0%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	54	100%	1.9%
Complaint Closures	6	0%	0%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Age	Race (Black or African American)	Reprisal

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	54	54	100%				
All Investigations	5	5	100%	198	151	-23.7%	187
All Complaint Closures	6			36	310	761.1%	388
Merit Decisions (no AJ)	0	0	0%	0	0	NA%	462
Dismissal Decisions (no AJ)	0			0	0	NA%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	12							
Total Closures	6							
Settlements	2	33.3%						
Withdrawals	3	50%						
Total Final Agency Actions	1	16.7%	0	0%	1	100%	0	0%
Dismissals	0	NA%	0	NA%	0	0%	0	0%
Merit Decisions	1	100%	0	0%	1	100%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	1	100%	0	0%	1	100%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	5	$41,956	$8,391
Complaint Closures with Monetary Benefits	2	$74,512	$37,256
ADR Settlements w/ Monetary Benefits	0	$0	$0

Federal Trade Commission (FTC) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	10		0		10	
Settlements	1	10%	0	0%	1	10%
Withdrawals or No Complaints Filed	9	90%	0	0%	9	90%
Complaints Filed*					0	0%
Decision to File Complaint Pending at End of FY					0	0%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	10	100%	0%
Complaint Closures	1	0%	0%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Race (Asian)	Race (Black or African American)	Race (White)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	10	10	100%				
All Investigations	0	0	NA%	0	0	NA%	187
All Complaint Closures	1			0	1,115	NA%	388
Merit Decisions (no AJ)	0	0	0%	0	0	NA%	462
Dismissal Decisions (no AJ)	0			0	0	NA%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	0							
Total Closures	1							
Settlements	0	0%						
Withdrawals	0	0%						
Total Final Agency Actions	1	100%	0	0%	1	100%	0	0%
Dismissals	0	NA%	0	NA%	0	0%	0	0%
Merit Decisions	1	100%	0	0%	1	100%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	1	100%	0	0%	1	100%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	0	$0	$0
Complaint Closures with Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0

General Services Administration (GSA) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	92		66		158	
Settlements	4	4.3%	5	7.6%	9	5.7%
Withdrawals or No Complaints Filed	28	30.4%	22	33.3%	50	31.7%
Complaints Filed*					92	58.2%
Decision to File Complaint Pending at End of FY					7	4.4%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	158	92.4%	41.8%
Complaint Closures	85	3.5%	2.4%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Age	Race (Black or African American)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	158	156	98.7%				
All Investigations	77	44	57.1%	263	266	1.1%	187
All Complaint Closures	85			411	425	3.4%	388
Merit Decisions (no AJ)	21	15	71.4%	424	398	-6.1%	462
Dismissal Decisions (no AJ)	11			53	43	-18.9%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	96							
Total Closures	85							
Settlements	18	21.2%						
Withdrawals	12	14.1%						
Total Final Agency Actions	55	64.7%	32	58.2%	23	41.8%	0	0%
Dismissals	11	20%	11	100%	0	0%	0	0%
Merit Decisions	44	80%	21	47.7%	23	52.3%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	44	100%	21	47.7%	23	52.3%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	1	$628	$628
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	77	$230,204	$2,989
Complaint Closures with Monetary Benefits	13	$279,370	$21,490
ADR Settlements w/ Monetary Benefits	0	$0	$0

Government Printing Office (GPO) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	70		0		70	
Settlements	0	0%	0	0%	0	0%
Withdrawals or No Complaints Filed	42	60%	0	0%	42	60%
Complaints Filed*					27	38.6%
Decision to File Complaint Pending at End of FY					1	1.4%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	70	100%	0%
Complaint Closures	29	0%	0%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Sex (Female)	Race (Black or African American)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	70	66	94.3%				
All Investigations	26	12	46.2%	214	274	28%	187
All Complaint Closures	29			280	330	17.9%	388
Merit Decisions (no AJ)	11	3	27.3%	355	358	0.8%	462
Dismissal Decisions (no AJ)	5			130	34	-73.8%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	27							
Total Closures	29							
Settlements	10	34.5%						
Withdrawals	1	3.5%						
Total Final Agency Actions	18	62.1%	16	88.9%	2	11.1%	0	0%
Dismissals	5	27.8%	5	100%	0	0%	0	0%
Merit Decisions	13	72.2%	11	84.6%	2	15.4%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	13	100%	11	84.6%	2	15.4%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	26	$79,107	$3,042
Complaint Closures with Monetary Benefits	7	$155,200	$22,171
ADR Settlements w/ Monetary Benefits	0	$0	$0

Department of Health and Human Services (HHS) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	472		202		674	
Settlements	10	2.1%	16	7.9%	26	3.9%
Withdrawals or No Complaints Filed	116	24.6%	52	25.7%	168	24.9%
Complaints Filed*					371	55%
Decision to File Complaint Pending at End of FY					109	16.2%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	674	95.7%	30%
Complaint Closures	409	25.7%	9.8%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Race (Black or African American)	Age

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	674	613	91%				
All Investigations	288	269	93.4%	148	153	3.4%	187
All Complaint Closures	409			309	341	10.4%	388
Merit Decisions (no AJ)	96	54	56.3%	344	404	17.4%	462
Dismissal Decisions (no AJ)	94			82	62	-24.4%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	382							
Total Closures	409							
Settlements	156	38.1%						
Withdrawals	28	6.9%						
Total Final Agency Actions	225	55%	190	84.4%	35	15.6%	0	0%
Dismissals	95	42.2%	94	98.9%	1	1.1%	0	0%
Merit Decisions	130	57.8%	96	73.8%	34	26.2%	0	0%
Finding Discrimination	4	3.1%	2	50%	2	50%	0	0%
Finding No Discrimination	126	96.9%	94	74.6%	32	25.4%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	2	$60,583	$30,291
ADR Settlements w/ Monetary Benefits	1	$7,500	$7,500
Investigation Costs	288	$1,233,362	$4,282
Complaint Closures with Monetary Benefits	115	$2,890,067	$25,131
ADR Settlements w/ Monetary Benefits	10	$111,356	$11,135

Department of Homeland Security (DHS) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	1,095		936		2,031	
Settlements	18	1.6%	137	14.6%	155	7.6%
Withdrawals or No Complaints Filed	378	34.5%	303	32.4%	681	33.5%
Complaints Filed*					1,142	56.2%
Decision to File Complaint Pending at End of FY					53	2.6%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	2,031	80.3%	46.1%
Complaint Closures	1,097	26.5%	5.3%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Age	Sex (Female)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	2,031	1,718	84.6%				
All Investigations	1,046	596	57%	243	230	-5.3%	187
All Complaint Closures	1,097			511	462	-9.6%	388
Merit Decisions (no AJ)	337	163	48.4%	579	494	-14.7%	462
Dismissal Decisions (no AJ)	164			153	128	-16.3%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	1,198							
Total Closures	1,097							
Settlements	244	22.2%						
Withdrawals	118	10.8%						
Total Final Agency Actions	735	67%	501	68.2%	231	31.4%	3	0.4%
Dismissals	180	24.5%	164	91.1%	16	8.9%	0	0%
Merit Decisions	555	75.5%	337	60.7%	215	38.7%	3	0.5%
Finding Discrimination	13	2.3%	1	7.7%	9	69.2%	3	23.1%
Finding No Discrimination	542	97.7%	336	62%	206	38%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	19	$544,996	$28,684
ADR Settlements w/ Monetary Benefits	15	$407,743	$27,182
Investigation Costs	1,046	$4,963,672	$4,745
Complaint Closures with Monetary Benefits	133	$3,032,436	$22,800
ADR Settlements w/ Monetary Benefits	5	$133,750	$26,750

Department of Housing and Urban Development (HUD) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	85		21		106	
Settlements	0	0%	0	0%	0	0%
Withdrawals or No Complaints Filed	29	34.1%	5	23.8%	34	32.1%
Complaints Filed*					63	59.4%
Decision to File Complaint Pending at End of FY					9	8.5%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	106	100%	19.8%
Complaint Closures	73	86.3%	6.9%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Age	Race (Black or African American)	Reprisal

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	106	68	64.2%				
All Investigations	77	26	33.8%	326	285	-12.6%	187
All Complaint Closures	73			398	594	49.2%	388
Merit Decisions (no AJ)	25	2	8%	335	624	86.3%	462
Dismissal Decisions (no AJ)	3			119	394	231.1%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	63							
Total Closures	73							
Settlements	23	31.5%						
Withdrawals	7	9.6%						
Total Final Agency Actions	43	58.9%	28	65.1%	15	34.9%	0	0%
Dismissals	3	7%	3	100%	0	0%	0	0%
Merit Decisions	40	93%	25	62.5%	15	37.5%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	40	100%	25	62.5%	15	37.5%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	77	$201,354	$2,614
Complaint Closures with Monetary Benefits	20	$569,242	$28,462
ADR Settlements w/ Monetary Benefits	3	$96,960	$32,320

Department of the Interior (DOI) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	437		155		592	
Settlements	27	6.2%	32	20.7%	59	10%
Withdrawals or No Complaints Filed	133	30.4%	43	27.7%	176	29.7%
Complaints Filed*					339	57.3%
Decision to File Complaint Pending at End of FY					18	3%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	592	78.4%	26.2%
Complaint Closures	307	63.8%	9.1%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Age	Sex (Female)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	592	473	79.9%				
All Investigations	238	123	51.7%	234	270	15.4%	187
All Complaint Closures	307			493	487	-1.2%	388
Merit Decisions (no AJ)	104	12	11.5%	468	574	22.6%	462
Dismissal Decisions (no AJ)	30			260	148	-43.1%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	352							
Total Closures	307							
Settlements	107	34.9%						
Withdrawals	23	7.5%						
Total Final Agency Actions	177	57.7%	134	75.7%	43	24.3%	0	0%
Dismissals	31	17.5%	30	96.8%	1	3.2%	0	0%
Merit Decisions	146	82.5%	104	71.2%	42	28.8%	0	0%
Finding Discrimination	3	2.1%	2	66.7%	1	33.3%	0	0%
Finding No Discrimination	143	98%	102	71.3%	41	28.7%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	17	$109,994	$6,470
ADR Settlements w/ Monetary Benefits	12	$80,449	$6,704
Investigation Costs	238	$781,905	$3,285
Complaint Closures with Monetary Benefits	75	$1,076,120	$14,348
ADR Settlements w/ Monetary Benefits	6	$96,921	$16,153

John F. Kennedy Center for the Performing Arts (JFKCPA) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	2		0		2	
Settlements	0	0%	0	0%	0	0%
Withdrawals or No Complaints Filed	1	50%	0	0%	1	50%
Complaints Filed*					1	50%
Decision to File Complaint Pending at End of FY					0	0%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	2	100%	0%
Complaint Closures	0	0%	0%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Race (Black or African American)	Sex (Female)	National Origin (Other)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	2	2	100%				
All Investigations	1	1	100%	0	61	NA%	187
All Complaint Closures	0			192	0	-100%	388
Merit Decisions (no AJ)	0	0	0%	375	0	-100%	462
Dismissal Decisions (no AJ)	0			100	0	-100%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	1							
Total Closures	0							
Settlements	0	0%						
Withdrawals	0	0%						
Total Final Agency Actions	0	0%	0	NA%	0	NA%	0	NA%
Dismissals	0	NA%	0	NA%	0	0%	0	0%
Merit Decisions	0	NA%	0	NA%	0	NA%	0	NA%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	0	NA%	0	NA%	0	NA%	0	NA%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	1	$3,974	$3,974
Complaint Closures with Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0

Department of Justice (DOJ) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	1,130		242		1,372	
Settlements	28	2.5%	54	22.3%	82	6%
Withdrawals or No Complaints Filed	475	42%	58	24%	533	38.9%
Complaints Filed*					737	53.7%
Decision to File Complaint Pending at End of FY					20	1.5%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	1,372	84.8%	17.6%
Complaint Closures	857	13.7%	6.5%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Sex (Female)	Age

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	1,372	1,242	90.5%				
All Investigations	614	483	78.7%	196	202	3.1%	187
All Complaint Closures	857			727	592	-18.6%	388
Merit Decisions (no AJ)	362	28	7.7%	960	776	-19.2%	462
Dismissal Decisions (no AJ)	110			163	136	-16.6%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	761							
Total Closures	857							
Settlements	148	17.3%						
Withdrawals	93	10.9%						
Total Final Agency Actions	616	71.9%	472	76.6%	140	22.7%	4	0.6%
Dismissals	110	17.9%	110	100%	0	0%	0	0%
Merit Decisions	506	82.1%	362	71.5%	140	27.7%	4	0.8%
Finding Discrimination	17	3.4%	10	58.8%	4	23.5%	3	17.6%
Finding No Discrimination	489	96.6%	352	72%	136	27.8%	1	0.2%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	22	$315,868	$14,357
ADR Settlements w/ Monetary Benefits	13	$267,535	$20,579
Investigation Costs	614	$2,575,296	$4,194
Complaint Closures with Monetary Benefits	107	$2,210,345	$20,657
ADR Settlements w/ Monetary Benefits	15	$96,052	$6,403

Department of Labor (DOL) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	102		104		206	
Settlements	0	0%	12	11.5%	12	5.8%
Withdrawals or No Complaints Filed	37	36.3%	15	14.4%	52	25.2%
Complaints Filed*					133	64.6%
Decision to File Complaint Pending at End of FY					9	4.4%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	206	100%	50.5%
Complaint Closures	134	100%	36.6%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Age	Race (Black or African American)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	206	193	93.7%				
All Investigations	85	83	97.6%	195	204	4.6%	187
All Complaint Closures	134			359	505	40.7%	388
Merit Decisions (no AJ)	44	38	86.4%	309	357	15.5%	462
Dismissal Decisions (no AJ)	11			187	86	-54%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	133							
Total Closures	134							
Settlements	49	36.6%						
Withdrawals	10	7.5%						
Total Final Agency Actions	75	56%	55	73.3%	20	26.7%	0	0%
Dismissals	19	25.3%	11	57.9%	8	42.1%	0	0%
Merit Decisions	56	74.7%	44	78.6%	12	21.4%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	56	100%	44	78.6%	12	21.4%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	2	$23,500	$11,750
ADR Settlements w/ Monetary Benefits	2	$23,500	$11,750
Investigation Costs	85	$262,000	$3,082
Complaint Closures with Monetary Benefits	35	$535,712	$15,306
ADR Settlements w/ Monetary Benefits	35	$495,812	$14,166

National Aeronautics and Space Administration (NASA) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	56		21		77	
Settlements	2	3.6%	6	28.6%	8	10.4%
Withdrawals or No Complaints Filed	23	41.1%	7	33.3%	30	39%
Complaints Filed*					37	48.1%
Decision to File Complaint Pending at End of FY					2	2.6%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	77	42.9%	27.3%
Complaint Closures	38	21.1%	7.9%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Race (Black or African American)	Sex (Female)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	77	61	79.2%				
All Investigations	21	17	81%	174	194	11.5%	187
All Complaint Closures	38			427	565	32.3%	388
Merit Decisions (no AJ)	11	0	0%	626	516	-17.6%	462
Dismissal Decisions (no AJ)	9			263	99	-62.4%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	39							
Total Closures	38							
Settlements	7	18.4%						
Withdrawals	1	2.6%						
Total Final Agency Actions	30	79%	20	66.7%	10	33.3%	0	0%
Dismissals	9	30%	9	100%	0	0%	0	0%
Merit Decisions	21	70%	11	52.4%	10	47.6%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	21	100%	11	52.4%	10	47.6%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	4	$44,000	$11,000
ADR Settlements w/ Monetary Benefits	3	$19,000	$6,333
Investigation Costs	21	$91,245	$4,345
Complaint Closures with Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0

National Archives and Records Administration (NARA) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	23		10		33	
Settlements	6	26.1%	7	70%	13	39.4%
Withdrawals or No Complaints Filed	14	60.9%	2	20%	16	48.5%
Complaints Filed*					3	9.1%
Decision to File Complaint Pending at End of FY					1	3%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	33	72.7%	30.3%
Complaint Closures	11	0%	0%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Race (Black or African American)	Religion

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	33	30	90.9%				
All Investigations	3	3	100%	168	170	1.2%	187
All Complaint Closures	11			486	685	40.9%	388
Merit Decisions (no AJ)	3	3	100%	574	636	10.8%	462
Dismissal Decisions (no AJ)	2			69	64	-7.2%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	4							
Total Closures	11							
Settlements	3	27.3%						
Withdrawals	0	0%						
Total Final Agency Actions	8	72.7%	5	62.5%	3	37.5%	0	0%
Dismissals	2	25%	2	100%	0	0%	0	0%
Merit Decisions	6	75%	3	50%	3	50%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	6	100%	3	50%	3	50%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	1	$1,650	$1,650
ADR Settlements w/ Monetary Benefits	1	$1,650	$1,650
Investigation Costs	3	$11,477	$3,825
Complaint Closures with Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0

National Credit Union Administration (NCUA) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	7		0		7	
Settlements	0	0%	0	0%	0	0%
Withdrawals or No Complaints Filed	4	57.1%	0	0%	4	57.1%
Complaints Filed*					3	42.9%
Decision to File Complaint Pending at End of FY					0	0%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	7	100%	0%
Complaint Closures	7	0%	0%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Age	Reprisal	Sex (Male)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	7	7	100%				
All Investigations	3	2	66.7%	191	217	13.6%	187
All Complaint Closures	7			240	425	77.1%	388
Merit Decisions (no AJ)	1	0	0%	0	541	NA%	462
Dismissal Decisions (no AJ)	0			0	0	NA%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	3							
Total Closures	7							
Settlements	6	85.7%						
Withdrawals	0	0%						
Total Final Agency Actions	1	14.3%	1	100%	0	0%	0	0%
Dismissals	0	NA%	0	NA%	0	0%	0	0%
Merit Decisions	1	100%	1	100%	0	0%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	1	100%	1	100%	0	0%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	3	$15,830	$5,276
Complaint Closures with Monetary Benefits	5	$209,777	$41,955
ADR Settlements w/ Monetary Benefits	0	$0	$0

National Gallery of Art (NGA) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	3		0		3	
Settlements	0	0%	0	0%	0	0%
Withdrawals or No Complaints Filed	1	33.3%	0	0%	1	33.3%
Complaints Filed*					2	66.7%
Decision to File Complaint Pending at End of FY					0	0%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	3	100%	0%
Complaint Closures	6	0%	0%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Race (Black or African American)	Religion	Reprisal

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	3	3	100%				
All Investigations	0	0	NA%	315	0	-100%	187
All Complaint Closures	6			493	817	65.7%	388
Merit Decisions (no AJ)	3	0	0%	510	761	49.2%	462
Dismissal Decisions (no AJ)	1			32	21	-34.4%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	2							
Total Closures	6							
Settlements	2	33.3%						
Withdrawals	0	0%						
Total Final Agency Actions	4	66.7%	4	100%	0	0%	0	0%
Dismissals	1	25%	1	100%	0	0%	0	0%
Merit Decisions	3	75%	3	100%	0	0%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	3	100%	3	100%	0	0%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	0	$0	$0
Complaint Closures with Monetary Benefits	2	$28,000	$14,000
ADR Settlements w/ Monetary Benefits	0	$0	$0

National Labor Relations Board (NLRB) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	17		2		19	
Settlements	1	5.9%	0	0%	1	5.3%
Withdrawals or No Complaints Filed	8	47.1%	1	50%	9	47.4%
Complaints Filed*					8	42.1%
Decision to File Complaint Pending at End of FY					1	5.3%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	19	94.7%	10.5%
Complaint Closures	8	100%	12.5%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Race (Black or African American)	Reprisal	Sex (Male)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	19	15	79%				
All Investigations	3	3	100%	235	167	-28.9%	187
All Complaint Closures	8			276	289	4.7%	388
Merit Decisions (no AJ)	2	2	100%	270	234	-13.3%	462
Dismissal Decisions (no AJ)	1			18	22	22.2%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	9							
Total Closures	8							
Settlements	3	37.5%						
Withdrawals	1	12.5%						
Total Final Agency Actions	4	50%	3	75%	1	25%	0	0%
Dismissals	1	25%	1	100%	0	0%	0	0%
Merit Decisions	3	75%	2	66.7%	1	33.3%	0	0%
Finding Discrimination	1	33.3%	1	100%	0	0%	0	0%
Finding No Discrimination	2	66.7%	1	50%	1	50%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	3	$29,953	$9,984
Complaint Closures with Monetary Benefits	3	$51,985	$17,328
ADR Settlements w/ Monetary Benefits	0	$0	$0

National Science Foundation (NSF) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	8		7		15	
Settlements	0	0%	2	28.6%	2	13.3%
Withdrawals or No Complaints Filed	4	50%	0	0%	4	26.7%
Complaints Filed*					9	60%
Decision to File Complaint Pending at End of FY					0	0%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	15	86.7%	46.7%
Complaint Closures	6	33.3%	33.3%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Age	Race (Black or African American)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	15	14	93.3%				
All Investigations	4	0	0%	195	372	90.8%	187
All Complaint Closures	6			631	364	-42.3%	388
Merit Decisions (no AJ)	0	0	0%	486	0	-100%	462
Dismissal Decisions (no AJ)	0			0	0	NA%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	11							
Total Closures	6							
Settlements	6	100%						
Withdrawals	0	0%						
Total Final Agency Actions	0	0%	0	NA%	0	NA%	0	NA%
Dismissals	0	NA%	0	NA%	0	0%	0	0%
Merit Decisions	0	NA%	0	NA%	0	NA%	0	NA%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	0	NA%	0	NA%	0	NA%	0	NA%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	4	$11,940	$2,985
Complaint Closures with Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0

Department of the Navy (NAVY) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	757		774		1,531	
Settlements	25	3.3%	203	26.2%	228	14.9%
Withdrawals or No Complaints Filed	332	43.9%	262	33.9%	594	38.8%
Complaints Filed*					696	45.5%
Decision to File Complaint Pending at End of FY					13	0.9%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	1,531	99.7%	50.6%
Complaint Closures	904	3.2%	2.2%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Age	Race (Black or African American)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	1,530	1,394	91.1%				
All Investigations	409	162	39.6%	263	277	5.3%	187
All Complaint Closures	904			365	332	-9%	388
Merit Decisions (no AJ)	117	117	100%	503	477	-5.2%	462
Dismissal Decisions (no AJ)	147			66	57	-13.6%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	696							
Total Closures	904							
Settlements	423	46.8%						
Withdrawals	141	15.6%						
Total Final Agency Actions	340	37.6%	264	77.6%	75	22.1%	1	0.3%
Dismissals	147	43.2%	147	100%	0	0%	0	0%
Merit Decisions	193	56.8%	117	60.6%	75	38.9%	1	0.5%
Finding Discrimination	8	4.2%	0	0%	7	87.5%	1	12.5%
Finding No Discrimination	185	95.9%	117	63.2%	68	36.8%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	25	$161,418	$6,456
ADR Settlements w/ Monetary Benefits	16	$40,654	$2,540
Investigation Costs	409	$3,715,910	$9,085
Complaint Closures with Monetary Benefits	303	$3,900,925	$12,874
ADR Settlements w/ Monetary Benefits	1	$1,500	$1,500

Nuclear Regulatory Commission (NRC) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	26		9		35	
Settlements	4	15.4%	5	55.6%	9	25.7%
Withdrawals or No Complaints Filed	9	34.6%	1	11.1%	10	28.6%
Complaints Filed*					16	45.7%
Decision to File Complaint Pending at End of FY					0	0%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	35	100%	25.7%
Complaint Closures	16	100%	6.3%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Age	Race (Black or African American)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	35	33	94.3%				
All Investigations	9	7	77.8%	199	209	5%	187
All Complaint Closures	16			172	298	73.3%	388
Merit Decisions (no AJ)	0	0	0%	282	0	-100%	462
Dismissal Decisions (no AJ)	0			66	0	-100%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	16							
Total Closures	16							
Settlements	11	68.8%						
Withdrawals	4	25%						
Total Final Agency Actions	1	6.3%	0	0%	1	100%	0	0%
Dismissals	0	NA%	0	NA%	0	0%	0	0%
Merit Decisions	1	100%	0	0%	1	100%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	1	100%	0	0%	1	100%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	4	$29,500	$7,375
ADR Settlements w/ Monetary Benefits	2	$9,500	$4,750
Investigation Costs	9	$45,000	$5,000
Complaint Closures with Monetary Benefits	7	$197,411	$28,201
ADR Settlements w/ Monetary Benefits	1	$3,700	$3,700

Office of Personnel Management (OPM) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	79		9		88	
Settlements	0	0%	1	11.1%	1	1.1%
Withdrawals or No Complaints Filed	30	38%	8	88.9%	38	43.2%
Complaints Filed*					44	50%
Decision to File Complaint Pending at End of FY					5	5.7%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	88	90.9%	10.2%
Complaint Closures	28	0%	0%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Age	Reprisal	Race (Black or African American)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	88	87	98.9%				
All Investigations	25	25	100%	102	103	1%	187
All Complaint Closures	28			353	505	43.1%	388
Merit Decisions (no AJ)	8	0	0%	360	1,128	213.3%	462
Dismissal Decisions (no AJ)	6			44	131	197.7%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	44							
Total Closures	28							
Settlements	3	10.7%						
Withdrawals	6	21.4%						
Total Final Agency Actions	19	67.9%	14	73.7%	5	26.3%	0	0%
Dismissals	6	31.6%	6	100%	0	0%	0	0%
Merit Decisions	13	68.4%	8	61.5%	5	38.5%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	13	100%	8	61.5%	5	38.5%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	1	$11,000	$11,000
ADR Settlements w/ Monetary Benefits	1	$11,000	$11,000
Investigation Costs	25	$191,010	$7,640
Complaint Closures with Monetary Benefits	3	$44,000	$14,666
ADR Settlements w/ Monetary Benefits	0	$0	$0

Peace Corps (PC) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	5		1		6	
Settlements	0	0%	0	0%	0	0%
Withdrawals or No Complaints Filed	2	40%	0	0%	2	33.3%
Complaints Filed*					4	66.7%
Decision to File Complaint Pending at End of FY					0	0%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	6	100%	16.7%
Complaint Closures	4	100%	0%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Age	National Origin (Other)	Race (Asian)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	6	6	100%				
All Investigations	4	4	100%	234	157	-32.9%	187
All Complaint Closures	4			463	509	9.9%	388
Merit Decisions (no AJ)	3	1	33.3%	454	367	-19.2%	462
Dismissal Decisions (no AJ)	0			0	0	NA%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	4							
Total Closures	4							
Settlements	0	0%						
Withdrawals	0	0%						
Total Final Agency Actions	4	100%	3	75%	1	25%	0	0%
Dismissals	1	25%	0	0%	1	100%	0	0%
Merit Decisions	3	75%	3	100%	0	0%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	3	100%	3	100%	0	0%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	4	$16,786	$4,196
Complaint Closures with Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0

Pension Benefit Guaranty Corporation (PBGC) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	19		1		20	
Settlements	0	0%	0	0%	0	0%
Withdrawals or No Complaints Filed	8	42.1%	0	0%	8	40%
Complaints Filed*					12	60%
Decision to File Complaint Pending at End of FY					0	0%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	20	100%	5%
Complaint Closures	20	65%	0%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Race (Black or African American)	Age

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	20	13	65%				
All Investigations	7	6	85.7%	202	194	-4%	187
All Complaint Closures	20			216	437	102.3%	388
Merit Decisions (no AJ)	5	5	100%	110	362	229.1%	462
Dismissal Decisions (no AJ)	6			51	34	-33.3%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	13							
Total Closures	20							
Settlements	1	5%						
Withdrawals	2	10%						
Total Final Agency Actions	17	85%	11	64.7%	5	29.4%	1	5.9%
Dismissals	6	35.3%	6	100%	0	0%	0	0%
Merit Decisions	11	64.7%	5	45.5%	5	45.5%	1	9.1%
Finding Discrimination	2	18.2%	1	50%	0	0%	1	50%
Finding No Discrimination	9	81.8%	4	44.4%	5	55.6%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	7	$18,000	$2,571
Complaint Closures with Monetary Benefits	2	$12,567	$6,283
ADR Settlements w/ Monetary Benefits	0	$0	$0

Railroad Retirement Board (RRB) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	4		2		6	
Settlements	0	0%	1	50%	1	16.7%
Withdrawals or No Complaints Filed	2	50%	1	50%	3	50%
Complaints Filed*					2	33.3%
Decision to File Complaint Pending at End of FY					0	0%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	6	66.7%	33.3%
Complaint Closures	1	0%	0%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Sex (Female)	Age	Race (Black or African American)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	6	6	100%				
All Investigations	4	4	100%	164	178	8.5%	187
All Complaint Closures	1			390	660	69.2%	388
Merit Decisions (no AJ)	0	0	0%	210	0	-100%	462
Dismissal Decisions (no AJ)	0			0	0	NA%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	2							
Total Closures	1							
Settlements	1	100%						
Withdrawals	0	0%						
Total Final Agency Actions	0	0%	0	NA%	0	NA%	0	NA%
Dismissals	0	NA%	0	NA%	0	0%	0	0%
Merit Decisions	0	NA%	0	NA%	0	NA%	0	NA%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	0	NA%	0	NA%	0	NA%	0	NA%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	4	$8,090	$2,022
Complaint Closures with Monetary Benefits	1	$3,500	$3,500
ADR Settlements w/ Monetary Benefits	0	$0	$0

Securities and Exchange Commission (SEC) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	26		4		30	
Settlements	0	0%	0	0%	0	0%
Withdrawals or No Complaints Filed	10	38.5%	0	0%	10	33.3%
Complaints Filed*					20	66.7%
Decision to File Complaint Pending at End of FY					0	0%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	30	53.3%	13.3%
Complaint Closures	4	0%	0%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Age	Disability (Physical)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	30	25	83.3%				
All Investigations	10	8	80%	175	260	48.6%	187
All Complaint Closures	4			228	308	35.1%	388
Merit Decisions (no AJ)	2	1	50%	374	334	-10.7%	462
Dismissal Decisions (no AJ)	1			42	66	57.1%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	20							
Total Closures	4							
Settlements	0	0%						
Withdrawals	0	0%						
Total Final Agency Actions	4	100%	3	75%	1	25%	0	0%
Dismissals	2	50%	1	50%	1	50%	0	0%
Merit Decisions	2	50%	2	100%	0	0%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	2	100%	2	100%	0	0%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	10	$36,258	$3,625
Complaint Closures with Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0

Small Business Administration (SBA) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	67		8		75	
Settlements	1	1.5%	3	37.5%	4	5.3%
Withdrawals or No Complaints Filed	32	47.8%	2	25%	34	45.3%
Complaints Filed*					35	46.7%
Decision to File Complaint Pending at End of FY					2	2.7%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	75	10.7%	10.7%
Complaint Closures	38	2.6%	2.6%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Age	Sex (Female)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	75	50	66.7%				
All Investigations	33	30	90.9%	202	204	1%	187
All Complaint Closures	38			257	313	21.8%	388
Merit Decisions (no AJ)	7	6	85.7%	140	329	135%	462
Dismissal Decisions (no AJ)	14			25	21	-16%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	36							
Total Closures	38							
Settlements	11	29%						
Withdrawals	1	2.6%						
Total Final Agency Actions	26	68.4%	21	80.8%	5	19.2%	0	0%
Dismissals	14	53.8%	14	100%	0	0%	0	0%
Merit Decisions	12	46.2%	7	58.3%	5	41.7%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	12	100%	7	58.3%	5	41.7%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	1	$9,788	$9,788
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	33	$111,641	$3,383
Complaint Closures with Monetary Benefits	6	$190,200	$31,700
ADR Settlements w/ Monetary Benefits	0	$0	$0

Smithsonian Institution (SI) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	5		33		38	
Settlements	0	0%	1	3%	1	2.6%
Withdrawals or No Complaints Filed	0	0%	10	30.3%	10	26.3%
Complaints Filed*					11	29%
Decision to File Complaint Pending at End of FY					16	42.1%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	38	100%	86.8%
Complaint Closures	15	93.3%	46.7%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Race (Black or African American)	Reprisal	Age

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	38	38	100%				
All Investigations	8	8	100%	160	174	8.8%	187
All Complaint Closures	15			200	500	150%	388
Merit Decisions (no AJ)	5	5	100%	246	213	-13.4%	462
Dismissal Decisions (no AJ)	4			64	38	-40.6%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	13							
Total Closures	15							
Settlements	3	20%						
Withdrawals	0	0%						
Total Final Agency Actions	12	80%	9	75%	3	25%	0	0%
Dismissals	4	33.3%	4	100%	0	0%	0	0%
Merit Decisions	8	66.7%	5	62.5%	3	37.5%	0	0%
Finding Discrimination	0	NA%	0	NA%	0	NA%	0	NA%
Finding No Discrimination	8	100%	5	62.5%	3	37.5%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	1	$618	$618
ADR Settlements w/ Monetary Benefits	1	$618	$618
Investigation Costs	8	$19,250	$2,406
Complaint Closures with Monetary Benefits	3	$255,260	$85,086
ADR Settlements w/ Monetary Benefits	0	$0	$0

Social Security Administration (SSA) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	511		406		917	
Settlements	15	2.9%	62	15.3%	77	8.4%
Withdrawals or No Complaints Filed	282	55.2%	61	15%	343	37.4%
Complaints Filed*					474	51.7%
Decision to File Complaint Pending at End of FY					23	2.5%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	917	85.7%	44.3%
Complaint Closures	414	81.6%	8.7%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Age	Disability (Physical)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	916	871	95.1%				
All Investigations	339	279	82.3%	190	195	2.6%	187
All Complaint Closures	414			418	506	21.1%	388
Merit Decisions (no AJ)	136	36	26.5%	392	460	17.3%	462
Dismissal Decisions (no AJ)	49			41	58	41.5%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	494							
Total Closures	414							
Settlements	50	12.1%						
Withdrawals	54	13%						
Total Final Agency Actions	310	74.9%	185	59.7%	117	37.7%	8	2.6%
Dismissals	58	18.7%	49	84.5%	9	15.5%	0	0%
Merit Decisions	252	81.3%	136	54%	108	42.9%	8	3.2%
Finding Discrimination	12	4.8%	0	0%	4	33.3%	8	66.7%
Finding No Discrimination	240	95.2%	136	56.7%	104	43.3%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	2	$28,500	$14,250
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	339	$1,520,762	$4,486
Complaint Closures with Monetary Benefits	26	$959,990	$36,922
ADR Settlements w/ Monetary Benefits	0	$0	$0

Department of State (STATE) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	206		65		271	
Settlements	8	3.9%	10	15.4%	18	6.6%
Withdrawals or No Complaints Filed	103	50%	16	24.6%	119	43.9%
Complaints Filed*					126	46.5%
Decision to File Complaint Pending at End of FY					8	3%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	271	67.9%	24%
Complaint Closures	110	13.6%	13.6%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Age	Race (Black or African American)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	270	199	73.7%				
All Investigations	97	52	53.6%	271	245	-9.6%	187
All Complaint Closures	110			466	413	-11.4%	388
Merit Decisions (no AJ)	40	1	2.5%	424	461	8.7%	462
Dismissal Decisions (no AJ)	16			81	24	-70.4%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	134							
Total Closures	110							
Settlements	27	24.6%						
Withdrawals	13	11.8%						
Total Final Agency Actions	70	63.6%	56	80%	13	18.6%	1	1.4%
Dismissals	16	22.9%	16	100%	0	0%	0	0%
Merit Decisions	54	77.1%	40	74.1%	13	24.1%	1	1.9%
Finding Discrimination	3	5.6%	0	0%	2	66.7%	1	33.3%
Finding No Discrimination	51	94.4%	40	78.4%	11	21.6%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	0	$0	$0
ADR Settlements w/ Monetary Benefits	0	$0	$0
Investigation Costs	97	$284,655	$2,934
Complaint Closures with Monetary Benefits	15	$573,865	$38,257
ADR Settlements w/ Monetary Benefits	5	$252,704	$50,540

Tennessee Valley Authority (TVA) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	66		20		86	
Settlements	7	10.6%	1	5%	8	9.3%
Withdrawals or No Complaints Filed	9	13.6%	0	0%	9	10.5%
Complaints Filed*					58	67.4%
Decision to File Complaint Pending at End of FY					11	12.8%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	86	90.7%	23.3%
Complaint Closures	58	100%	0%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Age	Reprisal	Race (Black or African American)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	86	85	98.8%				
All Investigations	44	44	100%	124	138	11.3%	187
All Complaint Closures	58			329	330	0.3%	388
Merit Decisions (no AJ)	20	20	100%	321	236	-26.5%	462
Dismissal Decisions (no AJ)	5			9	17	88.9%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	58							
Total Closures	58							
Settlements	12	20.7%						
Withdrawals	7	12.1%						
Total Final Agency Actions	39	67.2%	25	64.1%	14	35.9%	0	0%
Dismissals	5	12.8%	5	100%	0	0%	0	0%
Merit Decisions	34	87.2%	20	58.8%	14	41.2%	0	0%
Finding Discrimination	1	2.9%	1	100%	0	0%	0	0%
Finding No Discrimination	33	97.1%	19	57.6%	14	42.4%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	6	$94,279	$15,713
ADR Settlements w/ Monetary Benefits	1	$2,368	$2,368
Investigation Costs	44	$83,258	$1,892
Complaint Closures with Monetary Benefits	12	$184,580	$15,381
ADR Settlements w/ Monetary Benefits	0	$0	$0

Department of Transportation (DOT) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	299		242		541	
Settlements	9	3%	54	22.3%	63	11.7%
Withdrawals or No Complaints Filed	102	34.1%	71	29.3%	173	32%
Complaints Filed*					292	54%
Decision to File Complaint Pending at End of FY					13	2.4%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	541	67.7%	44.7%
Complaint Closures	335	2.1%	2.1%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Race (Black or African American)	Age

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	541	506	93.5%				
All Investigations	216	214	99.1%	146	136	-6.8%	187
All Complaint Closures	335			321	411	28%	388
Merit Decisions (no AJ)	89	47	52.8%	305	414	35.7%	462
Dismissal Decisions (no AJ)	85			42	122	190.5%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	315							
Total Closures	335							
Settlements	93	27.8%						
Withdrawals	13	3.9%						
Total Final Agency Actions	229	68.4%	174	76%	55	24%	0	0%
Dismissals	87	38%	85	97.7%	2	2.3%	0	0%
Merit Decisions	142	62%	89	62.7%	53	37.3%	0	0%
Finding Discrimination	3	2.1%	0	0%	3	100%	0	0%
Finding No Discrimination	139	97.9%	89	64%	50	36%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	4	$9,950	$2,487
ADR Settlements w/ Monetary Benefits	4	$9,950	$2,487
Investigation Costs	216	$1,376,310	$6,371
Complaint Closures with Monetary Benefits	68	$936,044	$13,765
ADR Settlements w/ Monetary Benefits	1	$21,552	$21,552

Department of the Treasury (TREAS) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	317		429		746	
Settlements	14	4.4%	138	32.2%	152	20.4%
Withdrawals or No Complaints Filed	110	34.7%	104	24.2%	214	28.7%
Complaints Filed*					367	49.2%
Decision to File Complaint Pending at End of FY					13	1.7%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	746	97.5%	57.5%
Complaint Closures	407	81.1%	10.1%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Disability (Physical)	Race (Black or African American)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	746	721	96.7%				
All Investigations	285	248	87%	170	198	16.5%	187
All Complaint Closures	407			475	468	-1.5%	388
Merit Decisions (no AJ)	123	108	87.8%	405	355	-12.3%	462
Dismissal Decisions (no AJ)	44			125	130	4%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	406							
Total Closures	407							
Settlements	96	23.6%						
Withdrawals	34	8.4%						
Total Final Agency Actions	277	68.1%	167	60.3%	110	39.7%	0	0%
Dismissals	51	18.4%	44	86.3%	7	13.7%	0	0%
Merit Decisions	226	81.6%	123	54.4%	103	45.6%	0	0%
Finding Discrimination	6	2.7%	5	83.3%	1	16.7%	0	0%
Finding No Discrimination	220	97.4%	118	53.6%	102	46.4%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	10	$65,250	$6,525
ADR Settlements w/ Monetary Benefits	9	$60,250	$6,694
Investigation Costs	285	$2,229,613	$7,823
Complaint Closures with Monetary Benefits	61	$792,477	$12,991
ADR Settlements w/ Monetary Benefits	3	$41,087	$13,695

U.S. Postal Service (USPS) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	3,963		9,180		13,143	
Settlements	120	3%	3,119	34%	3,239	24.6%
Withdrawals or No Complaints Filed	1,577	39.8%	3,786	41.2%	5,363	40.8%
Complaints Filed*					4,324	32.9%
Decision to File Complaint Pending at End of FY					217	1.7%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	13,143	92.5%	69.9%
Complaint Closures	4,579	8.2%	7%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Age	Disability (Physical)

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	13,121	12,906	98.4%				
All Investigations	2,660	2,636	99.1%	110	113	2.7%	187
All Complaint Closures	4,579			249	275	10.4%	388
Merit Decisions (no AJ)	1,088	1,062	97.6%	263	277	5.3%	462
Dismissal Decisions (no AJ)	1,570			43	48	11.6%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	4,532							
Total Closures	4,579							
Settlements	815	17.8%						
Withdrawals	240	5.2%						
Total Final Agency Actions	3,524	77%	2,658	75.4%	863	24.5%	3	0.1%
Dismissals	1,588	45.1%	1,570	98.9%	18	1.1%	0	0%
Merit Decisions	1,936	54.9%	1,088	56.2%	845	43.6%	3	0.2%
Finding Discrimination	50	2.6%	0	0%	47	94%	3	6%
Finding No Discrimination	1,886	97.4%	1,088	57.7%	798	42.3%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	455	$558,750	$1,228
ADR Settlements w/ Monetary Benefits	425	$491,996	$1,157
Investigation Costs	2,660	$4,395,336	$1,652
Complaint Closures with Monetary Benefits	663	$6,195,246	$9,344
ADR Settlements w/ Monetary Benefits	158	$114,964	$727

Department of Veterans Affairs (VA) FY 2012 EEO Complaint Processing Statistics

Outcome of Counselings Completed in FY 2012

Pre-Complaint Counseling Outcomes	Completed by EEO Counselor		Completed Using ADR		All Completed Counselings	
	#	%	#	%	#	%
Pre-Complaint Counselings	1,904		2,580		4,484	
Settlements	34	1.8%	319	12.4%	353	7.9%
Withdrawals or No Complaints Filed	845	44.4%	886	34.3%	1,731	38.6%
Complaints Filed*					2,280	50.9%
Decision to File Complaint Pending at End of FY					120	2.7%

*Includes only complaints filed in FY 2012 where counseling was also completed during FY 2012.

Agency Use of ADR for EEO Dispute Resolution in FY 2012

	Total Number	Offer Rate	Participation Rate
Pre-Complaint Counselings	4,484	98.5%	57.5%
Complaint Closures	2,123	4.5%	4.5%

Bases Most Frequently Alleged in FY 2012 Filed Complaints

	Top Basis 1	Top Basis 2	Top Basis 3
Bases of Alleged Discrimination	Reprisal	Race (Black or African American)	Age

Timeliness in FY 2012

	Total #	# Timely	% Timely	FY 2011 APD*	FY 2012 APD*	% Change	Govt Wide APD*
All Pre-Complaint Counselings (minus remands)	4,484	4,407	98.3%				
All Investigations	1,583	1,391	87.9%	180	165	-8.3%	187
All Complaint Closures	2,123			373	394	5.6%	388
Merit Decisions (no AJ)	597	30	5%	434	464	6.9%	462
Dismissal Decisions (no AJ)	392			68	88	29.4%	92

*APD =Average Processing Days

Outcomes of Complaints in FY 2012

	Complaint Closures		Final Agency Decision (no AJ Decision)		Final Order (AJ Decision Fully Implemented)		Final Order (AJ Decision Not Fully Implemented)	
	#	%	#	%	#	%	#	%
Total Complaints Filed	2,347							
Total Closures	2,123							
Settlements	520	24.5%						
Withdrawals	224	10.6%						
Total Final Agency Actions	1,379	65%	989	71.7%	387	28.1%	3	0.2%
Dismissals	406	29.4%	392	96.6%	14	3.5%	0	0%
Merit Decisions	973	70.6%	597	61.4%	373	38.3%	3	0.3%
Finding Discrimination	42	4.3%	16	38.1%	23	54.8%	3	7.1%
Finding No Discrimination	931	95.7%	581	62.4%	350	37.6%	0	0%

Costs Associated With EEO Process in FY 2012

	Total #	Total Amount	Average Amount
Pre-Complaint Settlements w/ Monetary Benefits	48	$485,766	$10,120
ADR Settlements w/ Monetary Benefits	44	$474,631	$10,787
Investigation Costs	1,583	$9,137,264	$5,772
Complaint Closures with Monetary Benefits	308	$8,717,951	$28,305
ADR Settlements w/ Monetary Benefits	41	$802,936	$19,583

APPENDIX I

APPENDIX I

GLOSSARY / DEFINITIONS

Administrative Support Workers - See "Occupational Categories."

Affirmation Rate – The percentage of appeal closures that were affirmed by the EEOC.

ADR Closures – The number of counselings or complaints that completed the ADR process during the fiscal year.

ADR Offer Rate - The percentage of completed/ended counselings or the complaint closures that received an ADR offer.

ADR Participation Rate - The percentage of completed/ended counseling or the complaint closures where both parties agreed to participate in ADR.

ADR Resolution Rate - The percentage of ADR closures that were resolved by either settlement or withdrawal from the EEO process.

Agency – Military departments as defined in Section 102 of Title 5, U.S. Code and executive agencies as defined in Section 105 of Tile 5, U.S. Code, the United States Postal Service, the Postal Regulatory Commission, the Tennessee Valley Authority, those units of the legislative and judicial branches of the Federal government having positions in the competitive service, the National Oceanic and Atmospheric Administration Commissioned Corps, the Government Printing Office and the Smithsonian Institution (including those with employees and applicants for employment who are paid from non-appropriated funds).

Annual Reports - Reports required to be submitted to EEOC on agencies' affirmative employment program accomplishments pursuant to EEOC Management Directive 715.

Appeal Closures – The number of appeals decided by the EEOC during the fiscal year.

Appeal Receipts – The number of appeals filed with the EEOC during the fiscal year.

Appeals Inventory – The number of appeals on hand at the end of the fiscal year.

Average Age of Open Pending Inventory – Average number of days of all complaints, hearings or appeals which are not yet resolved at the end of the reporting period.

Average Processing Time – The total number of days divided by the number of investigations, complaint closures, hearing closures, or appeal closures.

Central Personnel Data File (CPDF) - This is a computer data file created and maintained by the OPM. The file is based on personnel action information submitted directly to the OPM by Executive Branch federal agency appointing offices, and is updated monthly. Some Executive Branch agencies do not submit data to the CPDF including the following: the Tennessee Valley Authority, United States Postal Service, Army & Air Force Exchange Service, Central Intelligence Agency, Defense Intelligence Agency, National Geospatial-Intelligence Agency, and the National Security Agency.

Civilian Labor Force (CLF) - Data derived from the decennial census reflecting persons, 16 years of age or older who were employed or seeking employment, excluding those in the Armed Services. CLF data used in this report is based on the 2000 Census.

Complainants – Individuals, either employees or applicants, who filed a formal complaint against a federal agency during the fiscal year.

Complaint Closures – The number of complaints that were completed in the formal complaint process during the fiscal year.

Complainant Rate – The percentage of individuals who filed a complaint per the total work force.

Complaints Filed – The number of complaints that were filed against the federal government during the fiscal year.

Completed/Ended Counselings – The number of counselings which were concluded/closed, either by a written settlement agreement, a written withdrawal from the counseling process, the issuance of a notice of right to file a formal complaint, the forwarding of a counseling to an Administrative Judge when requested/ordered by the Administrative Judge, or the filing of a complaint after the regulatory counseling period has expired even though not all counseling duties have been performed during the fiscal year.

Counseling Rate – The percentage of individuals who completed counseling per the total work force.

Counselings Initiated – The number of new counselings that began during the current fiscal year.

Craft Workers - See "Occupational Categories."

Data from 2000 Census Special EEO File - Data derived from the 2000 decennial census (www.census.gov/eeo2000/).

Decision to File Complaint Pending – The number of completed counselings in which (1) the agency did not receive a complaint, and (2) the 15-day period for filing a complaint had not expired at the end of the fiscal year.

Disability - A physical or mental impairment that substantially limits one or more major life activities.

Dismissals – An agency's final action on a complaint of discrimination which meets the criteria set forth in 29 C.F.R. § 1614.107(a).

EEOC Form 462 Report – The document in which federal agencies report their discrimination complaint process statistics by October 31st of each year.

Federal Wage System Positions - Positions OPM classifies as those whose primary duty involves the performance of physical work which requires a knowledge or experience of a trade, craft, or manual-labor work.

Final Agency Actions – An agency's final action on a complaint of discrimination, which includes a final agency decision, a final order implementing an EEOC Administrative Judge's decision or a final determination on a breach of settlement agreement claim.

General Schedule Positions - Positions OPM classifies as those whose primary duty requires knowledge or experience of an administrative, clerical, scientific, artistic, or technical nature.

Hearing Closures – The number of hearings decided by EEOC Administrative Judges during the fiscal year.

Hearing Requests – The number of hearings requested by complainants during the fiscal year.

Hearings Inventory – The number of hearing requests on hand at the end of the fiscal year.

Investigations – The number of agency reviews or inquiries into claims of discrimination raised in an EEO complaint, resulting in a report of investigation.

Laborers and Helpers - See "Occupational Categories."

Lump Sum Payment - A single payment made in a settlement which does not identify the portion of the amount paid for back pay, compensatory damages, attorney fees, etc.

Major Occupations – Agency occupations that are mission related and heavily populated relative to other occupations within the agency.

Merit Decisions – Decisions that determine whether or not discrimination was proven. (issued by either a federal agency or an EEOC administrative judge).

MD-110 - EEO Management Directive 110 provides policies, procedures and guidance relating to the processing of employment discrimination complaints governed by the Commission's regulations in 29 CFR Part 1614.

MD-715 – EEO Management Directive 715 describes program responsibilities and reporting requirements relating to agencies' EEO programs.

MD-715 Report – The document which agencies use to annually report the status of its activities undertaken pursuant to its EEO program under Title VII of the Civil Rights Act of 1964 and its activities undertaken pursuant to its affirmative action obligations under the Rehabilitation Act of 1973.

Monetary Benefits – A payment that an agency agreed to provide in a settlement agreement, a final agency decision finding discrimination, a final order agreeing to fully implement an EEOC Administrative Judge's decision containing a payment award, or in compliance with an Office of Federal Operations' appellate decision which ordered a payment award.

No Complaint Filed – Occurs when: (1) agency issues a Notice of Right to File Letter and does not receive a formal complaint within 15 days; or (2) the individual notifies the agency in writing that s/he is withdrawing from counseling.

Occupational Categories - The occupational categories for the EEO-9 are as follows:

> **Administrative Support Workers** - Includes all clerical-type work regardless of level of difficulty, where the activities are predominantly non-manual though some manual work not directly involved with altering or transporting the products is included. Includes: bookkeepers, collectors (bills and accounts), messengers and office helpers, office machine operators (including computer), shipping and receiving clerks, stenographers, typists and secretaries, telegraph and telephone operators, legal assistants, and kindred workers.
>
> **Craft Workers** - Manual workers of relatively high skill level having a thorough and comprehensive knowledge of the processes involved in their work. Exercise considerable independent judgment and usually receive an extensive period of training. Includes: the building trades, hourly paid supervisors and lead operators who are not members of management, mechanics and repairers, skilled machining occupations, compositors and typesetters, electricians, engravers, painters (construction and maintenance), motion picture projectionists, pattern and model makers, stationary engineers, tailors, arts occupations, hand painters, coaters, bakers, decorating occupations, and kindred workers.

Laborers and Helpers - Workers in manual occupations which generally require no special training who perform elementary duties that may be learned in a few days and require the application of little or no independent judgment. Includes: garage laborers, car washers and greasers, grounds keepers and gardeners, farm workers, stevedores, wood choppers, laborers performing lifting, digging, mixing, loading and pulling operations, and kindred workers.

Officials and Managers - Occupations requiring administrative and managerial personnel who set broad policies, exercise overall responsibility for execution of these policies, and direct individual offices, programs, divisions or other units or special phases of an agency's operations. In the federal sector, this category is further broken down into four sub-categories: (1) Executive/Senior Level - includes those at the GS-15 grade or in the career Senior Executive Service, (2) Mid-Level - includes those at the GS-13 or 14 grade, (3) First-Level - includes those at or below the GS-12 grade and (4) Other - includes employees in a number of different occupations which are primarily business, financial and administrative in nature, and do not have supervisory or significant policy responsibilities, such as Administrative Officers.

Operatives - Workers who operate machine or processing equipment or perform other factory-type duties of intermediate skill level which can be mastered in a few weeks and require only limited training. Includes: apprentices (auto mechanics, plumbers, bricklayers, carpenters, electricians, machinists, mechanics, building trades, printing trades, etc.), operatives, attendants (auto service and parking), blasters, chauffeurs, delivery workers, sewers and stitchers, dryers, furnace workers, heaters, laundry and dry cleaning operatives, milliners, mine operatives and laborers, motor operators, oilers and greasers (except auto), painters (manufactured articles), photographic process workers, truck and tractor drivers, knitting, looping, taping and weaving machine operators, welders and flame cutters, electrical and electronic equipment assemblers, butchers and meat cutters, inspectors, testers and graders, hand packers and packagers, and kindred workers.

Professionals - Occupations requiring either college graduation or experience of such kind and amount as to provide a comparable background.

Technicians - Occupations requiring a combination of basic scientific knowledge and manual skill which can be obtained through two years of post high school education, such as is offered in many technical institutes and junior colleges, or through equivalent on-the-job training.

Sales - Occupations engaging wholly or primarily in direct selling.

Service Workers - Workers in both protective and non-protective service occupations.

Officials and Managers - See "Occupational Categories."

Operatives - See "Occupational Categories."

Other Pay System Positions – Those positions in alternative pay plans based on performance, like pay-banding, and market-based pay systems that are not easily converted to General Schedule and Related.

Outreach - Presentations and participation in meetings, conferences and seminars with employee and employer groups, professional associations, students, non-profit entities, community organizations and other members of the general public to provide general information about the EEOC, its mission, the employment discrimination laws enforced by EEOC and the complaint process.

Participation Rate - The extent to which members of a specific demographic group are represented in an agency's work force.

Permanent Work Force - Full-time, part-time and intermittent employees of a particular agency. For purposes of this Report, those persons employed as of September 30, 2011.

Professionals - See "Occupational Categories."

Race/Ethnicity -

American Indian or Alaska Native - All persons having origins in any of the original peoples of North and South America (including Central America), and who maintain cultural identification through tribal affiliation or community recognition.

Asian - All persons having origins in any of the original peoples of the Far East, Southeast Asia, the Indian subcontinent including, for example, Cambodia, China, India, Japan, Korea, Malaysia, Pakistan, the Philippine Islands, Thailand, and Vietnam.

Black or African American (Not of Hispanic Origin) - All persons having origins in any of the Black racial groups of Africa.

Hispanic or Latino - All persons of Cuban, Mexican, Puerto Rican, South or Central American, or other Spanish culture or origin, regardless of race.

Native Hawaiian or Other Pacific Islander – All persons having origins in any of the original peoples of Hawaii, Guam, Samoa, or other Pacific Islands.

White (Not of Hispanic Origin) - All persons having origins in any of the original peoples of Europe, the Middle East, or North Africa.

Persons of Two or More Races – All persons who identify with two or more of the above race categories.

Reportable Disability - Any self-identified disability reported by an employee to the employing agency.

Sales Workers - See "Occupational Categories."

Second Level Reporting Component - A subordinate component of a Federal agency which has 1,000 or more employees and which is required to file EEOC FORM 715-01 with the EEOC. While many Federal agencies have subordinate components, not every subordinate component is a Second Level Reporting Component for purposes of filing EEOC FORM 715-01. A list of Federal agencies and departments covered by MD-715 and Second Level

Reporting Components is posted on the EEOC's website at: Department or Agency List with Second Level Reporting Components.

Senior Pay Level Positions - Positions which include the career Senior Executive Service, Executive Schedule, Senior Foreign Service, and other employees earning salaries above grade 15 in the General Schedule in leadership positions.

Service workers - See "Occupational Categories."

Settlements – Where an agency agrees to award monetary or non-monetary benefits to an individual who agreed either to not file a formal complaint or to withdraw a formal complaint.

Targeted Disabilities - Those disabilities that the federal government, as a matter of policy, has identified for special emphasis. The targeted disabilities (and the codes that represent them on the Office of Personnel Management's Standard Form 256) are: hearing 18 (previously deafness (16 and 17)); vision 21 (previously blindness (23 and 25)); missing extremities 30 (previously 28 and 32 through 38); partial paralysis 69 (previously 64 through 68); complete paralysis 79 (previously 71 through 78); epilepsy 82 (previously convulsive disorders (82)); severe intellectual disability 90 (previously mental retardation (90)); psychiatric disability 91 (previously mental illness (91)); and dwarfism 92 (previously distortion of limb and/or spine (92))."

Technicians - See "Occupational Categories."

Temporary Work Force –Employees in positions established for a limited period of time, usually for less than a year.

Training – The process of educating managers and employees on the laws enforced by EEOC and how to prevent and correct discrimination in the workplace and educating EEO professionals in carrying out the agency's equal opportunity responsibilities.

Total Work Force - All employees of an agency subject to 29 C.F.R. Part 1614 regulations, including temporary, seasonal and permanent employees. Total Work Force numbers in Part I, Sections A-D are as reported in the OPM's CPDF. Total Work Force numbers in Part I, Section E are as reported by agencies in their EEO Form 462 Reports.

Withdrawals – An election to end the EEO process during the formal complaint stage.

APPENDIX II

APPENDIX II

FEDERAL SECTOR EEO COMPLAINT PROCESSING PROCEDURES

A. Contact EEO Counselor

Aggrieved persons who believe they have been discriminated against must contact an agency EEO counselor prior to filing a formal complaint. The person must initiate counselor contact within 45 days of the matter alleged to be discriminatory. 29 C.F.R. Section 1614.105(a)(1). This time limit shall be extended where the aggrieved person shows that: he or she was not notified of the time limits and was not otherwise aware of them; he or she did not and reasonably should not have known that the discriminatory matter occurred; despite due diligence he or she was prevented by circumstances beyond his or her control from contacting the counselor within the time limits. 29 C.F.R. Section 1614.105(a)(2).

B. EEO Counseling

EEO counselors provide information to the aggrieved individual concerning how the federal sector EEO process works, including time frames and appeal procedures, and attempt to informally resolve the matter. At the initial counseling session, counselors must advise individuals in writing of their rights and responsibilities in the EEO process, including the right to request a hearing before an EEOC Administrative Judge or an immediate final decision from the agency following its investigation of the complaint. Individuals must be informed of their right to elect between pursuing the matter in the EEO process under part 1614 and a grievance procedure (where available) or the Merit Systems Protection Board appeal process (where applicable). The counselor must also inform the individuals of their right to proceed directly to court in a lawsuit under the Age Discrimination in Employment Act, of their duty to mitigate damages, and that only claims raised in pre-complaint counseling or claims like or related to those raised in counseling may be alleged in a subsequent complaint filed with the agency. 29 C.F.R. Section 1614.105(b)(1).

Counseling must be completed within 30 days of the date the aggrieved person contacted the agency's EEO office to request counseling. If the matter is not resolved in that time period, the counselor must inform the individual in writing of the right to file a discrimination complaint. This notice ("Notice of Final Interview") must inform the individual that a complaint must be filed within 15 days of receipt of the notice, identify the agency official with whom the complaint must be filed, and of the individual's duty to inform the agency if he or she is represented. 29 C.F.R. Section 1614.105(d). The 30-day counseling period may be extended for an additional 60 days: (1) where the individual agrees to such extension in writing; or (2) where the aggrieved person chooses to participate in an ADR procedure. If the claim is not resolved before the 90th

day, the Notice of Final Interview described above must be issued to the individual. 29 C.F.R. Section 1614.105(e), (f). When a complaint is filed, the EEO counselor must submit a written report to the agency's EEO office concerning the issues discussed and the actions taken during counseling. 29 C.F.R. Section 1614.105(c).

C. Alternative Dispute Resolution (ADR)

Beginning January 1, 2000, all agencies were required to establish or make available an ADR program. Such program must be available for both the pre-complaint process and the formal complaint process. 29 C.F.R. Section 1614.102(b)(2). At the initial counseling session, counselors must advise individuals that, where an agency agrees to offer ADR in a particular case, the individual may choose between participation in the ADR program and EEO counseling. 29 C.F.R. Section 1614.105(b)(2). As noted above, if the matter is not resolved in the ADR process within 90 days of the date the individual contacted the agency's EEO office, a Notice of Final Interview must be issued to the individual giving him or her the right to proceed with a formal complaint.

D. Complaints

A complaint must be filed with the agency that allegedly discriminated against the complainant within 15 days of receipt of the Notice of Final Interview. The complaint must be a signed statement from the complainant or the complainant's attorney, containing the complainant's (or representative's) telephone number and address, and must be sufficiently precise to identify the complainant and the agency, and describe generally the action or practice which forms the basis of the complaint. 29 C.F.R. Section 1614.106.

A complainant may amend a complaint at any time prior to the conclusion of the investigation to include issues or claims like or related to those raised in the complaint. After requesting a hearing, a complainant may file a motion with the AJ to amend a complaint to include issues or claims like or related to those raised in the complaint. 29 C.F.R. Section 1614.106(d).

The agency must acknowledge receipt of the complaint in writing and inform the complainant of the date on which the complaint was filed, of the address of the EEOC office where a request for a hearing should be sent, that the complainant has the right to appeal the agency's final action or dismissal of a complaint, and that the agency must investigate the complaint within 180 days of the filing date. The agency's acknowledgment must also advise the complainant that when a complaint has been amended, the agency must complete the investigation within the earlier of: (1) 180 days after the last amendment to the complaint; or (2) 360 days after the filing of the original complaint. A complainant may request a hearing from an EEOC AJ on the

consolidated complaints any time after 180 days from the date of the first filed complaint. 29 C.F.R. Section 1614.106(e).

E. Dismissals of Complaints

Prior to a request for a hearing, in lieu of accepting a complaint for investigation, an agency may dismiss an entire complaint for any of the following reasons: (1) failure to state a claim, or stating the same claim that is pending or has been decided by the agency or the EEOC; (2) failure to comply with the time limits; (3) filing a complaint on a matter that has not been brought to the attention of an EEO counselor and which is not like or related to the matters counseled; (4) filing a complaint which is the basis of a pending civil action, or which was the basis of a civil action already decided by a court; (5) where the complainant has already elected to pursue the matter through either the negotiated grievance procedure or in an appeal to the Merit Systems Protection Board; (6) where the matter is moot or merely alleges a proposal to take a personnel action, unless the complaint alleges the proposal or preliminary step is retaliatory; (7) where the complainant cannot be located; (8) where the complainant fails to respond to a request to provide relevant information; (9) where the complaint alleges dissatisfaction with the processing of a previously filed complaint; (10) where the complaint is part of a clear pattern of misuse of the EEO process for a purpose other than the prevention and elimination of employment discrimination. 29 C.F.R. Section 1614.107.

If an agency believes that some, but not all, of the claims in a complaint should be dismissed for the above reasons, it must notify the complainant in writing of the rationale for this determination, identify the allegations which will not be investigated, and place a copy of this notice in the investigative file. This determination shall be reviewable by an EEOC AJ if a hearing is requested on the remainder of the complaint, but is not appealable until final action is taken by the agency on the remainder of the complaint. 29 C.F.R. Section 1614.107(b).

F. Investigations

Investigations are conducted by the respondent agency. The agency must develop an impartial and appropriate factual record upon which to make findings on the claims raised by the complaint. An appropriate factual record is defined in the regulations as one that allows a reasonable fact finder to draw conclusions as to whether discrimination occurred. 29 C.F.R. Section 1614.108(b).

The investigation must be completed within 180 days from the filing of the complaint.[21] A copy of the investigative file must be provided to the complainant, along with a notification that, within 30 days of receipt of the file, the complainant has the right to request a hearing and a decision from an EEOC AJ or may request an immediate final decision from the agency. 29 C.F.R. Section 1614.108(f). Where an agency is unable to complete the investigation within the prescribed timeframes, it must issue a written notice to complainant informing that the investigation is not complete, an estimated time it believes the investigation will be complete and explain that complainant may request a hearing or file a civil action in an appropriate US District Court if s/he does not wish to wait for the agency to complete its investigation. 29 C.F.R. Section 1614.108(g)

An agency may make an offer of resolution to a complainant who is represented by an attorney at any time after the filing of a complaint, but not later than the date an AJ is appointed to conduct a hearing. An agency may make an offer of resolution to a complaint, represented by an attorney or not, after the parties have received notice than an administrative judge has been appointed to conduct a hearing, but not later than 30 days prior to a hearing.

Such offer of resolution must be in writing and include a notice explaining the possible consequences of failing to accept the offer. If the complainant fails to accept the offer within 30 days of receipt, and the relief awarded in the final decision on the complaint is not more favorable than the offer, then the complainant shall not receive payment from the agency of attorney's fees or costs incurred after the expiration of the 30-day acceptance period. 29 C.F.R. Section 1614.109(c).

G. Hearings

Requests for a hearing must be sent by the complainant to the EEOC office indicated in the agency's acknowledgment letter, with a copy to the agency's EEO office. Within 15 days of receipt of the request for a hearing, the agency must provide a copy of the complaint file to EEOC. The EEOC will then appoint an AJ to conduct a hearing. 29 C.F.R. Section 1614.108(h).

Prior to the hearing, the parties may conduct discovery. The purpose of discovery is to enable a party to obtain relevant information for preparation of the party's case. Each party initially bears their own costs for discovery. For a more

[21]The 180-day statutory period for investigating complaints can be extended to no more than 360 days if the consolidation of two or more complaints occurs. See 29 C.F.R. § 1614.606.

detailed description of discovery procedures, see EEOC Management Directive 110, Chapter 6.

Agencies provide for the attendance of all employees approved as witnesses by the AJ. Hearings are considered part of the investigative process, and are closed to the public. The AJ conducts the hearing and receives relevant information or documents as evidence. The hearing is recorded and the agency is responsible for paying for the transcripts of the hearing. Rules of evidence are not strictly applied to the proceedings. If the AJ determines that some or all facts are not in genuine dispute, he or she may limit the scope of the hearing or issue a summary judgment.

An EEOC AJ may dismiss a complaint for any of the reasons set out above under Dismissals or the AJ must conduct the hearing and issue a decision on the complaint within 180 days of receipt by the AJ of the complaint file from the agency. 29 C.F.R. Section 1614.109(b). The AJ will send copies of the hearing record, the transcript and the decision to the parties. If an agency does not issue a final order within 40 days of receipt of the AJ's decision, then the decision becomes the final action by the agency in the matter. 29 C.F.R. Section 1614.109(i).

H. Final Action by Agencies

When an AJ issues a decision (either a dismissal, a summary judgment decision or a decision following a hearing), the agency must take final action on the complaint by issuing a final order within 40 days of receipt of the hearing file and the AJ's decision. The final order must notify the complainant whether or not the agency will fully implement the decision of the AJ, and shall contain notice of the complainant's right to appeal to EEOC or to file a civil action. If the final order does not fully implement the decision of the AJ, the agency must simultaneously file an appeal with EEOC and attach a copy of the appeal to the final order. 29 C.F.R. Section 1614.110(a).

When an AJ does not issue a decision (i.e., when an agency dismisses an entire complaint under 1614.107, receives a request for an immediate final decision, or does not receive a reply to the notice providing the complainant the right to either request a hearing or an immediate final decision), the agency must take final action by issuing a final decision. The agency's final decision will consist of findings by the agency on the merits of each issue in the complaint. Where the agency has not processed certain allegations in the complaint for procedural reasons set out in 29 C.F.R. Section 1614.107, it must provide the rationale for its decision not to process the allegations. The agency's decision must be issued within 60 days of receiving notification that the complainant has requested an immediate final decision. The agency's decision must contain notice of the complainant's right to appeal to the EEOC, or to file a civil action in federal court. 29 C.F.R. Section 1614.110(b).

I. Appeals to the EEOC

Several types of appeals may be brought to the EEOC. A complainant may appeal an agency's final action or dismissal of a complaint within 30 days of receipt. 29 C.F.R. Sections 1614.401(a), 1614.402(a). A complainant may also appeal to the EEOC for a determination as to whether the agency has complied with the terms of a settlement agreement or decision. 29 C.F.R. Section 1614.504(b). A grievant may appeal the final decision of the agency, arbitrator or the FLRA on a grievance when an issue of employment discrimination was raised in the grievance procedure. 29 C.F.R. Section 1614.401(d). If the agency's final action and order do not fully implement the AJ's decision, the agency must appeal to the EEOC. 29 C.F.R. Section 1614.110(a); 29 C.F.R. Section 1614.401(b).

If the complaint is a class action, the class agent or the agency may appeal an AJ's decision accepting or dismissing all or part of the class complaint. A class agent may appeal an agency's final action or the agency may appeal the AJ's decision on a class complaint. A class member may appeal a final decision on an individual claim for relief pursuant to a finding of class-wide discrimination. Finally, either the class agent or the agency may appeal from an AJ decision on the adequacy of a proposed settlement of a class action. 29 C.F.R. Section 1614.401(c).

Appeals must be filed with EEOC's Office of Federal Operations (OFO). Any statement or brief on behalf of a complainant in support of an appeal must be submitted to OFO within 30 days of filing the notice of appeal. Any statement or brief on behalf of the agency in support of its appeal must be filed within 20 days of filing the notice of appeal. An agency must submit the complaint file to OFO within 30 days of initial notification that the complainant has filed an appeal or within 30 days of submission of an appeal by the agency. Any statement or brief in opposition to an appeal must be submitted to OFO and served on the opposing party within 30 days of receipt of the statement or brief supporting the appeal, or, if no statement or brief supporting the appeal has been filed, within 60 days of receipt of the appeal. 29 C.F.R. Section 1614.403. Federal agencies must submit all case related documentation to EEOC in an acceptable digital format and complainants are encouraged to do so. 29 C.F.R. Section 1614.403(g). EEOC has the authority to draw adverse inferences against a party failing to comply with its appeal procedures or requests for information. 29 C.F.R. Section 1614.404(c). The decision on an appeal from an agency's final action is based on a *de novo* review, except that the review of the factual findings in a decision by an AJ following a hearing is based on a substantial evidence standard of review. 29 C.F.R. Section 1614.405(a).

A party may request that EEOC reconsider its decision within 30 days of receipt of the Commission's decision. Such requests are not a second appeal, and will be granted only when the previous EEOC decision involved a clearly erroneous

interpretation of material fact or law; or when the decision will have a substantial impact on the policies, practices or operations of the agency. 29 C.F.R. Section 1614.405(b). The EEOC's decision will be based on a preponderance of the evidence. The decision will also inform the complainant of his or her right to file a civil action.

J. Civil Actions

Prior to filing a civil action under Title VII of the Civil Rights Act of 1964 or the Rehabilitation Act of 1973, a federal sector complainant must first exhaust the administrative process set out at 29 C.F.R. Part 1614. "Exhaustion," for the purposes of filing a civil action, may occur at different stages of the process. The regulations provide that civil actions may be filed in an appropriate federal court: (1) within 90 days of receipt of the final action where no administrative appeal has been filed; (2) after 180 days from the date of filing a complaint if an administrative appeal has not been filed and final action has not been taken; (3) within 90 days of receipt of EEOC's final decision on an appeal; or (4) after 180 days from the filing of an appeal with EEOC if there has been no final decision by the EEOC. 29 C.F.R. Section 1614.407.

Under the Age Discrimination in Employment Act (ADEA), an individual may proceed directly to federal court after giving the EEOC notice of intent to sue. 29 C.F.R. Section 1614.201. An ADEA complainant who initiates the administrative process in 29 C.F.R. Part 1614 may also file a civil action within the time frames noted above. 29 C.F.R. Section 1614.407.

Under the Equal Pay Act, an individual may file a civil action within 2 years (3 years for willful violations), regardless of whether he or she has pursued an administrative complaint. 29 C.F.R. Section 1614.408. Filing a civil action terminates EEOC processing of an appeal. 29 C.F.R. Section 1614.409.

K. Class Complaints

Class complaints of discrimination are processed differently from individual complaints. See 29 C.F.R. Section 1614.204. The employee or applicant who wishes to file a class complaint must first seek counseling and be counseled, just like an individual complaint. However, once counseling is completed the class complaint is not investigated by the respondent agency. Rather, the complaint is forwarded to the nearest EEOC Field or District Office, where an EEOC AJ is appointed to make a decision as to whether to accept or dismiss the class complaint. The AJ examines the class to determine whether it meets the class certification requirements of numerosity, commonality, typicality and adequacy of representation. The AJ may issue a decision dismissing the class because it fails to meet any of these class certification requirements, as well as for any of the reasons for dismissal discussed above for individual complaints.

A class complaint may begin as an individual complaint of discrimination. At a certain point, it may become evident that there are many more individuals than the complainant affected by the issues raised in the individual complaint. EEOC's regulations provide that a complainant may move for class certification at any reasonable point in the process when it becomes apparent that there are class implications to the claims raised in an individual complaint. 29 C.F.R. Section 1614.204(b).

The AJ transmits his or her decision to accept or dismiss a class complaint to the class agent and the agency. The agency must then take final action by issuing a final order within 60 days of receipt of the AJ's decision. The final order must notify the agent whether or not the agency will implement the decision of the AJ. If the agency's final order does not implement the AJ's decision, the agency must simultaneously appeal the AJ's decision to EEOC's OFO. A copy of the agency's appeal must be appended to the agency's final order. 29 C.F.R. Section 1614.204(d)(7).

A dismissal of a class complaint shall inform the class agent either that the complaint is being filed on that date as an individual complaint and processed accordingly, or that the complaint is also dismissed as an individual complaint for one of the reasons for dismissal (discussed in section E, above). In addition, a dismissal must inform the class agent of the right to appeal to EEOC's OFO or to file a civil action in federal court.

When a class complaint is accepted, the agency must use reasonable means to notify the class members of the acceptance of the class complaint, a description of the issues accepted as part of the complaint, an explanation of the binding nature of the final decision or resolution on the class members, and the name, address and telephone number of the class representative. 29 C.F.R. Section 1614.204(e). In lieu of an investigation by the respondent agency, an EEOC AJ develops the record through discovery and a hearing. The AJ then issues a recommended decision to the agency. Within 60 days of receipt of the AJ's recommended decision on the merits of the class complaint, the agency must issue a final decision which either accepts, rejects or modifies the AJ's recommended decision. If the agency fails to issue such a decision within that time frame, the AJ's recommended decision becomes the agency's final decision in the class complaint.

When discrimination is found in the final decision and a class member believes that he or she is entitled to relief, the class member may file a written claim with the agency within 30 days of receipt of notification by the agency of its final decision. The EEOC AJ retains jurisdiction over the complaint in order to resolve disputed claims by class members. The claim for relief must contain a specific showing that the claimant is a class member entitled to relief. EEOC's regulations provide that, when a finding of

discrimination against a class has been made, there is a presumption of discrimination as to each member of the class. The agency must show by clear and convincing evidence that any class member is not entitled to relief. The agency must issue a final decision on each individual claim for relief within 90 days of filing. Such decision may be appealed to EEOC's OFO, or a civil action may be filed in federal court. 29 C.F.R. Section 1614.204(l)(3).

A class complaint may be resolved at any time by agreement between the agency and the class agent. Notice of such resolution must be provided to all class members, and reviewed and approved by an EEOC AJ. If the AJ finds that the proposed resolution is not fair to the class as a whole, the AJ will issue a decision vacating the agreement, and may replace the class agent with some other eligible class member to further process the class complaint. Such decision may be appealed to EEOC. If the AJ finds that the resolution is fair to the class as a whole, the resolution is binding on all class members. 29 C.F.R. Section 1614.204(g).

L. Grievances

Persons covered by collective bargaining agreements which permit allegations of discrimination to be raised in the grievance procedure, and who wish to file a complaint or grievance on an allegation of employment discrimination, must elect to proceed either under the procedures of 29 C.F.R. Part 1614 or the negotiated grievance procedures, but not both. 29 C.F.R. Section 1614.301(a). An election to proceed under Part 1614 is made by the filing of a complaint, and an election to proceed under the negotiated grievance procedures is made by filing a grievance. Participation in the pre-complaint procedures of Part 1614 is not an election of the 1614 procedures. The election requirement does not apply to employees of agencies not covered by 5 U.S.C. Section 7121(d), notably employees of the United States Postal Service.

M. Mixed Case Complaints

Some employment actions which may be the subject of a discrimination complaint under Part 1614 may also be appealed to the Merit Systems Protection Board (MSPB). In such cases, the employee must elect to proceed with a complaint as a "mixed case complaint" under Part 1614, or a "mixed case appeal" before the MSPB. Whichever is filed first is considered an election to proceed in that forum. 29 C.F.R. Section 1614.302.

Mixed case complaints are processed similarly to other complaints of discrimination, with the following notable exceptions: (1) the agency has only 120 days from the date of the filing of the mixed case complaint to issue a final decision, and the complainant may appeal the matter to the MSPB or file a civil action any time thereafter; (2) the complainant must appeal the agency's decision to the MSPB, not the

EEOC, within 30 days of receipt of the agency's decision; (3) at the completion of the investigation the complainant does not have the right to request a hearing before an EEOC AJ, and the agency must issue a decision within 45 days. 29 C.F.R. Section 1614.302(d). Individuals who have filed either a mixed case complaint or a mixed case appeal, and who have received a final decision from the MSPB, may petition the EEOC to review the MSPB final decision.

In contrast to non-mixed matters, individuals who wish to file a civil action in mixed-case matters must file within 30 days (not 90) of receipt of: (1) the agency's final decision; (2) the MSPB's final decision; or (3) the EEOC's decision on a petition to review. Alternatively, a civil action may be filed after 120 days from the date of filing the mixed case complaint with the agency or the mixed case appeal with the MSPB if there has been no final decision on the complaint or appeal, or 180 days after filing a petition to review with EEOC if there has been no decision by EEOC on the petition. 29 C.F.R. Section 1614.310.

APPENDIX III

Appendix III

FEDERAL AGENCIES' PROGRAM STATUS

Due to weather related closures in October 2012, the Form 462 was considered timely filed if certified by appropriate agency personnel on or before November 5, 2012, unless the agency requested and was granted an extension. No additional extensions were granted for the FY 2012 Form 462 report submission.

DEPARTMENT OR AGENCY Second Level Reporting Component √ Timely Filed / Yes ■ Filed After 11/5/2012 / No DNF Did Not File	Form 462 Report Timely Filed	EEO Director Reports to Agency Head	Provided EEO Staff with Training
African Development Foundation	√	√	√
Agency for International Development	√	√	√
American Battle Monuments Commission	√	■	√
Architectural & Transportation Barriers Compliance Board	√	√	■
Armed Forces Retirement Home	√	√	■
Broadcasting Board of Governors	√	√	√
Central Intelligence Agency	√	■	√
Chemical Safety and Hazard Investigation Board	√	√	√
Commission on Civil Rights	√	√	√
Committee for Purchase from People Who Are Blind or Severely Disabled	√	√	√
Commodity Futures Trading Commission	√	√	√
Consumer Financial Protection Bureau	√	√	■
Consumer Product Safety Commission	√	√	√
Corporation for National and Community Service	√	√	√
Court Services & Offender Supervision Agency for the DC	√	■	√
Defense Army and Air Force Exchange	√	√	√
Defense Commissary Agency	√	√	√
Defense Contract Audit Agency	√	√	√
Defense Contract Management Agency	√	√	√
Defense Finance and Accounting Service	√	■	√
Defense Human Resources Activity	√	√	√
Defense Information Systems Agency	√	■	√
Defense Intelligence Agency	√	√	√
Defense Joint Task Force Nat'l Capital Region Medical	√	■	√
Defense Logistics Agency	√	■	√
Defense Media Activity	√	√	√
Defense Missile Defense Agency	√	√	√
Defense National Geospatial-Intelligence Agency	√	√	√
Defense National Guard Bureau	■	■	√
Defense National Security Agency	√	√	√
Defense Nuclear Facilities Safety Board	√	√	√
Defense Office of the Inspector General	√	√	√
Defense Office of the Secretary/Wash. Hqtrs. Services	√	√	√
Defense Security Service	√	√	√
Defense Technical Information Center	√	√	√
Defense Threat Reduction Agency	√	■	√
Defense TRICARE Management Activity	√	■	√
Defense Uniformed Services University	√	√	√
Department of Agriculture	■	√	√
Agricultural Marketing Service	√	√	√
Agricultural Research Service	√	√	√
Agriculture Headquarters	■	√	√
Animal & Plant Health Inspection Service	√	√	√
National Institute of Food & Agriculture	√	√	√
Economic Research Service	√	■	√
Farm Service Agency	√	√	√

DEPARTMENT OR AGENCY Second Level Reporting Component √ Timely Filed / Yes ■ Filed After 11/5/2012 / No DNF Did Not File	Form 462 Report Timely Filed	EEO Director Reports to Agency Head	Provided EEO Staff with Training
Food and Nutrition Service	√	√	√
Food Safety And Inspection Service	■	■	√
Foreign Agricultural Service	√	√	√
Forest Service	√	■	√
Grain Inspection, Packers & Stockyards Administration	√	√	√
National Agricultural Statistics Service	√	√	√
National Appeals Division	■	√	■
Natural Resources Conservation Service	■	√	√
Office Of Inspector General	√	■	√
Office Of The Chief Financial Officer	■	■	√
Risk Management Agency	√	√	√
Rural Development	√	√	√
Department of Commerce	√	■	√
All Other Commerce Bureaus	√	■	√
Bureau of Census	√	■	√
Decennial Census	√	■	√
International Trade Administration	√	■	■
National Institute of Standards & Technology	√	■	√
National Oceanic & Atmospheric Admin	√	■	√
U. S. Patent and Trademark Office	√	√	√
Department of Defense Education Activity	√	√	√
Department of Education	√	■	√
Department of Energy	√	√	√
Department of Health and Human Services	√	√	√
Administration for Children and Families	√	■	√
Agency for Healthcare Research & Quality	√	■	√
Centers for Disease Control & Prevention	√	√	√
Centers for Medicare & Medicaid Services	√	√	√
Food and Drug Administration	√	■	√
Health Resources & Services Administration	√	√	√
Indian Health Service	√	■	√
National Institutes of Health	√	√	√
Office of the Secretary of HHS	√	√	√
Program Support Center	√	■	√
Substance Abuse & Mental Health Services Admin.	√	■	√
Department of Homeland Security	√	■	√
DHS Headquarters	√	■	√
Federal Emergency Management Ag	√	√	√
Federal Law Enforcement Training Center	√	√	√
Transportation Security Administration	√	√	√
U.S. Citizenship & Immigration Services	√	■	√
U.S. Coast Guard	√	√	√
U.S. Customs and Border Protection	√	√	√
U.S. Immigration & Customs Enforcement	√	√	√
U.S. Secret Service	√	√	√
Department of Housing and Urban Development	√	■	√

DEPARTMENT OR AGENCY Second Level Reporting Component √ Timely Filed / Yes ■ Filed After 11/5/2012 / No DNF Did Not File	Form 462 Report Timely Filed	EEO Director Reports to Agency Head	Provided EEO Staff with Training
Department of Justice	■	■	√
Alcohol, Tobacco, Firearms & Explosives	√	√	√
Bureau of Prisons	√	√	√
Drug Enforcement Administration	√	√	■
Executive Office for Immigration Review	√	√	√
Executive Office for U.S. Attorneys	√	■	√
Federal Bureau of Investigation	√	■	■
Office of Justice Programs	■	■	√
Offices, Boards, and Divisions	√	√	√
U.S. Marshals Service	√	√	√
Department of Labor	√	■	√
Bureau of Labor Statistics	√	■	√
DM and Others	√	■	√
Employment & Training Admin	√	■	√
Wage and Hour Division	√	■	√
Office of Workers Compensation Program	√	■	√
Mine Safety & Health Admin	√	■	√
Occupational Safety & Health Admin	√	■	√
Department of State	√	√	√
Department of the Air Force	√	√	√
Department of the Army	√	√	√
Department of the Interior	√	■	√
Bureau Of Indian Affairs	√	√	√
Bureau Of Land Management	√	■	√
Bureau of Ocean Energy Management	√	■	√
Bureau Of Reclamation	√	■	√
Bureau of Safety and Environmental Enforcement	√	■	√
Fish And Wildlife Service	√	■	√
Geological Survey	√	■	√
National Park Service	√	■	√
Office Of The Secretary	√	■	√
Office Of Surface Mining, Reclamation & Enforcement	√	■	√
Department of the Navy	√	√	√
Department of the Treasury	√	√	√
Alcohol & Tobacco Tax & Trade Bureau	√	√	√
Bureau of Engraving and Printing	√	■	√
Bureau of the Public Debt	√	■	√
Departmental Offices	√	■	√
Financial Crimes Enforcement Network	√	■	√
Financial Management Service	√	■	√
Internal Revenue Service	√	√	√
IRS Office of the Chief Counsel	√	√	√
Office of the Comptroller of the Currency	√	√	√
Office of the Inspector General	√	√	√
Special IG for Trouble Assets Relief Program	√	√	√
Treasury IG For Tax Administration	√	√	■
U. S. Mint	√	■	√

DEPARTMENT OR AGENCY Second Level Reporting Component √ Timely Filed / Yes ■ Filed After 11/5/2012 / No DNF Did Not File	Form 462 Report Timely Filed	EEO Director Reports to Agency Head	Provided EEO Staff with Training
Department of Transportation	√	√	√
Federal Aviation Admin	√	√	√
Federal Highway Admin	√	■	√
Federal Motor Carriers Safety Administration	√	√	√
Federal Railroad Administration	√	√	√
Federal Transit Administration	√	√	■
Maritime Administration	√	√	√
National Highway Traffic Safety Administration	√	√	√
DOT Office of Inspector General	√	■	√
DOT Office of the Secretary	√	√	√
Pipeline and Hazardous Management	√	√	√
Research and Innovative Technology Administration	√	√	√
St Lawrence Development Corp	√	√	√
Department of Veterans Affairs	√	√	√
National Cemeteries Administration	√	√	√
Veterans Benefits Administration	√	√	√
Veterans Health Administration	√	√	√
Headquarters and Others	√	√	√
Election Assistance Commission	**DNF**	**DNF**	**DNF**
Environmental Protection Agency	√	√	√
Equal Employment Opportunity Commission	√	√	√
Export-Import Bank of the US	√	√	√
Farm Credit Administration	√	√	√
Farm Credit System Insurance Corporation	√	√	√
Federal Communications Commission	√	√	√
Federal Deposit Insurance Corporation	√	■	√
Federal Election Commission	√	■	√
Federal Energy Regulatory Commission	√	√	√
Federal Housing Finance Agency	√	√	√
Federal Labor Relations Authority	√	√	√
Federal Maritime Commission	√	√	√
Federal Mediation and Conciliation Service	■	√	√
Federal Mine Safety and Health Review Commission	√	√	√
Federal Reserve System--Board of Governors	√	■	√
Federal Retirement Thrift Investment Board	**DNF**	**DNF**	**DNF**
Federal Trade Commission	√	√	√
General Services Administration	√	√	√
Government Printing Office	■	√	√
Harry S. Truman Scholarship Foundation	√	√	■
Holocaust Memorial Museum U.S.	√	■	√
Institute of Museum and Library Services	√	√	√
Inter-American Foundation	√	√	√
International Boundary and Water Commission	√	√	√
International Trade Commission	√	√	√
Japan-United States Friendship Commission	√	√	√
John F. Kennedy Center for the Performing Arts	√	■	√

DEPARTMENT OR AGENCY Second Level Reporting Component √ Timely Filed / Yes ■ Filed After 11/5/2012 / No DNF Did Not File	Form 462 Report Timely Filed	EEO Director Reports to Agency Head	Provided EEO Staff with Training
Marine Mammal Commission	√	■	■
Merit Systems Protection Board	√	√	√
Millennium Challenge Corporation	√	√	√
National Aeronautics and Space Administration	√	√	√
National Archives and Records Administration	√	√	√
National Capital Planning Commission	√	√	√
National Council on Disability	√	√	■
National Credit Union Administration	√	√	√
National Endowment for the Arts	√	√	√
National Endowment for the Humanities	√	√	√
National Gallery of Art	√	■	√
National Indian Gaming Commission	√	√	√
National Labor Relations Board	√	■	√
National Mediation Board	√	√	√
National Reconnaissance Office	√	√	√
National Science Foundation	√	√	√
National Transportation Safety Board	■	√	√
Navajo and Hopi Indian Relocation Commission	√	√	√
Nuclear Regulatory Commission	√	√	√
Occupational Safety and Health Review Commission	√	√	√
Office of Government Ethics	√	√	■
Office of Personnel Management	√	√	√
Office of Special Counsel	√	√	√
Office of the Director of National Intelligence	√	√	√
Overseas Private Investment Corporation	√	√	√
Peace Corps	√	√	√
Pension Benefit Guaranty Corporation	√	√	√
Postal Regulatory Commission	√	√	√
Railroad Retirement Board	√	√	√
Securities and Exchange Commission	√	√	√
Selective Service System	■	√	√
Small Business Administration	√	■	√
Smithsonian Institution	√	√	√
Social Security Administration	√	■	√
Tennessee Valley Authority	√	■	√
Trade and Development Agency	√	√	√
U.S. Postal Service	√	■	√
Capital Metro Area Operations	√	■	√
Eastern Area	√	■	√
Great Lakes Area	√	■	√
Headquarters	√	■	√
Northeast Area	√	■	√
Office of the Inspector General	√	■	√
Pacific Area	√	■	√
Southern Area	√	■	√
Western Area	√	■	√

APPENDIX IV

APPENDIX IV

FY 2012 FEDERAL EEO COMPLAINT PROCESSING TABLES

GOVERNMENT-WIDE EEO COMPLAINT PROCESSING, APPELLATE RECEIPTS AND CLOSURES, AND ALTERNATIVE DISPUTE RESOLUTION (Data provided by agencies' EEO Form 462 Reports)

Table B-1 FY 2012 Total Work Force, Counselings, and Complaints

Agency or Department	Total Work Force	Number Completed/ Ended Counselings	Number Individuals with Completed/ Ended Counselings	Counseled Individuals as % of Total Work Force	Number Complaints Filed	Number Complainants	Number Complainants as % of Total Work Force
Advisory Council on Historic Preservation	NRF	NRF	NRF	NRF	NRF	NRF	NRF
African Development Foundation	73	0	0	0.00%	0	0	0.00%
Agency for International Development	3,983	34	32	0.80%	14	13	0.33%
American Battle Monuments Commission	76	1	1	1.32%	1	1	1.32%
Appalachian Regional Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Architectural and Transportation Barriers Compliance Board	28	0	0	0.00%	0	0	0.00%
Arctic Research Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Armed Forces Retirement Home	282	5	5	1.77%	4	4	1.42%
Barry Goldwater Scholarship and Excellence in Education Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Broadcasting Board of Governors	1,675	53	45	2.69%	12	12	0.72%
Central Intelligence Agency *	0	42	38	0.00%	27	24	0.00%
Chemical Safety and Hazard Investigation Board	46	2	2	4.35%	1	1	2.17%
Christopher Columbus Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission of Fine Arts	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission on Civil Rights	44	0	0	0.00%	0	0	0.00%
Committee for Purchase from People Who Are Blind or Severely Disabled	31	0	0	0.00%	0	0	0.00%
Commodity Futures Trading Commission	707	1	1	0.14%	1	1	0.14%
Consumer Financial Protection Bureau	970	15	14	1.44%	11	11	1.13%
Consumer Product Safety Commission	522	3	3	0.57%	2	2	0.38%
Corporation for National and Community Service	615	7	7	1.14%	5	4	0.65%
Court Services and Offender Supervision Agency for the District of Columbia	1,242	24	22	1.77%	10	9	0.72%
Defense Army and Air Force Exchange	34,273	336	325	0.95%	101	99	0.29%
Defense Commissary Agency	14,382	227	226	1.57%	140	139	0.97%
Defense Contract Audit Agency	5,181	45	45	0.87%	28	28	0.54%
Defense Contract Management Agency	10,452	85	78	0.75%	45	41	0.39%

Table B-1 FY 2012 Total Work Force, Counselings, and Complaints							
Agency or Department	**Total Work Force**	**Number Completed/ Ended Counselings**	**Number Individuals with Completed/ Ended Counselings**	**Counseled Individuals as % of Total Work Force**	**Number Complaints Filed**	**Number Complainants**	**Number Complainants as % of Total Work Force**
Defense Finance and Accounting Service	11,982	92	88	0.73%	38	36	0.30%
Defense Human Resources Activity	1,176	8	8	0.68%	4	4	0.34%
Defense Information Systems Agency	6,304	30	30	0.48%	17	17	0.27%
Defense Intelligence Agency *	0	89	88	0.00%	42	42	0.00%
Defense JTF National Capital Region Medical	4,417	84	83	1.88%	33	33	0.75%
Defense Logistics Agency	25,229	312	296	1.17%	121	117	0.46%
Defense Media Activity	2,000	3	3	0.15%	1	1	0.05%
Defense Missile Defense Agency	2,326	11	11	0.47%	5	5	0.21%
Defense National Geospatial-Intelligence Agency *	0	31	29	0.00%	20	18	0.00%
Defense National Guard Bureau	57,511	113	111	0.19%	26	25	0.04%
Defense National Security Agency *	0	69	65	0.00%	19	18	0.00%
Defense Nuclear Facilities Safety Board	116	0	0	0.00%	0	0	0.00%
Defense Office of the Inspector General	1,600	9	9	0.56%	6	6	0.38%
Defense Office of the Secretary - Wash. Hqtrs. Services	6,766	45	44	0.65%	27	27	0.40%
Defense Security Service	874	18	13	1.49%	8	8	0.92%
Defense Technical Information Center	204	1	1	0.49%	0	0	0.00%
Defense Threat Reduction Agency	1,299	19	19	1.46%	9	9	0.69%
Defense TRICARE Management Activity	842	18	18	2.14%	10	10	1.19%
Defense Uniformed Services University	794	5	5	0.63%	2	2	0.25%
Department of Agriculture	103,822	975	937	0.90%	524	508	0.49%
Department of Commerce	45,766	325	304	0.66%	222	205	0.45%
Department of Defense Education Activity	16,346	136	135	0.83%	79	79	0.48%
Department of Education	4,373	48	48	1.10%	33	32	0.73%
Department of Energy	15,680	124	124	0.79%	72	72	0.46%
Department of Health and Human Services	83,123	674	649	0.78%	382	375	0.45%
Department of Homeland Security	200,559	2,031	1,946	0.97%	1,198	1,159	0.58%
Department of Housing and Urban Development	9,061	106	105	1.16%	63	62	0.68%
Department of Justice	116,973	1,372	1,333	1.14%	761	749	0.64%

Table B-1 FY 2012 Total Work Force, Counselings, and Complaints							
Agency or Department	**Total Work Force**	**Number Completed/ Ended Counselings**	**Number Individuals with Completed/ Ended Counselings**	**Counseled Individuals as % of Total Work Force**	**Number Complaints Filed**	**Number Complainants**	**Number Complainants as % of Total Work Force**
Department of Labor	16,819	206	201	1.20%	133	129	0.77%
Department of State	69,885	271	262	0.37%	134	132	0.19%
Department of the Air Force	173,807	1,002	934	0.54%	473	456	0.26%
Department of the Army	250,617	2,301	2,139	0.85%	1,226	1,157	0.46%
Department of the Interior	78,779	592	577	0.73%	352	348	0.44%
Department of the Navy	245,574	1,531	1,503	0.61%	696	679	0.28%
Department of the Treasury	115,292	746	688	0.60%	406	370	0.32%
Department of Transportation	57,187	541	505	0.88%	315	297	0.52%
Department of Veterans Affairs	323,154	4,484	4,060	1.26%	2,347	2,165	0.67%
Election Assistance Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Environmental Protection Agency	17,001	98	95	0.56%	78	78	0.46%
Equal Employment Opportunity Commission	2,291	41	40	1.75%	25	22	0.96%
Export-Import Bank of the U.S.	408	2	2	0.49%	1	1	0.25%
Farm Credit Administration	302	1	1	0.33%	0	0	0.00%
Farm Credit System Insurance Corporation	12	0	0	0.00%	0	0	0.00%
Federal Communications Commission	1,788	15	15	0.84%	10	10	0.56%
Federal Deposit Insurance Corporation	7,846	82	71	0.90%	44	37	0.47%
Federal Election Commission	355	4	4	1.13%	0	0	0.00%
Federal Energy Regulatory Commission	1,483	13	11	0.74%	6	4	0.27%
Federal Financial Institutions Examination Council	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Housing Finance Agency	706	17	17	2.41%	9	9	1.27%
Federal Labor Relations Authority	138	3	3	2.17%	1	1	0.72%
Federal Maritime Commission	124	3	3	2.42%	2	2	1.61%
Federal Mediation and Conciliation Service	243	2	2	0.82%	4	4	1.65%
Federal Mine Safety & Health Review Commission	78	0	0	0.00%	0	0	0.00%
Federal Reserve System--Board of Governors	2,412	54	54	2.24%	12	12	0.50%
Federal Retirement Thrift Investment Board	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Trade Commission	1,178	10	10	0.85%	0	0	0.00%
General Services Administration	12,416	158	143	1.15%	96	87	0.70%

Table B-1 FY 2012 Total Work Force, Counselings, and Complaints							
Agency or Department	**Total Work Force**	**Number Completed/ Ended Counselings**	**Number Individuals with Completed/ Ended Counselings**	**Counseled Individuals as % of Total Work Force**	**Number Complaints Filed**	**Number Complainants**	**Number Complainants as % of Total Work Force**
Government Printing Office	1,879	70	53	2.82%	27	23	1.22%
Harry S. Truman Scholarship Foundation	5	0	0	0.00%	0	0	0.00%
Holocaust Memorial Museum U.S.	397	0	0	0.00%	0	0	0.00%
Institute of Museum and Library Services	88	0	0	0.00%	0	0	0.00%
Inter-American Foundation	43	0	0	0.00%	0	0	0.00%
International Boundary and Water Commission	258	2	2	0.78%	0	0	0.00%
International Joint Commission: U.S. & Canada	NRF	NRF	NRF	NRF	NRF	NRF	NRF
International Trade Commission	397	2	2	0.50%	2	2	0.50%
James Madison Memorial Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Japan-United States Friendship Commission	4	0	0	0.00%	0	0	0.00%
John F. Kennedy Center for the Performing Arts	2,250	2	2	0.09%	1	1	0.04%
Marine Mammal Commission	14	0	0	0.00%	0	0	0.00%
Merit Systems Protection Board	208	3	3	1.44%	1	1	0.48%
Millennium Challenge Corporation	288	0	0	0.00%	0	0	0.00%
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Aeronautics and Space Administration	18,416	77	73	0.40%	39	38	0.21%
National Archives and Records Administration	3,381	33	32	0.95%	4	3	0.09%
National Capital Planning Commission	39	0	0	0.00%	0	0	0.00%
National Council on Disability	26	0	0	0.00%	0	0	0.00%
National Credit Union Administration	1,195	7	7	0.59%	3	3	0.25%
National Endowment for the Arts	174	8	8	4.60%	1	1	0.57%
National Endowment for the Humanities	199	0	0	0.00%	0	0	0.00%
National Foundation on the Arts & the Humanities	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Gallery of Art	834	3	3	0.36%	2	2	0.24%
National Indian Gaming Commission	97	1	1	1.03%	0	0	0.00%
National Labor Relations Board	1,702	19	19	1.12%	9	8	0.47%
National Mediation Board	50	0	0	0.00%	0	0	0.00%
National Reconnaissance Office *	0	7	7	0.00%	3	3	0.00%

Table B-1 FY 2012 Total Work Force, Counselings, and Complaints							
Agency or Department	**Total Work Force**	**Number Completed/ Ended Counselings**	**Number Individuals with Completed/ Ended Counselings**	**Counseled Individuals as % of Total Work Force**	**Number Complaints Filed**	**Number Complainants**	**Number Complainants as % of Total Work Force**
National Science Foundation	1,663	15	15	0.90%	11	10	0.60%
National Transportation Safety Board	413	3	3	0.73%	2	2	0.48%
Navajo and Hopi Indian Relocation Commission	38	0	0	0.00%	0	0	0.00%
Nuclear Regulatory Commission	3,775	35	33	0.87%	16	16	0.42%
Nuclear Waste Technical Review Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Occupational Safety & Health Review Commission	58	0	0	0.00%	0	0	0.00%
Office of Government Ethics	69	10	5	7.25%	0	0	0.00%
Office of Personnel Management	5,843	88	77	1.32%	44	39	0.67%
Office of Special Counsel	129	0	0	0.00%	0	0	0.00%
Office of the Director of National Intelligence *	0	5	5	0.00%	4	4	0.00%
Overseas Private Investment Corporation	241	2	2	0.83%	0	0	0.00%
Peace Corps	896	6	6	0.67%	4	4	0.45%
Pension Benefit Guaranty Corporation	971	20	18	1.85%	13	10	1.03%
Postal Regulatory Commission	73	1	1	1.37%	0	0	0.00%
Presidio Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Railroad Retirement Board	945	6	6	0.63%	2	2	0.21%
Securities and Exchange Commission	3,826	30	27	0.71%	20	17	0.44%
Selective Service System	121	2	2	1.65%	2	2	1.65%
Small Business Administration	5,228	75	70	1.34%	36	35	0.67%
Smithsonian Institution	6,057	38	35	0.58%	13	13	0.21%
Social Security Administration	65,474	917	816	1.25%	494	451	0.69%
Tennessee Valley Authority	12,762	86	84	0.66%	58	56	0.44%
Trade and Development Agency	46	0	0	0.00%	0	0	0.00%
U.S. Postal Service	625,701	13,143	11,976	1.91%	4,532	4,272	0.68%

Table B-1 FY 2012 Total Work Force, Counselings, and Complaints							
Agency or Department	**Total Work Force**	**Number Completed/ Ended Counselings**	**Number Individuals with Completed/ Ended Counselings**	**Counseled Individuals as % of Total Work Force**	**Number Complaints Filed**	**Number Complainants**	**Number Complainants as % of Total Work Force**
Utah Reclamation Mitigation & Conservation Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Valles Caldera Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Cabinet Level Subtotal	2,740,130	32,258	30,021	1.10%	14,650	13,931	0.51%
Midsize Agencies Subtotal	152,013	1,634	1,478	0.97%	913	845	0.56%
Small Agencies Subtotal	46,564	615	571	1.23%	272	248	0.53%
Micro Agencies Subtotal	1,186	14	9	0.75%	2	2	0.17%
Government-wide	2,939,893	34,521	32,079	1.09%	15,837	15,026	0.51%

NRF = No Report Filed

* Total work force numbers do not include employees not reported for national security reasons.

Table B-1a FY 2012 Total Work Force, Counselings, and Complaints - Sub-Component Data							
Agency or Department	**Total Work Force**	**Number Completed/ Ended Counselings**	**Number Individuals with Completed/ Ended Counselings**	**Counseled Individuals as % of Total Work Force**	**Number Complaints Filed**	**Number Complainants**	**Number Complainants as % of Total Work Force**
Defense Logistics Agency Wide	**25,229**	**312**	**296**	**1.17%**	**121**	**117**	**0.46%**
DLA Aviation	3,589	54	54	1.50%	22	22	0.61%
DLA Disposition Services	1,350	10	9	0.67%	3	3	0.22%
DLA Distribution	7,911	151	141	1.78%	52	50	0.63%
DLA Headquarters Operations Division	4,690	53	52	1.11%	27	26	0.55%
DLA Land and Maritime	4,394	20	20	0.46%	13	13	0.30%
DLA Logistics Information Service	959	2	2	0.21%	0	0	0.00%
DLA Troop Support	2,336	22	18	0.77%	4	3	0.13%
Defense National Guard Bureau Wide	**57,511**	**113**	**111**	**0.19%**	**26**	**25**	**0.04%**
Defense National Guard Bureau Headquarters	2	0	0	0.00%	0	0	0.00%
Alabama National Guard	1,210	1	1	0.08%	0	0	0.00%
Alaska National Guard	693	0	0	0.00%	0	0	0.00%
Arizona National Guard	2,371	6	5	0.21%	2	2	0.08%
Arkansas National Guard	968	3	3	0.31%	0	0	0.00%
California National Guard	2,316	17	16	0.69%	8	7	0.30%
Colorado National Guard	695	1	1	0.14%	1	1	0.14%
Connecticut National Guard	729	0	0	0.00%	0	0	0.00%
DC National Guard	447	1	1	0.22%	1	1	0.22%
Delaware National Guard	432	0	0	0.00%	0	0	0.00%
Florida National Guard	1,044	1	1	0.10%	1	1	0.10%
Georgia National Guard	1,200	0	0	0.00%	0	0	0.00%
Guam National Guard	0	0	0	0.00%	0	0	0.00%
Hawaii National Guard	1,123	0	0	0.00%	0	0	0.00%
Idaho National Guard	811	0	0	0.00%	0	0	0.00%
Illinois National Guard	1,143	0	0	0.00%	0	0	0.00%
Indiana National Guard	1,125	1	1	0.09%	1	1	0.09%
Iowa National Guard	1,013	34	34	3.36%	0	0	0.00%

Table B-1a FY 2012 Total Work Force, Counselings, and Complaints - Sub-Component Data							
Agency or Department	**Total Work Force**	**Number Completed/ Ended Counselings**	**Number Individuals with Completed/ Ended Counselings**	**Counseled Individuals as % of Total Work Force**	**Number Complaints Filed**	**Number Complainants**	**Number Complainants as % of Total Work Force**
Kansas National Guard	1,059	1	1	0.09%	0	0	0.00%
Kentucky National Guard	894	0	0	0.00%	0	0	0.00%
Louisiana National Guard	957	0	0	0.00%	0	0	0.00%
Maine National Guard	498	0	0	0.00%	0	0	0.00%
Maryland National Guard	799	0	0	0.00%	0	0	0.00%
Massachusetts National Guard	892	4	4	0.45%	0	0	0.00%
Michigan National Guard	1,113	5	5	0.45%	1	1	0.09%
Minnesota National Guard	1,029	1	1	0.10%	0	0	0.00%
Mississippi National Guard	1,294	1	1	0.08%	0	0	0.00%
Missouri National Guard	1,315	1	1	0.08%	1	1	0.08%
Montana National Guard	598	1	1	0.17%	0	0	0.00%
Nebraska National Guard	552	0	0	0.00%	0	0	0.00%
Nevada National Guard	587	2	2	0.34%	2	2	0.34%
New Hampshire National Guard	413	0	0	0.00%	0	0	0.00%
New Jersey National Guard	933	0	0	0.00%	0	0	0.00%
New Mexico National Guard	891	0	0	0.00%	0	0	0.00%
New York National Guard	2,099	6	6	0.29%	2	2	0.10%
North Carolina National Guard	1,066	0	0	0.00%	0	0	0.00%
North Dakota National Guard	643	1	1	0.16%	0	0	0.00%
Ohio National Guard	1,972	0	0	0.00%	0	0	0.00%
Oklahoma National Guard	965	0	0	0.00%	0	0	0.00%
Oregon National Guard	1,157	0	0	0.00%	0	0	0.00%
Pennsylvania National Guard	3,710	1	1	0.03%	0	0	0.00%
Puerto Rico National Guard	832	6	6	0.72%	0	0	0.00%
Rhode Island National Guard	479	0	0	0.00%	0	0	0.00%
South Carolina National Guard	1,050	1	1	0.10%	1	1	0.10%
South Dakota National Guard	600	0	0	0.00%	0	0	0.00%
Tennessee National Guard	1,792	1	1	0.06%	1	1	0.06%
Texas National Guard	1,781	1	1	0.06%	1	1	0.06%

Table B-1a FY 2012 Total Work Force, Counselings, and Complaints - Sub-Component Data							
Agency or Department	**Total Work Force**	**Number Completed/ Ended Counselings**	**Number Individuals with Completed/ Ended Counselings**	**Counseled Individuals as % of Total Work Force**	**Number Complaints Filed**	**Number Complainants**	**Number Complainants as % of Total Work Force**
Utah National Guard	697	4	4	0.57%	1	1	0.14%
Vermont National Guard	498	0	0	0.00%	0	0	0.00%
Virgin Islands National Guard	241	0	0	0.00%	0	0	0.00%
Virginia National Guard	794	2	2	0.25%	0	0	0.00%
Washington State National Guard	882	3	3	0.34%	2	2	0.23%
West Virginia National Guard	913	4	4	0.44%	0	0	0.00%
Wisconsin National Guard	994	0	0	0.00%	0	0	0.00%
Wyoming National Guard	3,200	2	2	0.06%	0	0	0.00%
Department of Agriculture Wide	**103,822**	**975**	**937**	**0.90%**	**524**	**508**	**0.49%**
USDA Agricultural Marketing Service	4,074	26	25	0.61%	21	20	0.49%
USDA Agricultural Research Service	8,369	40	40	0.48%	30	30	0.36%
USDA Agriculture Headquarters	3,056	51	51	1.67%	27	27	0.88%
USDA Animal and Plant Health Inspection Service	8,316	87	87	1.05%	47	47	0.57%
USDA Economic Research Service	351	1	1	0.28%	1	1	0.28%
USDA Farm Service Agency	4,622	47	47	1.02%	22	22	0.48%
USDA Food and Nutrition Service	1,392	12	12	0.86%	7	7	0.50%
USDA Food Safety And Inspection Service	9,984	180	171	1.71%	67	66	0.66%
USDA Foreign Agricultural Service	954	13	13	1.36%	10	10	1.05%
USDA Forest Service	41,093	302	274	0.67%	170	156	0.38%
USDA Grain Inspection,Packers & Stockyards Admin	765	15	15	1.96%	9	9	1.18%
USDA National Agricultural Statistics Service	1,160	4	4	0.34%	1	1	0.09%
USDA National Appeals Division	94	0	0	0.00%	0	0	0.00%
USDA National Institute of Food and Agriculture	380	2	2	0.53%	1	1	0.26%
USDA Natural Resources Conservation Service	11,821	74	74	0.63%	39	39	0.33%
USDA Office Of The Chief Financial Officer	1,271	41	41	3.23%	23	23	1.81%
USDA Office Of Inspector General	547	10	10	1.83%	8	8	1.46%
USDA Risk Management Agency	479	14	14	2.92%	5	5	1.04%
USDA Rural Development	5,094	56	56	1.10%	36	36	0.71%

Table B-1a FY 2012 Total Work Force, Counselings, and Complaints - Sub-Component Data							
Agency or Department	**Total Work Force**	**Number Completed/ Ended Counselings**	**Number Individuals with Completed/ Ended Counselings**	**Counseled Individuals as % of Total Work Force**	**Number Complaints Filed**	**Number Complainants**	**Number Complainants as % of Total Work Force**
Department of Commerce Wide	**45,766**	**325**	**304**	**0.66%**	**222**	**205**	**0.45%**
DOC All Other Commerce Bureaus	2,774	30	29	1.05%	24	23	0.83%
DOC Bureau of the Census	14,084	114	106	0.75%	67	63	0.45%
DOC Decennial Census	0	5	5	0.00%	4	4	0.00%
DOC International Trade Administration	1,468	11	11	0.75%	5	5	0.34%
DOC National Institute of Standards & Technology	3,199	24	24	0.75%	13	13	0.41%
DOC National Oceanic & Atmospheric Admin.	12,630	82	77	0.61%	65	60	0.48%
DOC U. S. Patent and Trademark Office	11,611	59	52	0.45%	44	37	0.32%
Department of Energy Wide	**15,680**	**124**	**124**	**0.79%**	**72**	**72**	**0.46%**
DOE Bonneville Power Administration	3,090	28	28	0.91%	11	11	0.36%
DOE Chicago Operations Office	301	1	1	0.33%	1	1	0.33%
DOE EM Consolidated Business Center	295	4	4	1.36%	2	2	0.68%
DOE Golden Field Office	153	5	5	3.27%	2	2	1.31%
DOE Headquarters	5,649	32	32	0.57%	20	20	0.35%
DOE Idaho Operations Office	238	3	3	1.26%	1	1	0.42%
DOE National Energy Technology Lab	587	2	2	0.34%	2	2	0.34%
DOE NNSA Service Center	2,659	21	21	0.79%	17	17	0.64%
DOE Oak Ridge Operations	218	2	2	0.92%	2	2	0.92%
DOE OSTI	43	0	0	0.00%	0	0	0.00%
DOE Richland Operations Office	393	1	1	0.25%	0	0	0.00%
DOE Savannah River Operations	287	6	6	2.09%	3	3	1.05%
DOE Southeastern Power Administration	43	0	0	0.00%	0	0	0.00%
DOE Southwestern Power Administration	184	3	3	1.63%	1	1	0.54%
DOE Strategic Petroleum Reserve	95	0	0	0.00%	0	0	0.00%
DOE Western Area Power Administration	1,445	16	16	1.11%	10	10	0.69%

Table B-1a FY 2012 Total Work Force, Counselings, and Complaints - Sub-Component Data							
Agency or Department	**Total Work Force**	**Number Completed/ Ended Counselings**	**Number Individuals with Completed/ Ended Counselings**	**Counseled Individuals as % of Total Work Force**	**Number Complaints Filed**	**Number Complainants**	**Number Complainants as % of Total Work Force**
Department of Health and Human Services Wide	**83,123**	**674**	**649**	**0.78%**	**382**	**375**	**0.45%**
HHS Administration for Children and Families	1,351	12	12	0.89%	9	9	0.67%
HHS Agency for Healthcare Research and Quality	301	3	2	0.66%	3	2	0.66%
HHS Centers for Disease Control and Prevention	11,229	127	127	1.13%	81	81	0.72%
HHS Centers for Medicare & Medicaid Services	5,610	38	37	0.66%	24	23	0.41%
HHS Food and Drug Administration	12,989	123	115	0.89%	70	68	0.52%
HHS Health Resources & Services Admin.	1,690	20	20	1.18%	12	12	0.71%
HHS Indian Health Service	13,722	198	189	1.38%	79	78	0.57%
HHS National Institutes of Health	18,560	99	93	0.50%	70	68	0.37%
HHS Office of the Sec. of Health & Human Srvcs	16,498	44	44	0.27%	24	24	0.15%
HHS Program Support Center	619	7	7	1.13%	7	7	1.13%
HHS Substance Abuse & Mental Health Srvcs Admin	554	3	3	0.54%	3	3	0.54%
Department of Homeland Security Wide	**200,559**	**2,031**	**1,946**	**0.97%**	**1,198**	**1,159**	**0.58%**
DHS Federal Emergency Management Agency	16,967	242	234	1.38%	137	135	0.80%
DHS Federal Law Enforcement Training Center	1,113	18	18	1.62%	11	11	0.99%
DHS Headquarters	7,752	77	75	0.97%	55	54	0.70%
DHS Transportation Security Administration	65,470	658	643	0.98%	391	382	0.58%
DHS U.S. Citizenship and Immigration Services	11,200	186	173	1.54%	114	108	0.96%
DHS U.S. Coast Guard	10,309	96	88	0.85%	45	43	0.42%
DHS U.S. Customs and Border Protection	60,668	464	439	0.72%	260	248	0.41%

Table B-1a FY 2012 Total Work Force, Counselings, and Complaints - Sub-Component Data							
Agency or Department	**Total Work Force**	**Number Completed/ Ended Counselings**	**Number Individuals with Completed/ Ended Counselings**	**Counseled Individuals as % of Total Work Force**	**Number Complaints Filed**	**Number Complainants**	**Number Complainants as % of Total Work Force**
DHS U.S. Immigration and Customs Enforcement	20,307	242	236	1.16%	154	152	0.75%
DHS U.S. Secret Service	6,773	48	40	0.59%	31	26	0.38%
Department of Justice Wide	**116,973**	**1,372**	**1,333**	**1.14%**	**761**	**749**	**0.64%**
DOJ Alcohol, Tobacco, Firearms and Explosives	4,816	67	67	1.39%	40	40	0.83%
DOJ Bureau of Prisons	38,327	838	815	2.13%	433	429	1.12%
DOJ Drug Enforcement Administration	9,764	44	40	0.41%	28	28	0.29%
DOJ Executive Office for Immigration Review	1,417	16	16	1.13%	15	15	1.06%
DOJ Executive Office for U.S. Attorneys	11,589	37	35	0.30%	26	24	0.21%
DOJ Federal Bureau of Investigation	36,188	221	221	0.61%	130	130	0.36%
DOJ Office of Justice Programs	609	18	14	2.30%	15	14	2.30%
DOJ Offices, Boards, and Divisions	8,619	46	46	0.53%	21	21	0.24%
DOJ U.S. Marshals Service	5,644	85	79	1.40%	53	48	0.85%
Department of Labor Wide	**16,819**	**206**	**201**	**1.20%**	**133**	**129**	**0.77%**
DOL (DM and others)	4,952	73	71	1.43%	42	40	0.81%
DOL Bureau of Labor Statistics	2,461	6	6	0.24%	6	6	0.24%
DOL Employment and Training Administration	1,164	17	16	1.37%	15	14	1.20%
DOL Mine Safety and Health Administration	2,430	31	30	1.23%	16	16	0.66%
DOL Occupational Safety & Health Admin.	2,276	22	22	0.97%	15	15	0.66%
DOL Office of Workers Compensation Programs	1,644	25	25	1.52%	15	15	0.91%
DOL Wage and Hour Division	1,892	32	31	1.64%	24	23	1.22%
Department of the Army Wide	**250,617**	**2,301**	**2,139**	**0.85%**	**1,226**	**1,157**	**0.46%**
Headquarters, Department of Army	13,988	171	160	1.14%	100	93	0.66%
U.S. Army Corps of Engineers	36,924	248	221	0.60%	147	133	0.36%

Table B-1a FY 2012 Total Work Force, Counselings, and Complaints - Sub-Component Data							
Agency or Department	**Total Work Force**	**Number Completed/ Ended Counselings**	**Number Individuals with Completed/ Ended Counselings**	**Counseled Individuals as % of Total Work Force**	**Number Complaints Filed**	**Number Complainants**	**Number Complainants as % of Total Work Force**
U.S. Army Europe	1,890	18	17	0.90%	6	6	0.32%
U.S. Army Forces Command	13,265	175	168	1.27%	86	84	0.63%
U.S. Army Installation Management Command	55,682	545	504	0.91%	281	268	0.48%
U.S. Army Intelligence and Security Command	3,384	22	20	0.59%	14	13	0.38%
U.S. Army Material Command	65,339	508	467	0.71%	281	264	0.40%
U.S. Army Medical Command	27,226	424	400	1.47%	211	200	0.73%
U.S. Army Network Enterprise Tech. Command	6,029	26	25	0.41%	17	16	0.27%
U.S. Army Pacific (USARPAC)	1,491	2	2	0.13%	2	2	0.13%
U.S. Army Space and Missile Defense Command	917	1	1	0.11%	1	1	0.11%
U.S. Army Special Ops Command (USASOC)	1,722	16	16	0.93%	7	7	0.41%
U.S. Army Test and Evaluation Command	4,032	16	16	0.40%	9	9	0.22%
U.S. Army Training and Doctrine Command	18,257	127	120	0.66%	62	59	0.32%
Department of the Interior Wide	**78,779**	**592**	**577**	**0.73%**	**352**	**348**	**0.44%**
Bureau of Ocean Energy Management	559	7	6	1.07%	4	4	0.72%
Bureau of Safety and Environmental Enforcement	680	7	7	1.03%	7	7	1.03%
DOI Bureau Of Indian Affairs	9,007	56	56	0.62%	35	35	0.39%
DOI Bureau Of Land Management	11,878	81	79	0.67%	46	44	0.37%
DOI Bureau Of Reclamation	5,489	78	75	1.37%	50	49	0.89%
DOI Fish And Wildlife Service	10,378	56	55	0.53%	36	36	0.35%
DOI Geological Survey	9,209	22	22	0.24%	13	13	0.14%
DOI National Park Service	26,674	208	200	0.75%	114	113	0.42%
DOI Office Of Surface Mining, Reclamation and Enforcement	511	6	6	1.17%	5	5	0.98%
DOI-Office Of The Secretary	4,394	71	71	1.62%	42	42	0.96%

Table B-1a FY 2012 Total Work Force, Counselings, and Complaints - Sub-Component Data							
Agency or Department	**Total Work Force**	**Number Completed/ Ended Counselings**	**Number Individuals with Completed/ Ended Counselings**	**Counseled Individuals as % of Total Work Force**	**Number Complaints Filed**	**Number Complainants**	**Number Complainants as % of Total Work Force**
Department of the Navy Wide	**245,574**	**1,531**	**1,503**	**0.61%**	**696**	**679**	**0.28%**
Chief Of Naval Operations	4,627	27	27	0.58%	12	12	0.26%
Commander Naval Installations Command	33,284	270	267	0.80%	111	109	0.33%
Commander Naval Reserve	465	0	0	0.00%	0	0	0.00%
Commander Pacific Fleet	18,967	125	123	0.65%	41	40	0.21%
DON Assistant for Administration	4,895	54	52	1.06%	29	29	0.59%
DON Bureau of Medicine & Surgery	12,042	120	120	1.00%	50	50	0.42%
DON SPAWAR	9,084	25	23	0.25%	8	6	0.07%
DON Strategic Systems Project Office	1,067	7	7	0.66%	7	7	0.66%
Fleet Cyber Command	0	16	15	0.00%	6	6	0.00%
Fleet Forces Command	22,743	88	87	0.38%	39	38	0.17%
Marine Corps HQ	33,293	233	233	0.70%	99	99	0.30%
Military Sealift Command	6,936	56	54	0.78%	37	35	0.50%
Naval Air Systems Command	24,739	162	162	0.65%	80	80	0.32%
Naval Education & Training Command	4,526	31	30	0.66%	14	14	0.31%
Naval Sea Systems Command	26,612	71	67	0.25%	36	34	0.13%
Naval Special Warfare Command	1,161	5	5	0.43%	3	3	0.26%
Naval Supply Systems Command	18,328	95	94	0.51%	44	43	0.23%
Naval Systems Management Activity	2	0	0	0.00%	0	0	0.00%
Navy Facilities & Engineering Command	16,203	118	110	0.68%	57	52	0.32%
Navy Military Personnel Command	1,770	9	9	0.51%	7	7	0.40%
Office Of Naval Intelligence	1,680	15	14	0.83%	13	12	0.71%
Office Of Naval Research	3,150	4	4	0.13%	3	3	0.10%
Department of the Treasury Wide	**115,292**	**746**	**688**	**0.60%**	**406**	**370**	**0.32%**
Treas Alcohol and Tobacco Tax and Trade Bureau	485	1	1	0.21%	1	1	0.21%
Treas Bureau of Engraving and Printing	1,934	31	31	1.60%	24	24	1.24%
Treas Bureau of the Public Debt	1,998	14	11	0.55%	4	4	0.20%

Table B-1a FY 2012 Total Work Force, Counselings, and Complaints - Sub-Component Data							
Agency or Department	**Total Work Force**	**Number Completed/ Ended Counselings**	**Number Individuals with Completed/ Ended Counselings**	**Counseled Individuals as % of Total Work Force**	**Number Complaints Filed**	**Number Complainants**	**Number Complainants as % of Total Work Force**
Treas Departmental Offices	1,934	16	16	0.83%	9	9	0.47%
Treas Financial Crimes Enforcement Network	305	5	5	1.64%	2	2	0.66%
Treas Financial Management Service	1,577	15	15	0.95%	12	12	0.76%
Treas Inspector General For Tax Administration	797	2	2	0.25%	2	2	0.25%
Treas Internal Revenue Service	97,942	587	535	0.55%	303	272	0.28%
Treas Office of the Comptroller of the Currency	3,823	17	17	0.44%	12	9	0.24%
Treas Special Inspector General for the Trouble Assets Relief Program	164	0	0	0.00%	0	0	0.00%
Treas U. S. Mint	1,778	50	47	2.64%	33	31	1.74%
Treas IRS Office of the Chief Counsel	2,380	7	7	0.29%	3	3	0.13%
Treas- Office of the Inspector General	175	1	1	0.57%	1	1	0.57%
Department of Transportation Wide	**57,187**	**541**	**505**	**0.88%**	**315**	**297**	**0.52%**
DOT Federal Aviation Administration	47,739	437	404	0.85%	256	238	0.50%
DOT Federal Highway Administration	2,951	27	25	0.85%	9	9	0.30%
DOT Federal Motor Carrier Safety Administration	1,104	8	8	0.72%	5	5	0.45%
DOT Federal Railroad Administrataion	874	4	4	0.46%	3	3	0.34%
DOT Federal Transit Administration	564	11	11	1.95%	7	7	1.24%
DOT Maritime Administration	844	13	13	1.54%	11	11	1.30%
DOT National Highway Traffic Safety Admin	595	10	10	1.68%	10	10	1.68%
DOT Office of Inspector General	436	3	3	0.69%	1	1	0.23%
DOT Office of the Secretary	795	11	11	1.38%	4	4	0.50%
DOT Pipeline & Hazardous Materials Safety Admin	447	8	7	1.57%	4	4	0.89%
DOT Research & Inovative Technology Administration	709	9	9	1.27%	5	5	0.71%
DOT St. Lawrence Development Corporation	129	0	0	0.00%	0	0	0.00%

Table B-1a FY 2012 Total Work Force, Counselings, and Complaints - Sub-Component Data							
Agency or Department	**Total Work Force**	**Number Completed/ Ended Counselings**	**Number Individuals with Completed/ Ended Counselings**	**Counseled Individuals as % of Total Work Force**	**Number Complaints Filed**	**Number Complainants**	**Number Complainants as % of Total Work Force**
Department of Veterans Affairs Wide	**323,154**	**4,484**	**4,060**	**1.26%**	**2,347**	**2,165**	**0.67%**
VA HQ and Others	12,448	165	152	1.22%	105	97	0.78%
VA National Cemetary Administration	1,717	50	38	2.21%	27	19	1.11%
VA Veterans Benefits Administration	20,739	295	272	1.31%	155	148	0.71%
VA Veterans Health Administration	288,250	3,974	3,598	1.25%	2,060	1,901	0.66%
Federal Housing Finance Agency Wide	**706**	**17**	**17**	**2.41%**	**9**	**9**	**1.27%**
Federal Housing Finance Agency Hqtrs	573	14	14	2.44%	9	9	1.57%
Federal Housing Finance Agency OIG	133	3	3	2.26%	0	0	0.00%
General Services Administration Wide	**12,416**	**158**	**143**	**1.15%**	**96**	**87**	**0.70%**
GSA Central Office	3,356	40	38	1.13%	21	21	0.63%
GSA National Capital Region	1,655	16	15	0.91%	9	9	0.54%
GSA Region 1	305	3	3	0.98%	1	1	0.33%
GSA Region 10	456	2	2	0.44%	2	2	0.44%
GSA Region 2	664	19	17	2.56%	14	12	1.81%
GSA Region 3	911	11	10	1.10%	4	3	0.33%
GSA Region 4	998	19	19	1.90%	12	12	1.20%
GSA Region 5	888	5	4	0.45%	4	3	0.34%
GSA Region 6	756	7	7	0.93%	3	3	0.40%
GSA Region 7	1,059	6	6	0.57%	3	3	0.28%
GSA Region 8	414	3	3	0.72%	3	3	0.72%
GSA Region 9	954	27	19	1.99%	20	15	1.57%

Table B-1a FY 2012 Total Work Force, Counselings, and Complaints - Sub-Component Data							
Agency or Department	**Total Work Force**	**Number Completed/ Ended Counselings**	**Number Individuals with Completed/ Ended Counselings**	**Counseled Individuals as % of Total Work Force**	**Number Complaints Filed**	**Number Complainants**	**Number Complainants as % of Total Work Force**
U.S. Postal Service Wide	**625,701**	**13,143**	**11,976**	**1.91%**	**4,532**	**4,272**	**0.68%**
USPS Capital Metro Area Operations	63,963	1,615	1,471	2.30%	559	538	0.84%
USPS Eastern Area	97,013	1,727	1,588	1.64%	696	649	0.67%
USPS Great Lakes Area	79,691	1,480	1,377	1.73%	517	494	0.62%
USPS Headquarters	9,976	140	129	1.29%	85	79	0.79%
USPS Northeast Area	91,597	1,554	1,441	1.57%	463	438	0.48%
USPS Office of Inspector General	1,169	21	19	1.63%	17	14	1.20%
USPS Pacific Area	66,700	1,825	1,638	2.46%	531	495	0.74%
USPS Southern Area	113,559	3,285	2,909	2.56%	1,128	1,055	0.93%
USPS Western Area	102,033	1,496	1,404	1.38%	536	510	0.50%

Table B-2 FY 2012 All Timely Completed Counselings							
Agency or Department	**Total Number Completed / Ended Counselings**	**Total Number Completed / Ended Counselings (excluding remands)**	**Number Timely within 30 Days**	**Number Timely with Written Extension**	**Number Timely with ADR Participation**	**Total Number Timely Completed / Ended Counselings**	**% Timely Completed/ Ended Counselings (excluding remands)**
Advisory Council on Historic Preservation	NRF	NRF	NRF	NRF	NRF	NRF	NRF
African Development Foundation	0	0	0	0	0	0	0.00%
Agency for International Development	34	34	16	6	1	23	67.65%
American Battle Monuments Commission	1	1	1	0	0	1	100.00%
Appalachian Regional Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Architectural & Transportation Barriers Compliance Board	0	0	0	0	0	0	0.00%
Arctic Research Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Armed Forces Retirement Home	5	5	1	3	0	4	80.00%
Barry Goldwater Scholarship and Excellence in Education Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Broadcasting Board of Governors	53	53	47	2	2	51	96.23%
Central Intelligence Agency	42	42	16	14	3	33	78.57%
Chemical Safety and Hazard Investigation Board	2	2	0	2	0	2	100.00%
Christopher Columbus Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission of Fine Arts	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission on Civil Rights	0	0	0	0	0	0	0.00%
Committee for Purchase from People Who Are Blind or Severely Disabled	0	0	0	0	0	0	0.00%
Commodity Futures Trading Commission	1	1	1	0	0	1	100.00%
Consumer Financial Protection Bureau	15	15	4	4	3	11	73.33%
Consumer Product Safety Commission	3	3	2	0	0	2	66.67%
Corporation for National and Community Service	7	7	1	2	0	3	42.86%
Court Services and Offender Supervision Agency for the District of Columbia	24	24	10	2	1	13	54.17%
Defense Army and Air Force Exchange	336	336	149	52	54	255	75.89%
Defense Commissary Agency	227	227	165	7	26	198	87.22%
Defense Contract Audit Agency	45	45	15	7	4	26	57.78%
Defense Contract Management Agency	85	85	49	0	36	85	100.00%
Defense Finance and Accounting Service	92	92	34	9	49	92	100.00%
Defense Human Resources Activity	8	8	1	0	5	6	75.00%

Table B-2 FY 2012 All Timely Completed Counselings							
Agency or Department	**Total Number Completed / Ended Counselings**	**Total Number Completed / Ended Counselings (excluding remands)**	**Number Timely within 30 Days**	**Number Timely with Written Extension**	**Number Timely with ADR Participation**	**Total Number Timely Completed / Ended Counselings**	**% Timely Completed/ Ended Counselings (excluding remands)**
Defense Information Systems Agency	30	29	24	4	1	29	100.00%
Defense Intelligence Agency	89	89	35	29	19	83	93.26%
Defense Joint Task Force National Capital Region Medical	84	84	21	26	6	53	63.10%
Defense Logistics Agency	312	312	122	23	131	276	88.46%
Defense Media Activity	3	3	2	1	0	3	100.00%
Defense Missile Defense Agency	11	11	0	3	0	3	27.27%
Defense National Geospatial-Intelligence Agency	31	31	15	10	2	27	87.10%
Defense National Guard Bureau	113	113	58	2	37	97	85.84%
Defense National Security Agency	69	69	27	28	11	66	95.65%
Defense Nuclear Facilities Safety Board	0	0	0	0	0	0	0.00%
Defense Office of the Inspector General	9	9	8	0	1	9	100.00%
Defense Office of the Secretary - Wash. Hqtrs. Services	45	45	26	11	8	45	100.00%
Defense Security Service	18	18	16	0	2	18	100.00%
Defense Technical Information Center	1	1	0	0	0	0	0.00%
Defense Threat Reduction Agency	19	19	11	2	5	18	94.74%
Defense TRICARE Management Activity	18	18	3	3	1	7	38.89%
Defense Uniformed Services University	5	5	5	0	0	5	100.00%
Department of Agriculture	975	975	255	265	193	713	73.13%
Department of Commerce	325	325	145	118	12	275	84.62%
Department of Defense Education Activity	136	136	93	15	26	134	98.53%
Department of Education	48	48	14	26	7	47	97.92%
Department of Energy	124	124	37	19	10	66	53.23%
Department of Health and Human Services	674	674	318	148	147	613	90.95%
Department of Homeland Security	2,031	2,031	627	331	760	1,718	84.59%
Department of Housing and Urban Development	106	106	30	21	17	68	64.15%
Department of Justice	1,372	1,372	569	522	151	1,242	90.52%
Department of Labor	206	206	102	0	91	193	93.69%
Department of State	271	270	143	27	29	199	73.70%
Department of the Air Force	1,002	996	337	211	349	897	90.06%

Table B-2 FY 2012 All Timely Completed Counselings							
Agency or Department	**Total Number Completed / Ended Counselings**	**Total Number Completed / Ended Counselings (excluding remands)**	**Number Timely within 30 Days**	**Number Timely with Written Extension**	**Number Timely with ADR Participation**	**Total Number Timely Completed / Ended Counselings**	**% Timely Completed/ Ended Counselings (excluding remands)**
Department of the Army	2,301	2,299	1,448	203	357	2,008	87.34%
Department of the Interior	592	592	163	183	127	473	79.90%
Department of the Navy	1,531	1,530	357	458	579	1,394	91.11%
Department of the Treasury	746	746	279	114	328	721	96.65%
Department of Transportation	541	541	187	95	224	506	93.53%
Department of Veterans Affairs	4,484	4,484	1,985	113	2,309	4,407	98.28%
Election Assistance Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Environmental Protection Agency	98	98	42	15	11	68	69.39%
Equal Employment Opportunity Commission	41	41	8	16	16	40	97.56%
Export-Import Bank of the US	2	2	2	0	0	2	100.00%
Farm Credit Administration	1	1	0	1	0	1	100.00%
Farm Credit System Insurance Corporation	0	0	0	0	0	0	0.00%
Federal Communications Commission	15	15	5	5	0	10	66.67%
Federal Deposit Insurance Corporation	82	82	35	6	39	80	97.56%
Federal Election Commission	4	4	4	0	0	4	100.00%
Federal Energy Regulatory Commission	13	13	10	3	0	13	100.00%
Federal Financial Institutions Examination Council	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Housing Finance Agency	17	16	4	1	10	15	93.75%
Federal Labor Relations Authority	3	3	1	1	1	3	100.00%
Federal Maritime Commission	3	3	3	0	0	3	100.00%
Federal Mediation and Conciliation Service	2	2	2	0	0	2	100.00%
Federal Mine Safety & Health Review Commission	0	0	0	0	0	0	0.00%
Federal Reserve System--Board of Governors	54	54	54	0	0	54	100.00%
Federal Retirement Thrift Investment Board	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Trade Commission	10	10	8	2	0	10	100.00%
General Services Administration	158	158	60	54	42	156	98.73%
Government Printing Office	70	70	53	13	0	66	94.29%
Harry S. Truman Scholarship Foundation	0	0	0	0	0	0	0.00%
Holocaust Memorial Museum U.S.	0	0	0	0	0	0	0.00%
Institute of Museum and Library Services	0	0	0	0	0	0	0.00%
Inter-American Foundation	0	0	0	0	0	0	0.00%

Table B-2 FY 2012 All Timely Completed Counselings							
Agency or Department	**Total Number Completed / Ended Counselings**	**Total Number Completed / Ended Counselings (excluding remands)**	**Number Timely within 30 Days**	**Number Timely with Written Extension**	**Number Timely with ADR Participation**	**Total Number Timely Completed / Ended Counselings**	**% Timely Completed/ Ended Counselings (excluding remands)**
International Boundary and Water Commission	2	2	2	0	0	2	100.00%
International Joint Commission: US and Canada	NRF	NRF	NRF	NRF	NRF	NRF	NRF
International Trade Commission	2	2	1	0	1	2	100.00%
James Madison Memorial Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Japan-United States Friendship Commission	0	0	0	0	0	0	0.00%
John F. Kennedy Center for the Performing Arts	2	2	2	0	0	2	100.00%
Marine Mammal Commission	0	0	0	0	0	0	0.00%
Merit Systems Protection Board	3	3	0	0	3	3	100.00%
Millennium Challenge Corporation	0	0	0	0	0	0	0.00%
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Aeronautics and Space Administration	77	77	22	22	17	61	79.22%
National Archives and Records Administration	33	33	18	2	10	30	90.91%
National Capital Planning Commission	0	0	0	0	0	0	0.00%
National Council on Disability	0	0	0	0	0	0	0.00%
National Credit Union Administration	7	7	6	1	0	7	100.00%
National Endowment for the Arts	8	8	8	0	0	8	100.00%
National Endowment for the Humanities	0	0	0	0	0	0	0.00%
National Foundation on the Arts & the Humanities	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Gallery of Art	3	3	1	2	0	3	100.00%
National Indian Gaming Commission	1	1	0	0	0	0	0.00%
National Labor Relations Board	19	19	8	7	0	15	78.95%
National Mediation Board	0	0	0	0	0	0	0.00%
National Reconnaissance Office	7	7	4	3	0	7	100.00%
National Science Foundation	15	15	8	0	6	14	93.33%
National Transportation Safety Board	3	3	3	0	0	3	100.00%
Navajo and Hopi Indian Relocation Commission	0	0	0	0	0	0	0.00%
Nuclear Regulatory Commission	35	35	16	8	9	33	94.29%
Nuclear Waste Technical Review Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Occupational Safety& Health Review Commission	0	0	0	0	0	0	0.00%
Office of Government Ethics	10	10	8	0	2	10	100.00%

Table B-2 FY 2012 All Timely Completed Counselings

Agency or Department	Total Number Completed / Ended Counselings	Total Number Completed / Ended Counselings (excluding remands)	Number Timely within 30 Days	Number Timely with Written Extension	Number Timely with ADR Participation	Total Number Timely Completed / Ended Counselings	% Timely Completed/ Ended Counselings (excluding remands)
Office of Personnel Management	88	88	75	10	2	87	98.86%
Office of Special Counsel	0	0	0	0	0	0	0.00%
Office of the Director of National Intelligence	5	5	0	5	0	5	100.00%
Overseas Private Investment Corporation	2	2	2	0	0	2	100.00%
Peace Corps	6	6	3	2	1	6	100.00%
Pension Benefit Guaranty Corporation	20	20	5	8	0	13	65.00%
Postal Regulatory Commission	1	1	1	0	0	1	100.00%
Presidio Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Railroad Retirement Board	6	6	0	4	2	6	100.00%
Securities and Exchange Commission	30	30	6	16	3	25	83.33%
Selective Service System	2	2	2	0	0	2	100.00%
Small Business Administration	75	75	45	0	5	50	66.67%
Smithsonian Institution	38	38	3	2	33	38	100.00%
Social Security Administration	917	916	338	309	224	871	95.09%
Tennessee Valley Authority	86	86	36	29	20	85	98.84%
Trade and Development Agency	0	0	0	0	0	0	0.00%
U.S. Postal Service	13,143	13,121	2,077	2,421	8,408	12,906	98.36%
Utah Reclamation Mitigation and Conservation Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Valles Caldera Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Cabinet Level Subtotal	32,258	32,225	9,952	5,507	14,522	29,981	93.04%
Midsize Agencies Subtotal	1,634	1,633	660	451	396	1,507	92.28%
Small Agencies Subtotal	615	614	343	129	69	541	88.11%
Micro Agencies Subtotal	14	14	10	2	2	14	100.00%
Government-wide	34,521	34,486	10,965	6,089	14,989	32,043	92.92%

NRF = No Report Filed

Table B-2a FY 2012 All Timely Completed Counselings - Sub-Component Data

Agency or Department	Total Number Completed / Ended Counselings	Total Number Completed / Ended Counselings (excluding remands)	Number Timely within 30 Days	Number Timely with Written Extension	Number Timely with ADR Participation	Total Number Timely Completed/ Ended Counselings	% Timely Completed/ Ended Counselings (excluding remands)
Defense Logistics Agency Wide	**312**	**312**	**122**	**23**	**131**	**276**	**88.46%**
DLA Aviation	54	54	33	1	14	48	88.89%
DLA Disposition Services	10	10	6	0	1	7	70.00%
DLA Distribution	151	151	58	9	73	140	92.72%
DLA Headquarters Operations Division	53	53	12	6	25	43	81.13%
DLA Land and Maritime	20	20	5	7	3	15	75.00%
DLA Logistics Information Service	2	2	2	0	0	2	100.00%
DLA Troop Support	22	22	6	0	15	21	95.45%
Defense National Guard Bureau Wide	**113**	**113**	**58**	**2**	**37**	**97**	**85.84%**
Alabama National Guard	1	1	1	0	0	1	100.00%
Alaska National Guard	0	0	0	0	0	0	0.00%
Arizona National Guard	6	6	3	0	3	6	100.00%
Arkansas National Guard	3	3	3	0	0	3	100.00%
California National Guard	17	17	11	1	0	12	70.59%
Colorado National Guard	1	1	1	0	0	1	100.00%
Connecticut National Guard	0	0	0	0	0	0	0.00%
DC National Guard	1	1	1	0	0	1	100.00%
Delaware National Guard	0	0	0	0	0	0	0.00%
Florida National Guard	1	1	1	0	0	1	100.00%
Georgia National Guard	0	0	0	0	0	0	0.00%
Guam National Guard	0	0	0	0	0	0	0.00%
Hawaii National Guard	0	0	0	0	0	0	0.00%
Idaho National Guard	0	0	0	0	0	0	0.00%
Illinois National Guard	0	0	0	0	0	0	0.00%
Indiana National Guard	1	1	1	0	0	1	100.00%
Iowa National Guard	34	34	3	0	30	33	97.06%

Table B-2a FY 2012 All Timely Completed Counselings - Sub-Component Data							
Agency or Department	**Total Number Completed / Ended Counselings**	**Total Number Completed / Ended Counselings (excluding remands)**	**Number Timely within 30 Days**	**Number Timely with Written Extension**	**Number Timely with ADR Participation**	**Total Number Timely Completed/ Ended Counselings**	**% Timely Completed/ Ended Counselings (excluding remands)**
Kansas National Guard	1	1	1	0	0	1	100.00%
Kentucky National Guard	0	0	0	0	0	0	0.00%
Louisiana National Guard	0	0	0	0	0	0	0.00%
Maine National Guard	0	0	0	0	0	0	0.00%
Maryland National Guard	0	0	0	0	0	0	0.00%
Massachusetts National Guard	4	4	4	0	0	4	100.00%
Michigan National Guard	5	5	1	0	2	3	60.00%
Minnesota National Guard	1	1	1	0	0	1	100.00%
Mississippi National Guard	1	1	1	0	0	1	100.00%
Missouri National Guard	1	1	1	0	0	1	100.00%
Montana National Guard	1	1	1	0	0	1	100.00%
Nebraska National Guard	0	0	0	0	0	0	0.00%
Nevada National Guard	2	2	0	1	0	1	50.00%
New Hampshire National Guard	0	0	0	0	0	0	0.00%
New Jersey National Guard	0	0	0	0	0	0	0.00%
New Mexico National Guard	0	0	0	0	0	0	0.00%
New York National Guard	6	6	0	0	0	0	0.00%
North Carolina National Guard	0	0	0	0	0	0	0.00%
North Dakota National Guard	1	1	1	0	0	1	100.00%
Ohio National Guard	0	0	0	0	0	0	0.00%
Oklahoma National Guard	0	0	0	0	0	0	0.00%
Oregon National Guard	0	0	0	0	0	0	0.00%
Pennsylvania National Guard	1	1	1	0	0	1	100.00%
Puerto Rico National Guard	6	6	6	0	0	6	100.00%
Rhode Island National Guard	0	0	0	0	0	0	0.00%
South Carolina National Guard	1	1	1	0	0	1	100.00%
South Dakota National Guard	0	0	0	0	0	0	0.00%
Tennessee National Guard	1	1	1	0	0	1	100.00%
Texas National Guard	1	1	1	0	0	1	100.00%

Table B-2a FY 2012 All Timely Completed Counselings - Sub-Component Data							
Agency or Department	**Total Number Completed / Ended Counselings**	**Total Number Completed / Ended Counselings (excluding remands)**	**Number Timely within 30 Days**	**Number Timely with Written Extension**	**Number Timely with ADR Participation**	**Total Number Timely Completed/ Ended Counselings**	**% Timely Completed/ Ended Counselings (excluding remands)**
Utah National Guard	4	4	4	0	0	4	100.00%
Vermont National Guard	0	0	0	0	0	0	0.00%
Virgin Islands National Guard	0	0	0	0	0	0	0.00%
Virginia National Guard	2	2	2	0	0	2	100.00%
Washington State National Guard	3	3	3	0	0	3	100.00%
West Virginia National Guard	4	4	2	0	2	4	100.00%
Wisconsin National Guard	0	0	0	0	0	0	0.00%
Wyoming National Guard	2	2	1	0	0	1	50.00%
Department of Agriculture Wide	**975**	**975**	**255**	**265**	**193**	**713**	**73.13%**
USDA Agricultural Marketing Service	26	26	7	5	14	26	100.00%
USDA Agricultural Research Service	40	40	13	19	6	38	95.00%
USDA Agriculture Headquarters	51	51	8	3	4	15	29.41%
USDA Animal and Plant Health Inspection Service	87	87	5	18	8	31	35.63%
USDA Economic Research Service	1	1	0	1	0	1	100.00%
USDA Farm Service Agency	47	47	21	15	9	45	95.74%
USDA Food and Nutrition Service	12	12	6	5	1	12	100.00%
USDA Food Safety And Inspection Service	180	180	79	35	57	171	95.00%
USDA Foreign Agricultural Service	13	13	1	2	3	6	46.15%
USDA Forest Service	302	302	84	139	26	249	82.45%
USDA Grain Inspection, Packers & Stockyards Admin	15	15	0	1	5	6	40.00%
USDA National Agricultural Statistics Service	4	4	2	1	1	4	100.00%
USDA National Appeals Division	0	0	0	0	0	0	0.00%
USDA National Institute of Food and Agriculture	2	2	1	1	0	2	100.00%
USDA Natural Resources Conservation Service	74	74	13	3	39	55	74.32%
USDA Office Of The Chief Financial Officer	41	41	7	14	7	28	68.29%
USDA Office Of Inspector General	10	10	2	2	3	7	70.00%
USDA Risk Management Agency	14	14	1	1	7	9	64.29%
USDA Rural Development	56	56	5	0	3	8	14.29%

Table B-2a FY 2012 All Timely Completed Counselings - Sub-Component Data							
Agency or Department	**Total Number Completed / Ended Counselings**	**Total Number Completed / Ended Counselings (excluding remands)**	**Number Timely within 30 Days**	**Number Timely with Written Extension**	**Number Timely with ADR Participation**	**Total Number Timely Completed/ Ended Counselings**	**% Timely Completed/ Ended Counselings (excluding remands)**
Department of Commerce Wide	**325**	**325**	**145**	**118**	**12**	**275**	**84.62%**
DOC All Other Commerce Bureaus	30	30	7	1	1	9	30.00%
DOC Bureau of the Census	114	114	69	34	2	105	92.11%
DOC Decennial Census	5	5	5	0	0	5	100.00%
DOC International Trade Administration	11	11	2	5	0	7	63.64%
DOC National Institute of Standards & Technology	24	24	5	18	0	23	95.83%
DOC National Oceanic & Atmospheric Administration	82	82	39	27	5	71	86.59%
DOC U. S. Patent and Trademark Office	59	59	18	33	4	55	93.22%
Department of Energy Wide	**124**	**124**	**37**	**19**	**10**	**66**	**53.23%**
DOE Bonneville Power Administration	28	28	0	4	3	7	25.00%
DOE Chicago Operations Office	1	1	1	0	0	1	100.00%
DOE EM Consolidated Business Center	4	4	0	1	0	1	25.00%
DOE Golden Field Office	5	5	4	1	0	5	100.00%
DOE Headquarters	32	32	9	0	2	11	34.38%
DOE Idaho Operations Office	3	3	1	2	0	3	100.00%
DOE National Energy Technology Lab	2	2	1	0	0	1	50.00%
DOE NNSA Service Center	21	21	6	5	1	12	57.14%
DOE Oak Ridge Operations	2	2	2	0	0	2	100.00%
DOE OSTI	0	0	0	0	0	0	0.00%
DOE Richland Operations Office	1	1	0	1	0	1	100.00%
DOE Savannah River Operations	6	6	1	0	4	5	83.33%
DOE Southeastern Power Administration	0	0	0	0	0	0	0.00%
DOE Southwestern Power Administration	3	3	2	1	0	3	100.00%
DOE Strategic Petroleum Reserve	0	0	0	0	0	0	0.00%
DOE Western Area Power Administration	16	16	10	4	0	14	87.50%

Table B-2a FY 2012 All Timely Completed Counselings - Sub-Component Data							
Agency or Department	**Total Number Completed / Ended Counselings**	**Total Number Completed / Ended Counselings (excluding remands)**	**Number Timely within 30 Days**	**Number Timely with Written Extension**	**Number Timely with ADR Participation**	**Total Number Timely Completed/ Ended Counselings**	**% Timely Completed/ Ended Counselings (excluding remands)**
Department of Health &Human Services Wide	**674**	**674**	**318**	**148**	**147**	**613**	**90.95%**
HHS Administration for Children and Families	12	12	3	2	3	8	66.67%
HHS Agency for Healthcare Research and Quality	3	3	3	0	0	3	100.00%
HHS Centers for Disease Control and Prevention	127	127	44	25	52	121	95.28%
HHS Centers for Medicare & Medicaid Services	38	38	3	24	9	36	94.74%
HHS Food and Drug Administration	123	123	55	35	32	122	99.19%
HHS Health Resources and Services Administration	20	20	6	10	4	20	100.00%
HHS Indian Health Service	198	198	104	41	27	172	86.87%
HHS National Institutes of Health	99	99	71	2	15	88	88.89%
HHS Office of the Sec. of Health& Human Srvcs	44	44	24	7	3	34	77.27%
HHS Program Support Center	7	7	4	1	1	6	85.71%
HHS Substance Abuse & Mental Health Srvcs Admin	3	3	1	1	1	3	100.00%
Department of Homeland Security Wide	**2,031**	**2,031**	**627**	**331**	**760**	**1,718**	**84.59%**
DHS Federal Emergency Management Agency	242	242	116	64	2	182	75.21%
DHS Federal Law Enforcement Training Center	18	18	9	5	4	18	100.00%
DHS Headquarters	77	77	21	29	4	54	70.13%
DHS Transportation Security Administration	658	658	123	126	309	558	84.80%
DHS U.S. Citizenship and Immigration Services	186	186	59	42	84	185	99.46%
DHS U.S. Coast Guard	96	96	55	13	26	94	97.92%
DHS U.S. Customs and Border Protection	464	464	184	1	279	464	100.00%
DHS U.S. Immigration and Customs Enforcement	242	242	15	50	51	116	47.93%
DHS U.S. Secret Service	48	48	45	1	1	47	97.92%

Table B-2a FY 2012 All Timely Completed Counselings - Sub-Component Data							
Agency or Department	**Total Number Completed / Ended Counselings**	**Total Number Completed / Ended Counselings (excluding remands)**	**Number Timely within 30 Days**	**Number Timely with Written Extension**	**Number Timely with ADR Participation**	**Total Number Timely Completed/ Ended Counselings**	**% Timely Completed/ Ended Counselings (excluding remands)**
Department of Justice Wide	**1,372**	**1,372**	**569**	**522**	**151**	**1,242**	**90.52%**
DOJ Alcohol, Tobacco, Firearms and Explosives	67	67	21	15	17	53	79.10%
DOJ Bureau of Prisons	838	838	328	394	98	820	97.85%
DOJ Drug Enforcement Administration	44	44	12	14	1	27	61.36%
DOJ Executive Office for Immigration Review	16	16	8	8	0	16	100.00%
DOJ Executive Office for U.S. Attorneys	37	37	30	0	7	37	100.00%
DOJ Federal Bureau of Investigation	221	221	91	46	13	150	67.87%
DOJ Office of Justice Programs	18	18	4	5	9	18	100.00%
DOJ Offices, Boards, and Divisions	46	46	11	20	6	37	80.43%
DOJ U.S. Marshals Service	85	85	64	20	0	84	98.82%
Department of Labor Wide	**206**	**206**	**102**	**0**	**91**	**193**	**93.69%**
DOL (DM and others)	73	73	39	0	30	69	94.52%
DOL Bureau of Labor Statistics	6	6	2	0	4	6	100.00%
DOL Employment and Training Administration	17	17	10	0	6	16	94.12%
DOL Mine Safety and Health Administration	31	31	9	0	19	28	90.32%
DOL Occupational Safety and Health Administration	22	22	11	0	9	20	90.91%
DOL Office of Workers Compensation Programs	25	25	14	0	9	23	92.00%
DOL Wage and Hour Division	32	32	17	0	14	31	96.88%
Department of the Army Wide	**2,301**	**2,299**	**1,448**	**203**	**357**	**2,008**	**87.34%**
Eighth U.S. Army (KOREA)	2	2	0	0	0	0	0.00%
Headquarters, Department of Army	171	171	117	10	24	151	88.30%
U.S. Army Corps of Engineers	248	248	154	43	19	216	87.10%

Table B-2a FY 2012 All Timely Completed Counselings - Sub-Component Data							
Agency or Department	**Total Number Completed / Ended Counselings**	**Total Number Completed / Ended Counselings (excluding remands)**	**Number Timely within 30 Days**	**Number Timely with Written Extension**	**Number Timely with ADR Participation**	**Total Number Timely Completed/ Ended Counselings**	**% Timely Completed/ Ended Counselings (excluding remands)**
U.S. Army Europe	18	18	17	0	1	18	100.00%
U.S. Army Forces Command	175	175	163	4	4	171	97.71%
U.S. Army Installation Management Command	545	544	346	51	85	482	88.60%
U.S. Army Intelligence and Security Command	22	22	13	1	4	18	81.82%
U.S. Army Material Command	508	507	276	53	119	448	88.36%
U.S. Army Medical Command	424	424	260	30	66	356	83.96%
U.S. Army Network Enterprise Technology Command	26	26	14	2	4	20	76.92%
U.S. Army Pacific (USARPAC)	2	2	1	0	1	2	100.00%
U.S. Army Space and Missile Defense Command	1	1	0	1	0	1	100.00%
U.S. Army Special Operations Command (USASOC)	16	16	6	0	6	12	75.00%
U.S. Army Test and Evaluation Command	16	16	8	0	4	12	75.00%
U.S. Army Training and Doctrine Command	127	127	73	8	20	101	79.53%
Department of the Interior Wide	**592**	**592**	**163**	**183**	**127**	**473**	**79.90%**
Bureau of Ocean Energy Management	7	7	2	0	2	4	57.14%
Bureau of Safety and Environmental Enforcement	7	7	1	0	1	2	28.57%
DOI Bureau Of Indian Affairs	56	56	3	36	17	56	100.00%
DOI Bureau Of Land Management	81	81	24	19	22	65	80.25%
DOI Bureau Of Reclamation	78	78	31	24	8	63	80.77%
DOI Fish And Wildlife Service	56	56	17	27	6	50	89.29%
DOI Geological Survey	22	22	8	8	6	22	100.00%
DOI National Park Service	208	208	61	39	37	137	65.87%
DOI Office Of Surface Mining, Reclamation & Enforce.	6	6	2	1	1	4	66.67%
DOI-Office Of The Secretary	71	71	14	29	27	70	98.59%

Table B-2a FY 2012 All Timely Completed Counselings - Sub-Component Data

Agency or Department	Total Number Completed / Ended Counselings	Total Number Completed / Ended Counselings (excluding remands)	Number Timely within 30 Days	Number Timely with Written Extension	Number Timely with ADR Participation	Total Number Timely Completed/ Ended Counselings	% Timely Completed/ Ended Counselings (excluding remands)
Department of the Navy Wide	**1,531**	**1,530**	**357**	**458**	**579**	**1,394**	**91.11%**
Chief Of Naval Operations	27	27	8	6	12	26	96.30%
Commander Naval Installations Command	270	270	59	66	124	249	92.22%
Commander Naval Reserve	0	0	0	0	0	0	0.00%
Commander Pacific Fleet	125	124	39	26	56	121	97.58%
DON Assistant for Administration	54	54	11	24	13	48	88.89%
DON Bureau of Medicine & Surgery	120	120	27	27	49	103	85.83%
DON SPAWAR	25	25	4	6	7	17	68.00%
DON Strategic Systems Project Office	7	7	0	6	1	7	100.00%
Fleet Cyber Command	16	16	5	5	5	15	93.75%
Fleet Forces Command	88	88	27	13	41	81	92.05%
Marine Corps HQ	233	233	48	91	62	201	86.27%
Military Sealift Command	56	56	3	14	38	55	98.21%
Naval Air Systems Command	162	162	44	66	43	153	94.44%
Naval Education & Training Command	31	31	3	9	15	27	87.10%
Naval Sea Systems Command	71	71	21	28	17	66	92.96%
Naval Special Warfare Command	5	5	0	2	2	4	80.00%
Naval Supply Systems Command	95	95	20	40	26	86	90.53%
Naval Systems Management Activity	0	0	0	0	0	0	0.00%
Navy Facilities & Engineering Command	118	118	33	24	53	110	93.22%
Navy Military Personnel Command	9	9	3	1	3	7	77.78%
Office Of Naval Intelligence	15	15	1	4	9	14	93.33%
Office Of Naval Research	4	4	1	0	3	4	100.00%
Department of the Treasury Wide	**746**	**746**	**279**	**114**	**328**	**721**	**96.65%**
Treas - Alcohol and Tobacco Tax and Trade Bureau	1	1	0	1	0	1	100.00%
Treas - Bureau of Engraving and Printing	31	31	24	1	3	28	90.32%
Treas - Bureau of the Public Debt	14	14	10	1	3	14	100.00%

Table B-2a FY 2012 All Timely Completed Counselings - Sub-Component Data							
Agency or Department	**Total Number Completed / Ended Counselings**	**Total Number Completed / Ended Counselings (excluding remands)**	**Number Timely within 30 Days**	**Number Timely with Written Extension**	**Number Timely with ADR Participation**	**Total Number Timely Completed/ Ended Counselings**	**% Timely Completed/ Ended Counselings (excluding remands)**
Treas - Departmental Offices	16	16	9	0	6	15	93.75%
Treas - Financial Crimes Enforcement Network	5	5	2	1	2	5	100.00%
Treas - Financial Management Service	15	15	1	0	1	2	13.33%
Treas - Inspector General For Tax Administration	2	2	2	0	0	2	100.00%
Treas - Internal Revenue Service	587	587	201	89	292	582	99.15%
Treas - Office of the Comptroller of the Currency	17	17	6	6	5	17	100.00%
Treas - Special Inspector General for the Trouble Assets Relief Program	0	0	0	0	0	0	0.00%
Treas - U. S. Mint	50	50	21	11	15	47	94.00%
Treas -Internal Revenue Service Office of the Chief Counsel	7	7	2	4	1	7	100.00%
Treas- Office of the Inspector General	1	1	1	0	0	1	100.00%
Department of Transportation Wide	**541**	**541**	**187**	**95**	**224**	**506**	**93.53%**
DOT Federal Aviation Administration	437	437	166	57	209	432	98.86%
DOT Federal Highway Administration	27	27	5	11	11	27	100.00%
DOT Federal Motor Carrier Safety Administration	8	8	0	7	1	8	100.00%
DOT Federal Railroad Administrataion	4	4	0	0	0	0	0.00%
DOT Federal Transit Administration	11	11	3	6	1	10	90.91%
DOT Maritime Administration	13	13	1	2	0	3	23.08%
DOT National Highway Traffic Safety Administration	10	10	4	3	0	7	70.00%
DOT Office of Inspector General	3	3	2	1	0	3	100.00%
DOT Office of the Secretary	11	11	5	4	2	11	100.00%
DOT Pipeline &Hazardous Materials Safety Admin	8	8	1	1	0	2	25.00%
DOT Research & Innovative Technology Administration	9	9	0	3	0	3	33.33%
DOT St. Lawrence Development Corporation	0	0	0	0	0	0	0.00%

Table B-2a FY 2012 All Timely Completed Counselings - Sub-Component Data							
Agency or Department	**Total Number Completed / Ended Counselings**	**Total Number Completed / Ended Counselings (excluding remands)**	**Number Timely within 30 Days**	**Number Timely with Written Extension**	**Number Timely with ADR Participation**	**Total Number Timely Completed/ Ended Counselings**	**% Timely Completed/ Ended Counselings (excluding remands)**
Department of Veterans Affairs Wide	**4,484**	**4,484**	**1,985**	**113**	**2,309**	**4,407**	**98.28%**
VA-HQ and Others	165	165	63	8	92	163	98.79%
VA-NCA	50	50	15	3	31	49	98.00%
VA-Veterans Benefits Administration	295	295	134	4	153	291	98.64%
VA-Veterans Health Administration	3,974	3,974	1,773	98	2,033	3,904	98.24%
Federal Housing Finance Agency Wide	**17**	**16**	**4**	**1**	**10**	**15**	**93.75%**
Federal Housing Finance Agency Hqtrs	14	13	1	1	10	12	92.31%
Federal Housing Finance Agency OIG	3	3	3	0	0	3	100.00%
General Services Administration Wide	**158**	**158**	**60**	**54**	**42**	**156**	**98.73%**
GSA Central Office	40	40	11	16	13	40	100.00%
GSA National Capital Region	16	16	5	6	5	16	100.00%
GSA Region 1	3	3	0	1	2	3	100.00%
GSA Region 10	2	2	2	0	0	2	100.00%
GSA Region 2	19	19	7	6	6	19	100.00%
GSA Region 3	11	11	4	4	3	11	100.00%
GSA Region 4	19	19	6	10	1	17	89.47%
GSA Region 5	5	5	0	5	0	5	100.00%
GSA Region 6	7	7	1	0	6	7	100.00%
GSA Region 7	6	6	4	0	2	6	100.00%
GSA Region 8	3	3	1	0	2	3	100.00%
GSA Region 9	27	27	19	6	2	27	100.00%

Table B-2a FY 2012 All Timely Completed Counselings - Sub-Component Data							
Agency or Department	**Total Number Completed / Ended Counselings**	**Total Number Completed / Ended Counselings (excluding remands)**	**Number Timely within 30 Days**	**Number Timely with Written Extension**	**Number Timely with ADR Participation**	**Total Number Timely Completed/ Ended Counselings**	**% Timely Completed/ Ended Counselings (excluding remands)**
U.S. Postal Service Wide	**13,143**	**13,121**	**2,077**	**2,421**	**8,408**	**12,906**	**98.36%**
USPS Capital Metro Area Operations	1,615	1,613	249	300	1,047	1,596	98.95%
USPS Eastern Area	1,727	1,726	251	495	940	1,686	97.68%
USPS Great Lakes Area	1,480	1,477	201	301	952	1,454	98.44%
USPS Headquarters	140	140	28	49	58	135	96.43%
USPS Northeast Area	1,554	1,553	153	354	1,015	1,522	98.00%
USPS Office of Inspector General	21	21	12	4	5	21	100.00%
USPS Pacific Area	1,825	1,823	240	185	1,379	1,804	98.96%
USPS Southern Area	3,285	3,275	733	448	2,044	3,225	98.47%
USPS Western Area	1,496	1,493	210	285	968	1,463	97.99%

Table B-3 FY 2012 Outcomes of All Pre-Complaint Closures

Agency or Department	Number Completed / Ended Counselings	Number Completed/ Ended by Settlements	% Settlements	Number Completed/ Ended by Withdrawals/No Complaints Filed	% Withdrawals/No Complaints Filed	Total Number Completed/ Ended by Resolution	% Resolutions	Number Completed/ Ended by Filing Complaint	% Complaints	Number Decision to File Complaint Pending	% Decision to File Complaint Pending
Advisory Council on Historic Preservation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
African Development Foundation	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Agency for International Development	34	1	2.94%	17	50.00%	18	52.94%	14	41.18%	2	5.88%
American Battle Monuments Commission	1	0	0.00%	0	0.00%	0	0.00%	1	100.00%	0	0.00%
Appalachian Regional Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Architectural and Transportation Barriers Compliance Board	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Arctic Research Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Armed Forces Retirement Home	5	0	0.00%	1	20.00%	1	20.00%	4	80.00%	0	0.00%
Barry Goldwater Scholarship and Excellence in Education Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Broadcasting Board of Governors	53	5	9.43%	36	67.92%	41	77.36%	12	22.64%	0	0.00%
Central Intelligence Agency	42	1	2.38%	15	35.71%	16	38.10%	26	61.90%	0	0.00%
Chemical Safety and Hazard Investigation Board	2	0	0.00%	1	50.00%	1	50.00%	1	50.00%	0	0.00%
Christopher Columbus Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission of Fine Arts	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission on Civil Rights	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Committee for Purchase from People Who Are Blind or Severely Disabled	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Commodity Futures Trading Commission	1	0	0.00%	0	0.00%	0	0.00%	1	100.00%	0	0.00%
Consumer Financial Protection Bureau	15	2	13.33%	2	13.33%	4	26.67%	11	73.33%	0	0.00%
Consumer Product Safety Commission	3	0	0.00%	0	0.00%	0	0.00%	2	66.67%	1	33.33%
Corporation for National and Community Service	7	0	0.00%	3	42.86%	3	42.86%	4	57.14%	0	0.00%
Court Services and Offender Supervision Agency for the District of Columbia	24	3	12.50%	11	45.83%	14	58.33%	10	41.67%	0	0.00%
Defense Army and Air Force Exchange	336	26	7.74%	204	60.71%	230	68.45%	98	29.17%	8	2.38%
Defense Commissary Agency	227	10	4.41%	75	33.04%	85	37.44%	138	60.79%	4	1.76%
Defense Contract Audit Agency	45	4	8.89%	10	22.22%	14	31.11%	28	62.22%	3	6.67%
Defense Contract Management Agency	85	6	7.06%	36	42.35%	42	49.41%	41	48.24%	2	2.35%
Defense Finance and Accounting Service	92	23	25.00%	29	31.52%	52	56.52%	36	39.13%	4	4.35%
Defense Human Resources Activity	8	1	12.50%	4	50.00%	5	62.50%	3	37.50%	0	0.00%
Defense Information Systems Agency	30	0	0.00%	13	43.33%	13	43.33%	17	56.67%	0	0.00%
Defense Intelligence Agency	89	7	7.87%	39	43.82%	46	51.69%	39	43.82%	4	4.49%
Defense Joint Task Force National Capital Region Medical	84	6	7.14%	45	53.57%	51	60.71%	33	39.29%	0	0.00%
Defense Logistics Agency	312	60	19.23%	132	42.31%	192	61.54%	114	36.54%	6	1.92%
Defense Media Activity	3	0	0.00%	2	66.67%	2	66.67%	1	33.33%	0	0.00%
Defense Missile Defense Agency	11	1	9.09%	3	27.27%	4	36.36%	4	36.36%	3	27.27%
Defense National Geospatial-Intelligence Agency	31	6	19.35%	7	22.58%	13	41.94%	16	51.61%	2	6.45%
Defense National Guard Bureau	113	47	41.59%	34	30.09%	81	71.68%	26	23.01%	6	5.31%
Defense National Security Agency	69	6	8.70%	43	62.32%	49	71.01%	18	26.09%	2	2.90%
Defense Nuclear Facilities Safety Board	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Defense Office of the Inspector General	9	2	22.22%	0	0.00%	2	22.22%	6	66.67%	1	11.11%

Table B-3 FY 2012 Outcomes of All Pre-Complaint Closures

Agency or Department	Number Completed / Ended Counselings	Number Completed/ Ended by Settlements	% Settlements	Number Completed/ Ended by Withdrawals/No Complaints Filed	% Withdrawals/No Complaints Filed	Total Number Completed/ Ended by Resolution	% Resolutions	Number Completed/ Ended by Filing Complaint	% Complaints	Number Decision to File Complaint Pending	% Decision to File Complaint Pending
Defense Office of the Secretary - Wash. Hqtrs. Services	45	2	4.44%	18	40.00%	20	44.44%	25	55.56%	0	0.00%
Defense Security Service	18	2	11.11%	3	16.67%	5	27.78%	8	44.44%	5	27.78%
Defense Technical Information Center	1	0	0.00%	1	100.00%	1	100.00%	0	0.00%	0	0.00%
Defense Threat Reduction Agency	19	3	15.79%	7	36.84%	10	52.63%	9	47.37%	0	0.00%
Defense TRICARE Management Activity	18	0	0.00%	8	44.44%	8	44.44%	10	55.56%	0	0.00%
Defense Uniformed Services University	5	0	0.00%	3	60.00%	3	60.00%	2	40.00%	0	0.00%
Department of Agriculture	975	97	9.95%	355	36.41%	452	46.36%	496	50.87%	27	2.77%
Department of Commerce	325	11	3.38%	85	26.15%	96	29.54%	222	68.31%	7	2.15%
Department of Defense Education Activity	136	10	7.35%	52	38.24%	62	45.59%	72	52.94%	2	1.47%
Department of Education	48	2	4.17%	13	27.08%	15	31.25%	32	66.67%	1	2.08%
Department of Energy	124	12	9.68%	37	29.84%	49	39.52%	72	58.06%	3	2.42%
Department of Health and Human Services	674	26	3.86%	168	24.93%	194	28.78%	371	55.04%	109	16.17%
Department of Homeland Security	2,031	155	7.63%	681	33.53%	836	41.16%	1,142	56.23%	53	2.61%
Department of Housing and Urban Development	106	0	0.00%	34	32.08%	34	32.08%	63	59.43%	9	8.49%
Department of Justice	1,372	82	5.98%	533	38.85%	615	44.83%	737	53.72%	20	1.46%
Department of Labor	206	12	5.83%	52	25.24%	64	31.07%	133	64.56%	9	4.37%
Department of State	271	18	6.64%	119	43.91%	137	50.55%	126	46.49%	8	2.95%
Department of the Air Force	1,002	186	18.56%	343	34.23%	529	52.79%	458	45.71%	15	1.50%
Department of the Army	2,301	264	11.47%	785	34.12%	1,049	45.59%	1,179	51.24%	73	3.17%
Department of the Interior	592	59	9.97%	176	29.73%	235	39.70%	339	57.26%	18	3.04%
Department of the Navy	1,531	228	14.89%	594	38.80%	822	53.69%	696	45.46%	13	0.85%
Department of the Treasury	746	152	20.38%	214	28.69%	366	49.06%	367	49.20%	13	1.74%
Department of Transportation	541	63	11.65%	173	31.98%	236	43.62%	292	53.97%	13	2.40%
Department of Veterans Affairs	4,484	353	7.87%	1,731	38.60%	2,084	46.48%	2,280	50.85%	120	2.68%
Election Assistance Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Environmental Protection Agency	98	4	4.08%	19	19.39%	23	23.47%	70	71.43%	5	5.10%
Equal Employment Opportunity Commission	41	2	4.88%	16	39.02%	18	43.90%	23	56.10%	0	0.00%
Export-Import Bank of the US	2	1	50.00%	0	0.00%	1	50.00%	1	50.00%	0	0.00%
Farm Credit Administration	1	0	0.00%	1	100.00%	1	100.00%	0	0.00%	0	0.00%
Farm Credit System Insurance Corporation	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Federal Communications Commission	15	0	0.00%	5	33.33%	5	33.33%	10	66.67%	0	0.00%
Federal Deposit Insurance Corporation	82	11	13.41%	23	28.05%	34	41.46%	44	53.66%	4	4.88%
Federal Election Commission	4	0	0.00%	4	100.00%	4	100.00%	0	0.00%	0	0.00%
Federal Energy Regulatory Commission	13	0	0.00%	7	53.85%	7	53.85%	6	46.15%	0	0.00%
Federal Financial Institutions Examination Council	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Housing Finance Agency	17	2	11.76%	6	35.29%	8	47.06%	9	52.94%	0	0.00%
Federal Labor Relations Authority	3	1	33.33%	1	33.33%	2	66.67%	1	33.33%	0	0.00%
Federal Maritime Commission	3	1	33.33%	0	0.00%	1	33.33%	2	66.67%	0	0.00%
Federal Mediation and Conciliation Service	2	0	0.00%	0	0.00%	0	0.00%	2	100.00%	0	0.00%
Federal Mine Safety & Health Review Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Federal Reserve System--Board of Governors	54	0	0.00%	42	77.78%	42	77.78%	12	22.22%	0	0.00%
Federal Retirement Thrift Investment Board	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Trade Commission	10	1	10.00%	9	90.00%	10	100.00%	0	0.00%	0	0.00%

Table B-3 FY 2012 Outcomes of All Pre-Complaint Closures

Agency or Department	Number Completed / Ended Counselings	Number Completed/ Ended by Settlements	% Settlements	Number Completed/ Ended by Withdrawals/No Complaints Filed	% Withdrawals/No Complaints Filed	Total Number Completed/ Ended by Resolution	% Resolutions	Number Completed/ Ended by Filing Complaint	% Complaints	Number Decision to File Complaint Pending	% Decision to File Complaint Pending
General Services Administration	158	9	5.70%	50	31.65%	59	37.34%	92	58.23%	7	4.43%
Government Printing Office	70	0	0.00%	42	60.00%	42	60.00%	27	38.57%	1	1.43%
Harry S. Truman Scholarship Foundation	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Holocaust Memorial Museum U.S.	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Institute of Museum and Library Services	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Inter-American Foundation	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
International Boundary and Water Commission	2	0	0.00%	2	100.00%	2	100.00%	0	0.00%	0	0.00%
International Joint Commission: US and Canada	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
International Trade Commission	2	0	0.00%	0	0.00%	0	0.00%	2	100.00%	0	0.00%
James Madison Memorial Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Japan-United States Friendship Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
John F. Kennedy Center for the Performing Arts	2	0	0.00%	1	50.00%	1	50.00%	1	50.00%	0	0.00%
Marine Mammal Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Merit Systems Protection Board	3	1	33.33%	1	33.33%	2	66.67%	1	33.33%	0	0.00%
Millennium Challenge Corporation	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Aeronautics and Space Administration	77	8	10.39%	30	38.96%	38	49.35%	37	48.05%	2	2.60%
National Archives and Records Administration	33	13	39.39%	16	48.48%	29	87.88%	3	9.09%	1	3.03%
National Capital Planning Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
National Council on Disability	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
National Credit Union Administration	7	0	0.00%	4	57.14%	4	57.14%	3	42.86%	0	0.00%
National Endowment for the Arts	8	0	0.00%	7	87.50%	7	87.50%	1	12.50%	0	0.00%
National Endowment for the Humanities	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
National Foundation on the Arts & the Humanities	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Gallery of Art	3	0	0.00%	1	33.33%	1	33.33%	2	66.67%	0	0.00%
National Indian Gaming Commission	1	1	100.00%	0	0.00%	1	100.00%	0	0.00%	0	0.00%
National Labor Relations Board	19	1	5.26%	9	47.37%	10	52.63%	8	42.11%	1	5.26%
National Mediation Board	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
National Reconnaissance Office	7	1	14.29%	3	42.86%	4	57.14%	3	42.86%	0	0.00%
National Science Foundation	15	2	13.33%	4	26.67%	6	40.00%	9	60.00%	0	0.00%
National Transportation Safety Board	3	0	0.00%	1	33.33%	1	33.33%	2	66.67%	0	0.00%
Navajo and Hopi Indian Relocation Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Nuclear Regulatory Commission	35	9	25.71%	10	28.57%	19	54.29%	16	45.71%	0	0.00%
Nuclear Waste Technical Review Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Occupational Safety & Health Review Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Office of Government Ethics	10	0	0.00%	10	100.00%	10	100.00%	0	0.00%	0	0.00%
Office of Personnel Management	88	1	1.14%	38	43.18%	39	44.32%	44	50.00%	5	5.68%
Office of Special Counsel	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Office of the Director of National Intelligence	5	0	0.00%	1	20.00%	1	20.00%	4	80.00%	0	0.00%
Overseas Private Investment Corporation	2	0	0.00%	2	100.00%	2	100.00%	0	0.00%	0	0.00%
Peace Corps	6	0	0.00%	2	33.33%	2	33.33%	4	66.67%	0	0.00%
Pension Benefit Guaranty Corporation	20	0	0.00%	8	40.00%	8	40.00%	12	60.00%	0	0.00%
Postal Regulatory Commission	1	0	0.00%	1	100.00%	1	100.00%	0	0.00%	0	0.00%

Table B-3 FY 2012 Outcomes of All Pre-Complaint Closures

Agency or Department	Number Completed / Ended Counselings	Number Completed/ Ended by Settlements	% Settlements	Number Completed/ Ended by Withdrawals/No Complaints Filed	% Withdrawals/No Complaints Filed	Total Number Completed/ Ended by Resolution	% Resolutions	Number Completed/ Ended by Filing Complaint	% Complaints	Number Decision to File Complaint Pending	% Decision to File Complaint Pending
Presidio Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Railroad Retirement Board	6	1	16.67%	3	50.00%	4	66.67%	2	33.33%	0	0.00%
Securities and Exchange Commission	30	0	0.00%	10	33.33%	10	33.33%	20	66.67%	0	0.00%
Selective Service System	2	0	0.00%	1	50.00%	1	50.00%	1	50.00%	0	0.00%
Small Business Administration	75	4	5.33%	34	45.33%	38	50.67%	35	46.67%	2	2.67%
Smithsonian Institution	38	1	2.63%	10	26.32%	11	28.95%	11	28.95%	16	42.11%
Social Security Administration	917	77	8.40%	343	37.40%	420	45.80%	474	51.69%	23	2.51%
Tennessee Valley Authority	86	8	9.30%	9	10.47%	17	19.77%	58	67.44%	11	12.79%
Trade and Development Agency	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
U.S. Postal Service	13,143	3,239	24.64%	5,363	40.80%	8,602	65.45%	4,324	32.90%	217	1.65%
Utah Reclamation Mitigation and Conservation Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Valles Caldera Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Cabinet Level Subtotal	32,258	5,181	16.06%	12,224	37.89%	17,405	53.96%	14,073	43.63%	780	2.42%
Midsize Agencies Subtotal	1,634	125	7.65%	558	34.15%	683	41.80%	876	53.61%	75	4.59%
Small Agencies Subtotal	615	47	7.64%	302	49.11%	349	56.75%	260	42.28%	6	0.98%
Micro Agencies Subtotal	14	0	0.00%	12	80.00%	12	80.00%	2	13.33%	1	6.67%
Government-wide	34,521	5,353	15.51%	13,096	37.94%	18,449	53.44%	15,211	44.06%	862	2.50%

NRF = No Report Filed

Table B-3a FY 2012 Outcomes of All Pre-Complaint Closures - Sub-Component Data

Agency or Department	Number Completed / Ended Counselings	Number Completed/ Ended by Settlements	% Settlements	Number Completed/ Ended by Withdrawals/No Complaints Filed	% Withdrawals/No Complaints Filed	Total Number Completed/ Ended by Resolution	% Resolutions	Number Completed/ Ended by Filing Complaint	% Complaints	Number Decision to File Complaint Pending	% Decision to File Complaint Pending
Defense Logistics Agency Wide	**312**	**60**	**19.23%**	**132**	**42.31%**	**192**	**61.54%**	**114**	**36.54%**	**6**	**1.92%**
DLA Aviation	54	9	16.67%	21	38.89%	30	55.56%	22	40.74%	2	3.70%
DLA Disposition Services	10	0	0.00%	7	70.00%	7	70.00%	3	30.00%	0	0.00%
DLA Distribution	151	33	21.85%	70	46.36%	103	68.21%	47	31.13%	1	0.66%
DLA Headquarters Operations Division	53	7	13.21%	16	30.19%	23	43.40%	27	50.94%	3	5.66%
DLA Land and Maritime	20	1	5.00%	8	40.00%	9	45.00%	11	55.00%	0	0.00%
DLA Logistics Information Service	2	1	50.00%	1	50.00%	2	100.00%	0	0.00%	0	0.00%
DLA Troop Support	22	9	40.91%	9	40.91%	18	81.82%	4	18.18%	0	0.00%
Defense National Guard Bureau Wide	**113**	**47**	**41.59%**	**34**	**30.09%**	**81**	**71.68%**	**26**	**23.01%**	**6**	**5.31%**
Alabama National Guard	1	0	0.00%	1	100.00%	1	100.00%	0	0.00%	0	0.00%
Alaska National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Arizona National Guard	6	3	50.00%	0	0.00%	3	50.00%	2	33.33%	1	16.67%
Arkansas National Guard	3	3	100.00%	0	0.00%	3	100.00%	0	0.00%	0	0.00%
California National Guard	17	0	0.00%	8	47.06%	8	47.06%	8	47.06%	1	5.88%
Colorado National Guard	1	0	0.00%	0	0.00%	0	0.00%	1	100.00%	0	0.00%
Connecticut National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
DC National Guard	1	0	0.00%	0	0.00%	0	0.00%	1	100.00%	0	0.00%
Delaware National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Florida National Guard	1	0	0.00%	0	0.00%	0	0.00%	1	100.00%	0	0.00%
Georgia National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Guam National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Hawaii National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Idaho National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Illinois National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Indiana National Guard	1	0	0.00%	0	0.00%	0	0.00%	1	100.00%	0	0.00%
Iowa National Guard	34	30	88.24%	4	11.76%	34	100.00%	0	0.00%	0	0.00%
Kansas National Guard	1	0	0.00%	1	100.00%	1	100.00%	0	0.00%	0	0.00%
Kentucky National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Louisiana National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Maine National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Maryland National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Massachusetts National Guard	4	4	100.00%	0	0.00%	4	100.00%	0	0.00%	0	0.00%
Michigan National Guard	5	1	20.00%	1	20.00%	2	40.00%	1	20.00%	2	40.00%
Minnesota National Guard	1	0	0.00%	1	100.00%	1	100.00%	0	0.00%	0	0.00%
Mississippi National Guard	1	0	0.00%	1	100.00%	1	100.00%	0	0.00%	0	0.00%
Missouri National Guard	1	0	0.00%	0	0.00%	0	0.00%	1	100.00%	0	0.00%
Montana National Guard	1	0	0.00%	1	100.00%	1	100.00%	0	0.00%	0	0.00%
Nebraska National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Nevada National Guard	2	0	0.00%	0	0.00%	0	0.00%	2	100.00%	0	0.00%

Table B-3a FY 2012 Outcomes of All Pre-Complaint Closures - Sub-Component Data

Agency or Department	Number Completed / Ended Counselings	Number Completed/ Ended by Settlements	% Settlements	Number Completed/ Ended by Withdrawals/No Complaints Filed	% Withdrawals/No Complaints Filed	Total Number Completed/ Ended by Resolution	% Resolutions	Number Completed/ Ended by Filing Complaint	% Complaints	Number Decision to File Complaint Pending	% Decision to File Complaint Pending
New Hampshire National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
New Jersey National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
New Mexico National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
New York National Guard	6	0	0.00%	4	66.67%	4	66.67%	2	33.33%	0	0.00%
North Carolina National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
North Dakota National Guard	1	0	0.00%	1	100.00%	1	100.00%	0	0.00%	0	0.00%
Ohio National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Oklahoma National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Oregon National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Pennsylvania National Guard	1	0	0.00%	1	100.00%	1	100.00%	0	0.00%	0	0.00%
Puerto Rico National Guard	6	0	0.00%	6	100.00%	6	100.00%	0	0.00%	0	0.00%
Rhode Island National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
South Carolina National Guard	1	0	0.00%	0	0.00%	0	0.00%	1	100.00%	0	0.00%
South Dakota National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Tennessee National Guard	1	0	0.00%	0	0.00%	0	0.00%	1	100.00%	0	0.00%
Texas National Guard	1	0	0.00%	0	0.00%	0	0.00%	1	100.00%	0	0.00%
Utah National Guard	4	3	75.00%	0	0.00%	3	75.00%	1	25.00%	0	0.00%
Vermont National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Virgin Islands National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Virginia National Guard	2	0	0.00%	2	100.00%	2	100.00%	0	0.00%	0	0.00%
Washington State National Guard	3	1	33.33%	0	0.00%	1	33.33%	2	66.67%	0	0.00%
West Virginia National Guard	4	2	50.00%	0	0.00%	2	50.00%	0	0.00%	2	50.00%
Wisconsin National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Wyoming National Guard	2	0	0.00%	2	100.00%	2	100.00%	0	0.00%	0	0.00%
Department of Agriculture Wide	**975**	**97**	**9.95%**	**355**	**36.41%**	**452**	**46.36%**	**496**	**50.87%**	**27**	**2.77%**
USDA Agricultural Marketing Service	26	4	15.38%	1	3.85%	5	19.23%	21	80.77%	0	0.00%
USDA Agricultural Research Service	40	5	12.50%	5	12.50%	10	25.00%	29	72.50%	1	2.50%
USDA Agriculture Headquarters	51	7	13.73%	17	33.33%	24	47.06%	27	52.94%	0	0.00%
USDA Animal and Plant Health Inspection Service	87	6	6.90%	32	36.78%	38	43.68%	47	54.02%	2	2.30%
USDA Economic Research Service	1	0	0.00%	0	0.00%	0	0.00%	1	100.00%	0	0.00%
USDA Farm Service Agency	47	8	17.02%	16	34.04%	24	51.06%	22	46.81%	1	2.13%
USDA Food and Nutrition Service	12	1	8.33%	3	25.00%	4	33.33%	7	58.33%	1	8.33%
USDA Food Safety And Inspection Service	180	22	12.22%	95	52.78%	117	65.00%	61	33.89%	2	1.11%
USDA Foreign Agricultural Service	13	2	15.38%	1	7.69%	3	23.08%	10	76.92%	0	0.00%
USDA Forest Service	302	13	4.30%	120	39.74%	133	44.04%	161	53.31%	8	2.65%
USDA Grain Inspection, Packers & Stockyards Admin	15	3	20.00%	3	20.00%	6	40.00%	9	60.00%	0	0.00%
USDA National Agricultural Statistics Service	4	0	0.00%	3	75.00%	3	75.00%	1	25.00%	0	0.00%
USDA National Appeals Division	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
USDA National Institute of Food and Agriculture	2	0	0.00%	1	50.00%	1	50.00%	1	50.00%	0	0.00%

Table B-3a FY 2012 Outcomes of All Pre-Complaint Closures - Sub-Component Data

Agency or Department	Number Completed / Ended Counselings	Number Completed/ Ended by Settlements	% Settlements	Number Completed/ Ended by Withdrawals/No Complaints Filed	% Withdrawals/No Complaints Filed	Total Number Completed/ Ended by Resolution	% Resolutions	Number Completed/ Ended by Filing Complaint	% Complaints	Number Decision to File Complaint Pending	% Decision to File Complaint Pending
USDA Natural Resources Conservation Service	74	9	12.16%	21	28.38%	30	40.54%	38	51.35%	6	8.11%
USDA Office Of The Chief Financial Officer	41	6	14.63%	13	31.71%	19	46.34%	22	53.66%	0	0.00%
USDA - Office Of Inspector General	10	1	10.00%	2	20.00%	3	30.00%	7	70.00%	0	0.00%
USDA Risk Management Agency	14	4	28.57%	3	21.43%	7	50.00%	5	35.71%	2	14.29%
USDA Rural Development	56	6	10.71%	19	33.93%	25	44.64%	27	48.21%	4	7.14%
Department of Commerce Wide	**325**	**11**	**3.38%**	**85**	**26.15%**	**96**	**29.54%**	**222**	**68.31%**	**7**	**2.15%**
DOC All Other Commerce Bureaus	30	3	10.00%	3	10.00%	6	20.00%	24	80.00%	0	0.00%
DOC Bureau of the Census	114	2	1.75%	40	35.09%	42	36.84%	67	58.77%	5	4.39%
DOC Decennial Census	5	0	0.00%	1	20.00%	1	20.00%	4	80.00%	0	0.00%
DOC International Trade Administration	11	3	27.27%	3	27.27%	6	54.55%	5	45.45%	0	0.00%
DOC National Institute of Standards & Technology	24	2	8.33%	8	33.33%	10	41.67%	13	54.17%	1	4.17%
DOC National Oceanic & Atmospheric Admin	82	1	1.22%	16	19.51%	17	20.73%	65	79.27%	0	0.00%
DOC U. S. Patent and Trademark Office	59	0	0.00%	14	23.73%	14	23.73%	44	74.58%	1	1.69%
Department of Energy Wide	**124**	**12**	**9.68%**	**37**	**29.84%**	**49**	**39.52%**	**72**	**58.06%**	**3**	**2.42%**
DOE Bonneville Power Administration	28	2	7.14%	15	53.57%	17	60.71%	11	39.29%	0	0.00%
DOE Chicago Operations Office	1	0	0.00%	0	0.00%	0	0.00%	1	100.00%	0	0.00%
DOE EM Consolidated Business Center	4	1	25.00%	1	25.00%	2	50.00%	2	50.00%	0	0.00%
DOE Golden Field Office	5	0	0.00%	2	40.00%	2	40.00%	2	40.00%	1	20.00%
DOE Headquarters	32	4	12.50%	6	18.75%	10	31.25%	20	62.50%	2	6.25%
DOE Idaho Operations Office	3	0	0.00%	2	66.67%	2	66.67%	1	33.33%	0	0.00%
DOE National Energy Technology Lab	2	0	0.00%	0	0.00%	0	0.00%	2	100.00%	0	0.00%
DOE NNSA Service Center	21	3	14.29%	1	4.76%	4	19.05%	17	80.95%	0	0.00%
DOE Oak Ridge Operations	2	0	0.00%	0	0.00%	0	0.00%	2	100.00%	0	0.00%
DOE OSTI	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
DOE Richland Operations Office	1	0	0.00%	1	100.00%	1	100.00%	0	0.00%	0	0.00%
DOE Savannah River Operations	6	1	16.67%	2	33.33%	3	50.00%	3	50.00%	0	0.00%
DOE Southeastern Power Administration	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
DOE Southwestern Power Administration	3	0	0.00%	2	66.67%	2	66.67%	1	33.33%	0	0.00%
DOE Strategic Petroleum Reserve	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
DOE Western Area Power Administration	16	1	6.25%	5	31.25%	6	37.50%	10	62.50%	0	0.00%

Table B-3a FY 2012 Outcomes of All Pre-Complaint Closures - Sub-Component Data

Agency or Department	Number Completed / Ended Counselings	Number Completed/ Ended by Settlements	% Settlements	Number Completed/ Ended by Withdrawals/No Complaints Filed	% Withdrawals/No Complaints Filed	Total Number Completed/ Ended by Resolution	% Resolutions	Number Completed/ Ended by Filing Complaint	% Complaints	Number Decision to File Complaint Pending	% Decision to File Complaint Pending
Department of Health and Human Services Wide	**674**	**26**	**3.86%**	**168**	**24.93%**	**194**	**28.78%**	**371**	**55.04%**	**109**	**16.17%**
HHS Administration for Children and Families	12	2	16.67%	1	8.33%	3	25.00%	9	75.00%	0	0.00%
HHS Agency for Healthcare Research and Quality	3	0	0.00%	1	33.33%	1	33.33%	2	66.67%	0	0.00%
HHS Centers for Disease Control and Prevention	127	2	1.57%	41	32.28%	43	33.86%	81	63.78%	3	2.36%
HHS Centers for Medicare & Medicaid Services	38	0	0.00%	14	36.84%	14	36.84%	22	57.89%	2	5.26%
HHS Food and Drug Administration	123	5	4.07%	51	41.46%	56	45.53%	64	52.03%	3	2.44%
HHS Health Resources& Services Administration	20	4	20.00%	4	20.00%	8	40.00%	12	60.00%	0	0.00%
HHS Indian Health Service	198	11	5.56%	11	5.56%	22	11.11%	79	39.90%	97	48.99%
HHS National Institutes of Health	99	0	0.00%	29	29.29%	29	29.29%	68	68.69%	2	2.02%
HHS Office of the Sec of Health& Human Srvcs	44	2	4.55%	16	36.36%	18	40.91%	24	54.55%	2	4.55%
HHS Program Support Center	7	0	0.00%	0	0.00%	0	0.00%	7	100.00%	0	0.00%
HHS Substance Abuse & Mental Health Srvcs Admin	3	0	0.00%	0	0.00%	0	0.00%	3	100.00%	0	0.00%
Department of Homeland Security Wide	**2,031**	**155**	**7.63%**	**681**	**33.53%**	**836**	**41.16%**	**1,142**	**56.23%**	**53**	**2.61%**
DHS Federal Emergency Management Agency	242	7	2.89%	101	41.74%	108	44.63%	129	53.31%	5	2.07%
DHS Federal Law Enforcement Training Center	18	3	16.67%	3	16.67%	6	33.33%	11	61.11%	1	5.56%
DHS Headquarters	77	1	1.30%	20	25.97%	21	27.27%	55	71.43%	1	1.30%
DHS Transportation Security Administration	658	68	10.33%	202	30.70%	270	41.03%	373	56.69%	15	2.28%
DHS U.S. Citizenship and Immigration Services	186	20	10.75%	48	25.81%	68	36.56%	113	60.75%	5	2.69%
DHS U.S. Coast Guard	96	17	17.71%	36	37.50%	53	55.21%	41	42.71%	2	2.08%
DHS U.S. Customs and Border Protection	464	24	5.17%	184	39.66%	208	44.83%	243	52.37%	13	2.80%
DHS U.S. Immigration and Customs Enforcement	242	15	6.20%	73	30.17%	88	36.36%	148	61.16%	6	2.48%
DHS U.S. Secret Service	48	0	0.00%	14	29.17%	14	29.17%	29	60.42%	5	10.42%
Department of Justice Wide	**1,372**	**82**	**5.98%**	**533**	**38.85%**	**615**	**44.83%**	**737**	**53.72%**	**20**	**1.46%**
DOJ Alcohol, Tobacco, Firearms and Explosives	67	6	8.96%	19	28.36%	25	37.31%	40	59.70%	2	2.99%
DOJ Bureau of Prisons	838	50	5.97%	366	43.68%	416	49.64%	415	49.52%	7	0.84%
DOJ Drug Enforcement Administration	44	2	4.55%	12	27.27%	14	31.82%	28	63.64%	2	4.55%
DOJ Executive Office for Immigration Review	16	0	0.00%	1	6.25%	1	6.25%	14	87.50%	1	6.25%
DOJ Executive Office for U.S. Attorneys	37	3	8.11%	10	27.03%	13	35.14%	24	64.86%	0	0.00%
DOJ Federal Bureau of Investigation	221	12	5.43%	77	34.84%	89	40.27%	130	58.82%	2	0.90%
DOJ Office of Justice Programs	18	1	5.56%	2	11.11%	3	16.67%	15	83.33%	0	0.00%
DOJ Offices, Boards, and Divisions	46	8	17.39%	16	34.78%	24	52.17%	21	45.65%	1	2.17%
DOJ U.S. Marshals Service	85	0	0.00%	30	35.29%	30	35.29%	50	58.82%	5	5.88%

Table B-3a FY 2012 Outcomes of All Pre-Complaint Closures - Sub-Component Data											
Agency or Department	**Number Completed / Ended Counselings**	**Number Completed/ Ended by Settlements**	**% Settlements**	**Number Completed/ Ended by Withdrawals/No Complaints Filed**	**% Withdrawals/No Complaints Filed**	**Total Number Completed/ Ended by Resolution**	**% Resolutions**	**Number Completed/ Ended by Filing Complaint**	**% Complaints**	**Number Decision to File Complaint Pending**	**% Decision to File Complaint Pending**
Department of Labor Wide	**206**	**12**	**5.83%**	**52**	**25.24%**	**64**	**31.07%**	**133**	**64.56%**	**9**	**4.37%**
DOL (DM and others)	73	5	6.85%	22	30.14%	27	36.99%	42	57.53%	4	5.48%
DOL Bureau of Labor Statistics	6	0	0.00%	0	0.00%	0	0.00%	6	100.00%	0	0.00%
DOL Employment and Training Administration	17	0	0.00%	1	5.88%	1	5.88%	15	88.24%	1	5.88%
DOL Mine Safety and Health Administration	31	5	16.13%	8	25.81%	13	41.94%	16	51.61%	2	6.45%
DOL Occupational Safety and Health Administration	22	1	4.55%	6	27.27%	7	31.82%	15	68.18%	0	0.00%
DOL Office of Workers Compensation Programs	25	1	4.00%	8	32.00%	9	36.00%	15	60.00%	1	4.00%
DOL Wage and Hour Division	32	0	0.00%	7	21.88%	7	21.88%	24	75.00%	1	3.13%
Department of the Army Wide	**2,301**	**264**	**11.47%**	**785**	**34.12%**	**1,049**	**45.59%**	**1,179**	**51.24%**	**73**	**3.17%**
Eighth U.S. Army (KOREA)	2	0	0.00%	0	0.00%	0	0.00%	2	100.00%	0	0.00%
Headquarters, Department of Army	171	15	8.77%	55	32.16%	70	40.94%	95	55.56%	6	3.51%
U.S. Army Corps of Engineers	248	26	10.48%	77	31.05%	103	41.53%	138	55.65%	7	2.82%
U.S. Army Europe	18	2	11.11%	10	55.56%	12	66.67%	6	33.33%	0	0.00%
U.S. Army Forces Command	175	5	2.86%	80	45.71%	85	48.57%	83	47.43%	7	4.00%
U.S. Army Installation Management Command	545	67	12.29%	189	34.68%	256	46.97%	275	50.46%	14	2.57%
U.S. Army Intelligence and Security Command	22	1	4.55%	6	27.27%	7	31.82%	14	63.64%	1	4.55%
U.S. Army Material Command	508	57	11.22%	168	33.07%	225	44.29%	267	52.56%	16	3.15%
U.S. Army Medical Command	424	58	13.68%	147	34.67%	205	48.35%	201	47.41%	18	4.25%
U.S. Army Network Enterprise Technology Command	26	2	7.69%	6	23.08%	8	30.77%	17	65.38%	1	3.85%
U.S. Army Pacific (USARPAC)	2	0	0.00%	0	0.00%	0	0.00%	2	100.00%	0	0.00%
U.S. Army Space and Missile Defense Command	1	0	0.00%	0	0.00%	0	0.00%	1	100.00%	0	0.00%
U.S. Army Special Operations Command (USASOC)	16	6	37.50%	3	18.75%	9	56.25%	7	43.75%	0	0.00%
U.S. Army Test and Evaluation Command	16	4	25.00%	3	18.75%	7	43.75%	9	56.25%	0	0.00%
U.S. Army Training and Doctrine Command	127	21	16.54%	41	32.28%	62	48.82%	62	48.82%	3	2.36%
Department of the Interior Wide	**592**	**59**	**9.97%**	**176**	**29.73%**	**235**	**39.70%**	**339**	**57.26%**	**18**	**3.04%**
Bureau of Ocean Energy Management	7	0	0.00%	2	28.57%	2	28.57%	4	57.14%	1	14.29%
Bureau of Safety and Environmental Enforcement	7	0	0.00%	0	0.00%	0	0.00%	7	100.00%	0	0.00%
DOI Bureau Of Indian Affairs	56	1	1.79%	18	32.14%	19	33.93%	33	58.93%	4	7.14%
DOI Bureau Of Land Management	81	9	11.11%	25	30.86%	34	41.98%	46	56.79%	1	1.23%
DOI Bureau Of Reclamation	78	4	5.13%	22	28.21%	26	33.33%	50	64.10%	2	2.56%
DOI Fish And Wildlife Service	56	9	16.07%	12	21.43%	21	37.50%	35	62.50%	0	0.00%
DOI Geological Survey	22	2	9.09%	6	27.27%	8	36.36%	13	59.09%	1	4.55%
DOI National Park Service	208	27	12.98%	71	34.13%	98	47.12%	107	51.44%	3	1.44%
DOI Office Of Surface Mining, Reclamation & Enforce.	6	0	0.00%	1	16.67%	1	16.67%	5	83.33%	0	0.00%
DOI-Office Of The Secretary	71	7	9.86%	19	26.76%	26	36.62%	39	54.93%	6	8.45%

Table B-3a FY 2012 Outcomes of All Pre-Complaint Closures - Sub-Component Data

Agency or Department	Number Completed / Ended Counselings	Number Completed/ Ended by Settlements	% Settlements	Number Completed/ Ended by Withdrawals/No Complaints Filed	% Withdrawals/No Complaints Filed	Total Number Completed/ Ended by Resolution	% Resolutions	Number Completed/ Ended by Filing Complaint	% Complaints	Number Decision to File Complaint Pending	% Decision to File Complaint Pending
Department of the Navy Wide	**1,531**	**228**	**14.89%**	**594**	**38.80%**	**822**	**53.69%**	**696**	**45.46%**	**13**	**0.85%**
Chief Of Naval Operations	27	2	7.41%	13	48.15%	15	55.56%	12	44.44%	0	0.00%
Commander Naval Installations Command	270	56	20.74%	102	37.78%	158	58.52%	111	41.11%	1	0.37%
Commander Naval Reserve	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Commander Pacific Fleet	125	23	18.40%	59	47.20%	82	65.60%	41	32.80%	2	1.60%
DON Assistant for Administration	54	7	12.96%	18	33.33%	25	46.30%	29	53.70%	0	0.00%
DON Bureau of Medicine & Surgery	120	23	19.17%	47	39.17%	70	58.33%	50	41.67%	0	0.00%
DON SPAWAR	25	6	24.00%	10	40.00%	16	64.00%	8	32.00%	1	4.00%
DON Strategic Systems Project Office	7	0	0.00%	0	0.00%	0	0.00%	7	100.00%	0	0.00%
Fleet Cyber Command	16	2	12.50%	8	50.00%	10	62.50%	6	37.50%	0	0.00%
Fleet Forces Command	88	14	15.91%	34	38.64%	48	54.55%	39	44.32%	1	1.14%
Marine Corps HQ	233	34	14.59%	100	42.92%	134	57.51%	99	42.49%	0	0.00%
Military Sealift Command	56	0	0.00%	19	33.93%	19	33.93%	37	66.07%	0	0.00%
Naval Air Systems Command	162	18	11.11%	64	39.51%	82	50.62%	80	49.38%	0	0.00%
Naval Education & Training Command	31	7	22.58%	6	19.35%	13	41.94%	14	45.16%	4	12.90%
Naval Sea Systems Command	71	6	8.45%	28	39.44%	34	47.89%	36	50.70%	1	1.41%
Naval Special Warfare Command	5	1	20.00%	0	0.00%	1	20.00%	3	60.00%	1	20.00%
Naval Supply Systems Command	95	13	13.68%	38	40.00%	51	53.68%	44	46.32%	0	0.00%
Naval Systems Management Activity	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Navy Facilities & Engineering Command	118	15	12.71%	44	37.29%	59	50.00%	57	48.31%	2	1.69%
Navy Military Personnel Command	9	1	11.11%	1	11.11%	2	22.22%	7	77.78%	0	0.00%
Office Of Naval Intelligence	15	0	0.00%	2	13.33%	2	13.33%	13	86.67%	0	0.00%
Office Of Naval Research	4	0	0.00%	1	25.00%	1	25.00%	3	75.00%	0	0.00%
Department of the Treasury Wide	**746**	**152**	**20.38%**	**214**	**28.69%**	**366**	**49.06%**	**367**	**49.20%**	**13**	**1.74%**
Treas - Alcohol and Tobacco Tax and Trade Bureau	1	0	0.00%	0	0.00%	0	0.00%	1	100.00%	0	0.00%
Treas - Bureau of Engraving and Printing	31	0	0.00%	9	29.03%	9	29.03%	22	70.97%	0	0.00%
Treas - Bureau of the Public Debt	14	2	14.29%	8	57.14%	10	71.43%	4	28.57%	0	0.00%
Treas - Departmental Offices	16	3	18.75%	4	25.00%	7	43.75%	9	56.25%	0	0.00%
Treas - Financial Crimes Enforcement Network	5	1	20.00%	2	40.00%	3	60.00%	2	40.00%	0	0.00%
Treas - Financial Management Service	15	1	6.67%	2	13.33%	3	20.00%	12	80.00%	0	0.00%
Treas - Inspector General For Tax Administration	2	0	0.00%	0	0.00%	0	0.00%	2	100.00%	0	0.00%
Treas - Internal Revenue Service	587	132	22.49%	173	29.47%	305	51.96%	272	46.34%	10	1.70%
Treas - Office of the Comptroller of the Currency	17	2	11.76%	6	35.29%	8	47.06%	6	35.29%	3	17.65%
Treas - Special Inspector General for the Trouble Assets Relief Program	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Treas - U. S. Mint	50	9	18.00%	8	16.00%	17	34.00%	33	66.00%	0	0.00%
Treas -Internal Revenue Service Office of the Chief Counsel	7	2	28.57%	2	28.57%	4	57.14%	3	42.86%	0	0.00%
Treas- Office of the Inspector General	1	0	0.00%	0	0.00%	0	0.00%	1	100.00%	0	0.00%

Table B-3a FY 2012 Outcomes of All Pre-Complaint Closures - Sub-Component Data

Agency or Department	Number Completed / Ended Counselings	Number Completed/ Ended by Settlements	% Settlements	Number Completed/ Ended by Withdrawals/No Complaints Filed	% Withdrawals/No Complaints Filed	Total Number Completed/ Ended by Resolution	% Resolutions	Number Completed/ Ended by Filing Complaint	% Complaints	Number Decision to File Complaint Pending	% Decision to File Complaint Pending
Department of Transportation Wide	**541**	**63**	**11.65%**	**173**	**31.98%**	**236**	**43.62%**	**292**	**53.97%**	**13**	**2.40%**
DOT Federal Aviation Administration	437	55	12.59%	135	30.89%	190	43.48%	235	53.78%	12	2.75%
DOT Federal Highway Administration	27	6	22.22%	12	44.44%	18	66.67%	9	33.33%	0	0.00%
DOT Federal Motor Carrier Safety Administration	8	1	12.50%	2	25.00%	3	37.50%	5	62.50%	0	0.00%
DOT Federal Railroad Administrataion	4	0	0.00%	1	25.00%	1	25.00%	3	75.00%	0	0.00%
DOT Federal Transit Administration	11	1	9.09%	3	27.27%	4	36.36%	7	63.64%	0	0.00%
DOT Maritime Administration	13	0	0.00%	3	23.08%	3	23.08%	9	69.23%	1	7.69%
DOT National Highway Traffic Safety Administration	10	0	0.00%	0	0.00%	0	0.00%	10	100.00%	0	0.00%
DOT Office of Inspector General	3	0	0.00%	2	66.67%	2	66.67%	1	33.33%	0	0.00%
DOT Office of the Secretary	11	0	0.00%	7	63.64%	7	63.64%	4	36.36%	0	0.00%
DOT Pipeline& Hazardous Materials Safety Admin	8	0	0.00%	4	50.00%	4	50.00%	4	50.00%	0	0.00%
DOT Research & Innovative Technology Administration	9	0	0.00%	4	44.44%	4	44.44%	5	55.56%	0	0.00%
DOT St. Lawrence Development Corporation	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Department of Veterans Affairs Wide	**4,484**	**353**	**7.87%**	**1,731**	**38.60%**	**2,084**	**46.48%**	**2,280**	**50.85%**	**120**	**2.68%**
VA-HQ and Others	165	10	6.06%	53	32.12%	63	38.18%	99	60.00%	3	1.82%
VA-NCA	50	5	10.00%	15	30.00%	20	40.00%	27	54.00%	3	6.00%
VA-Veterans Benefits Administration	295	28	9.49%	101	34.24%	129	43.73%	153	51.86%	13	4.41%
VA-Veterans Health Administration	3,974	310	7.80%	1,562	39.31%	1,872	47.11%	2,001	50.35%	101	2.54%
Federal Housing Finance Agency Wide	**17**	**2**	**11.76%**	**6**	**35.29%**	**8**	**47.06%**	**9**	**52.94%**	**0**	**0.00%**
Federal Housing Finance Agency Hqtrs	14	1	7.14%	4	28.57%	5	35.71%	9	64.29%	0	0.00%
Federal Housing Finance Agency OIG	3	1	33.33%	2	66.67%	3	100.00%	0	0.00%	0	0.00%
General Services Administration Wide	**158**	**9**	**5.70%**	**50**	**31.65%**	**59**	**37.34%**	**92**	**58.23%**	**7**	**4.43%**
GSA Central Office	40	3	7.50%	15	37.50%	18	45.00%	19	47.50%	3	7.50%
GSA National Capital Region	16	0	0.00%	9	56.25%	9	56.25%	7	43.75%	0	0.00%
GSA Region 1	3	0	0.00%	2	66.67%	2	66.67%	1	33.33%	0	0.00%
GSA Region 10	2	0	0.00%	0	0.00%	0	0.00%	2	100.00%	0	0.00%
GSA Region 2	19	1	5.26%	4	21.05%	5	26.32%	14	73.68%	0	0.00%
GSA Region 3	11	1	9.09%	2	18.18%	3	27.27%	4	36.36%	4	36.36%
GSA Region 4	19	0	0.00%	7	36.84%	7	36.84%	12	63.16%	0	0.00%
GSA Region 5	5	1	20.00%	0	0.00%	1	20.00%	4	80.00%	0	0.00%
GSA Region 6	7	3	42.86%	1	14.29%	4	57.14%	3	42.86%	0	0.00%
GSA Region 7	6	0	0.00%	3	50.00%	3	50.00%	3	50.00%	0	0.00%
GSA Region 8	3	0	0.00%	0	0.00%	0	0.00%	3	100.00%	0	0.00%
GSA Region 9	27	0	0.00%	7	25.93%	7	25.93%	20	74.07%	0	0.00%

Table B-3a FY 2012 Outcomes of All Pre-Complaint Closures - Sub-Component Data

Agency or Department	Number Completed / Ended Counselings	Number Completed/ Ended by Settlements	% Settlements	Number Completed/ Ended by Withdrawals/No Complaints Filed	% Withdrawals/No Complaints Filed	Total Number Completed/ Ended by Resolution	% Resolutions	Number Completed/ Ended by Filing Complaint	% Complaints	Number Decision to File Complaint Pending	% Decision to File Complaint Pending
U.S. Postal Service Wide	**13,143**	**3,239**	**24.64%**	**5,363**	**40.80%**	**8,602**	**65.45%**	**4,324**	**32.90%**	**217**	**1.65%**
USPS Capital Metro Area Operations	1,615	381	23.59%	671	41.55%	1,052	65.14%	535	33.13%	28	1.73%
USPS Eastern Area	1,727	238	13.78%	782	45.28%	1,020	59.06%	674	39.03%	33	1.91%
USPS Great Lakes Area	1,480	313	21.15%	645	43.58%	958	64.73%	493	33.31%	29	1.96%
USPS Headquarters	140	13	9.29%	44	31.43%	57	40.71%	81	57.86%	2	1.43%
USPS Northeast Area	1,554	345	22.20%	742	47.75%	1,087	69.95%	436	28.06%	31	1.99%
USPS Office of Inspector General	21	2	9.52%	4	19.05%	6	28.57%	15	71.43%	0	0.00%
USPS Pacific Area	1,825	675	36.99%	624	34.19%	1,299	71.18%	505	27.67%	21	1.15%
USPS Southern Area	3,285	887	27.00%	1,278	38.90%	2,165	65.91%	1,071	32.60%	49	1.49%
USPS Western Area	1,496	385	25.74%	573	38.30%	958	64.04%	514	34.36%	24	1.60%

Table B-4 FY 2012 Pre-Complaint ADR Offers, Rejections, and Acceptances

Agency or Department	Number Completed / Ended Counselings	Number Completed / Ended Counselings Offered ADR	% Completed / Ended Counselings Offered ADR (Offer Rate)	Number Offers Rejected by Individual	Total Completed / Ended Counselings Accepted/Participated in ADR Program	% Completed / Ended Counselings Accepted into ADR Program (Participation Rate)
Advisory Council on Historic Preservation	NRF	NRF	NRF	NRF	NRF	NRF
African Development Foundation	0	0	0.00%	0	0	0.00%
Agency for International Development	34	29	85.29%	24	5	14.71%
American Battle Monuments Commission	1	1	100.00%	1	0	0.00%
Appalachian Regional Commission	NRF	NRF	NRF	NRF	NRF	NRF
Architectural and Transportation Barriers Compliance Board	0	0	0.00%	0	0	0.00%
Arctic Research Commission	NRF	NRF	NRF	NRF	NRF	NRF
Armed Forces Retirement Home	5	4	80.00%	4	0	0.00%
Barry Goldwater Scholarship and Excellence in Education Foundation	NRF	NRF	NRF	NRF	NRF	NRF
Broadcasting Board of Governors	53	53	100.00%	51	2	3.77%
Central Intelligence Agency	42	38	90.48%	28	10	23.81%
Chemical Safety and Hazard Investigation Board	2	2	100.00%	2	0	0.00%
Christopher Columbus Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF
Commission of Fine Arts	NRF	NRF	NRF	NRF	NRF	NRF
Commission on Civil Rights	0	0	0.00%	0	0	0.00%
Committee for Purchase from People Who Are Blind or Severely Disabled	0	0	0.00%	0	0	0.00%
Commodity Futures Trading Commission	1	1	100.00%	1	0	0.00%
Consumer Financial Protection Bureau	15	13	86.67%	6	7	46.67%
Consumer Product Safety Commission	3	3	100.00%	2	1	33.33%
Corporation for National and Community Service	7	0	0.00%	0	0	0.00%
Court Services and Offender Supervision Agency for the District of Columbia	24	9	37.50%	5	4	16.67%
Defense Army and Air Force Exchange	336	336	100.00%	254	76	22.62%
Defense Commissary Agency	227	184	81.06%	62	122	53.74%
Defense Contract Audit Agency	45	7	15.56%	2	5	11.11%
Defense Contract Management Agency	85	38	44.71%	2	36	42.35%
Defense Finance and Accounting Service	92	71	77.17%	16	55	59.78%
Defense Human Resources Activity	8	7	87.50%	1	6	75.00%

Table B-4 FY 2012 Pre-Complaint ADR Offers, Rejections, and Acceptances

Agency or Department	Number Completed / Ended Counselings	Number Completed / Ended Counselings Offered ADR	% Completed / Ended Counselings Offered ADR (Offer Rate)	Number Offers Rejected by Individual	Total Completed / Ended Counselings Accepted/Participated in ADR Program	% Completed / Ended Counselings Accepted into ADR Program (Participation Rate)
Defense Information Systems Agency	30	30	100.00%	29	1	3.33%
Defense Intelligence Agency	89	78	87.64%	55	23	25.84%
Defense Joint Task Force National Capital Region Medical	84	84	100.00%	67	17	20.24%
Defense Logistics Agency	312	297	95.19%	106	191	61.22%
Defense Media Activity	3	2	66.67%	2	0	0.00%
Defense Missile Defense Agency	11	4	36.36%	3	1	9.09%
Defense National Geospatial-Intelligence Agency	31	29	93.55%	25	4	12.90%
Defense National Guard Bureau	113	83	73.45%	36	47	41.59%
Defense National Security Agency	69	69	100.00%	58	11	15.94%
Defense Nuclear Facilities Safety Board	0	0	0.00%	0	0	0.00%
Defense Office of the Inspector General	9	9	100.00%	7	2	22.22%
Defense Office of the Secretary - Wash. Hqtrs. Services	45	9	20.00%	0	9	20.00%
Defense Security Service	18	7	38.89%	5	2	11.11%
Defense Technical Information Center	1	1	100.00%	1	0	0.00%
Defense Threat Reduction Agency	19	19	100.00%	12	7	36.84%
Defense TRICARE Management Activity	18	15	83.33%	14	1	5.56%
Defense Uniformed Services University	5	0	0.00%	0	0	0.00%
Department of Agriculture	975	749	76.82%	494	255	26.15%
Department of Commerce	325	92	28.31%	55	37	11.38%
Department of Defense Education Activity	136	52	38.24%	23	29	21.32%
Department of Education	48	43	89.58%	33	10	20.83%
Department of Energy	124	79	63.71%	50	29	23.39%
Department of Health and Human Services	674	645	95.70%	443	202	29.97%
Department of Homeland Security	2,031	1,631	80.31%	695	936	46.09%
Department of Housing and Urban Development	106	106	100.00%	85	21	19.81%
Department of Justice	1,372	1,164	84.84%	922	242	17.64%
Department of Labor	206	206	100.00%	102	104	50.49%
Department of State	271	184	67.90%	119	65	23.99%
Department of the Air Force	1,002	743	74.15%	304	439	43.81%

Table B-4 FY 2012 Pre-Complaint ADR Offers, Rejections, and Acceptances

Agency or Department	Number Completed / Ended Counselings	Number Completed / Ended Counselings Offered ADR	% Completed / Ended Counselings Offered ADR (Offer Rate)	Number Offers Rejected by Individual	Total Completed / Ended Counselings Accepted/Participated in ADR Program	% Completed / Ended Counselings Accepted into ADR Program (Participation Rate)
Department of the Army	2,301	995	43.24%	442	553	24.03%
Department of the Interior	592	464	78.38%	309	155	26.18%
Department of the Navy	1,531	1,527	99.74%	753	774	50.56%
Department of the Treasury	746	727	97.45%	298	429	57.51%
Department of Transportation	541	366	67.65%	124	242	44.73%
Department of Veterans Affairs	4,484	4,416	98.48%	1,836	2,580	57.54%
Election Assistance Commission	NRF	NRF	NRF	NRF	NRF	NRF
Environmental Protection Agency	98	83	84.69%	55	28	28.57%
Equal Employment Opportunity Commission	41	38	92.68%	21	17	41.46%
Export-Import Bank of the US	2	2	100.00%	2	0	0.00%
Farm Credit Administration	1	1	100.00%	1	0	0.00%
Farm Credit System Insurance Corporation	0	0	0.00%	0	0	0.00%
Federal Communications Commission	15	0	0.00%	0	0	0.00%
Federal Deposit Insurance Corporation	82	71	86.59%	32	39	47.56%
Federal Election Commission	4	4	100.00%	4	0	0.00%
Federal Energy Regulatory Commission	13	0	0.00%	0	0	0.00%
Federal Financial Institutions Examination Council	NRF	NRF	NRF	NRF	NRF	NRF
Federal Housing Finance Agency	17	16	94.12%	3	13	76.47%
Federal Labor Relations Authority	3	3	100.00%	2	1	33.33%
Federal Maritime Commission	3	3	100.00%	3	0	0.00%
Federal Mediation and Conciliation Service	2	0	0.00%	0	0	0.00%
Federal Mine Safety & Health Review Commission	0	0	0.00%	0	0	0.00%
Federal Reserve System--Board of Governors	54	54	100.00%	53	1	1.85%
Federal Retirement Thrift Investment Board	NRF	NRF	NRF	NRF	NRF	NRF
Federal Trade Commission	10	10	100.00%	10	0	0.00%
General Services Administration	158	146	92.41%	80	66	41.77%
Government Printing Office	70	70	100.00%	70	0	0.00%
Harry S. Truman Scholarship Foundation	0	0	0.00%	0	0	0.00%
Holocaust Memorial Museum U.S.	0	0	0.00%	0	0	0.00%
Institute of Museum and Library Services	0	0	0.00%	0	0	0.00%
Inter-American Foundation	0	0	0.00%	0	0	0.00%

Table B-4 FY 2012 Pre-Complaint ADR Offers, Rejections, and Acceptances

Agency or Department	Number Completed / Ended Counselings	Number Completed / Ended Counselings Offered ADR	% Completed / Ended Counselings Offered ADR (Offer Rate)	Number Offers Rejected by Individual	Total Completed / Ended Counselings Accepted/Participated in ADR Program	% Completed / Ended Counselings Accepted into ADR Program (Participation Rate)
International Boundary and Water Commission	2	2	100.00%	2	0	0.00%
International Joint Commission: US & Canada	NRF	NRF	NRF	NRF	NRF	NRF
International Trade Commission	2	2	100.00%	1	1	50.00%
James Madison Memorial Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF
Japan-United States Friendship Commission	0	0	0.00%	0	0	0.00%
John F. Kennedy Center for the Performing Arts	2	2	100.00%	2	0	0.00%
Marine Mammal Commission	0	0	0.00%	0	0	0.00%
Merit Systems Protection Board	3	3	100.00%	0	3	100.00%
Millennium Challenge Corporation	0	0	0.00%	0	0	0.00%
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation	NRF	NRF	NRF	NRF	NRF	NRF
National Aeronautics and Space Administration	77	33	42.86%	12	21	27.27%
National Archives and Records Administration	33	24	72.73%	14	10	30.30%
National Capital Planning Commission	0	0	0.00%	0	0	0.00%
National Council on Disability	0	0	0.00%	0	0	0.00%
National Credit Union Administration	7	7	100.00%	7	0	0.00%
National Endowment for the Arts	8	1	12.50%	0	1	12.50%
National Endowment for the Humanities	0	0	0.00%	0	0	0.00%
National Foundation on the Arts & the Humanities	NRF	NRF	NRF	NRF	NRF	NRF
National Gallery of Art	3	3	100.00%	3	0	0.00%
National Indian Gaming Commission	1	1	100.00%	0	1	100.00%
National Labor Relations Board	19	18	94.74%	16	2	10.53%
National Mediation Board	0	0	0.00%	0	0	0.00%
National Reconnaissance Office	7	4	57.14%	2	2	28.57%
National Science Foundation	15	13	86.67%	6	7	46.67%
National Transportation Safety Board	3	2	66.67%	2	0	0.00%
Navajo and Hopi Indian Relocation Commission	0	0	0.00%	0	0	0.00%
Nuclear Regulatory Commission	35	35	100.00%	26	9	25.71%
Nuclear Waste Technical Review Commission	NRF	NRF	NRF	NRF	NRF	NRF
Occupational Safety & Health Review Commission	0	0	0.00%	0	0	0.00%
Office of Government Ethics	10	10	100.00%	0	10	100.00%

Table B-4 FY 2012 Pre-Complaint ADR Offers, Rejections, and Acceptances

Agency or Department	Number Completed / Ended Counselings	Number Completed / Ended Counselings Offered ADR	% Completed / Ended Counselings Offered ADR (Offer Rate)	Number Offers Rejected by Individual	Total Completed / Ended Counselings Accepted/Participated in ADR Program	% Completed / Ended Counselings Accepted into ADR Program (Participation Rate)
Office of Personnel Management	88	80	90.91%	71	9	10.23%
Office of Special Counsel	0	0	0.00%	0	0	0.00%
Office of the Director of National Intelligence	5	4	80.00%	4	0	0.00%
Overseas Private Investment Corporation	2	0	0.00%	0	0	0.00%
Peace Corps	6	6	100.00%	5	1	16.67%
Pension Benefit Guaranty Corporation	20	20	100.00%	19	1	5.00%
Postal Regulatory Commission	1	0	0.00%	0	0	0.00%
Presidio Trust	NRF	NRF	NRF	NRF	NRF	NRF
Railroad Retirement Board	6	4	66.67%	2	2	33.33%
Securities and Exchange Commission	30	16	53.33%	12	4	13.33%
Selective Service System	2	0	0.00%	0	0	0.00%
Small Business Administration	75	8	10.67%	0	8	10.67%
Smithsonian Institution	38	38	100.00%	5	33	86.84%
Social Security Administration	917	786	85.71%	380	406	44.27%
Tennessee Valley Authority	86	78	90.70%	58	20	23.26%
Trade and Development Agency	0	0	0.00%	0	0	0.00%
U.S. Postal Service	13,143	12,155	92.48%	2,975	9,180	69.85%
Utah Reclamation Mitigation and Conservation Commission	NRF	NRF	NRF	NRF	NRF	NRF
Valles Caldera Trust	NRF	NRF	NRF	NRF	NRF	NRF
Cabinet Level Subtotal	32,258	27,723	85.94%	10,819	16,898	52.38%
Midsize Agencies Subtotal	1,634	1,336	81.76%	699	637	38.98%
Small Agencies Subtotal	615	505	82.11%	407	98	15.93%
Micro Agencies Subtotal	15	13	86.67%	3	10	66.67%
Government-wide	34,521	29,577	85.68%	11,928	17,643	51.11%

NRF = No Report Filed

Table B-5 FY 2012 ADR Pre-Complaint Resolutions (Informal Phase)							
Agency or Department	**Number ADR Closures**	**Number ADR Settlements**	**% ADR Settlements**	**Number ADR Withdrawals/ No Complaints Filed**	**% ADR Withdrawals No Complaints Filed**	**Number ADR Resolutions**	**% ADR Resolutions (Resolution Rate)**
Advisory Council on Historic Preservation	NRF	NRF	NRF	NRF	NRF	NRF	NRF
African Development Foundation	0	0	0.00%	0	0.00%	0	0.00%
Agency for International Development	5	1	20.00%	3	60.00%	4	80.00%
American Battle Monuments Commission	0	0	0.00%	0	0.00%	0	0.00%
Appalachian Regional Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Architectural and Transportation Barriers Compliance Board	0	0	0.00%	0	0.00%	0	0.00%
Arctic Research Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Armed Forces Retirement Home	0	0	0.00%	0	0.00%	0	0.00%
Barry Goldwater Scholarship and Excellence in Education Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Broadcasting Board of Governors	2	0	0.00%	2	100.00%	2	100.00%
Central Intelligence Agency	10	0	0.00%	4	40.00%	4	40.00%
Chemical Safety and Hazard Investigation Board	0	0	0.00%	0	0.00%	0	0.00%
Christopher Columbus Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission of Fine Arts	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission on Civil Rights	0	0	0.00%	0	0.00%	0	0.00%
Committee for Purchase from People Who Are Blind or Severely Disabled	0	0	0.00%	0	0.00%	0	0.00%
Commodity Futures Trading Commission	0	0	0.00%	0	0.00%	0	0.00%
Consumer Financial Protection Bureau	7	2	28.57%	1	14.29%	3	42.86%
Consumer Product Safety Commission	1	0	0.00%	0	0.00%	0	0.00%
Corporation for National and Community Service	0	0	0.00%	0	0.00%	0	0.00%
Court Services and Offender Supervision Agency for the District of Columbia	4	2	50.00%	2	50.00%	4	100.00%
Defense Army and Air Force Exchange	76	18	23.68%	33	43.42%	51	67.11%
Defense Commissary Agency	122	9	7.38%	33	27.05%	42	34.43%
Defense Contract Audit Agency	5	4	80.00%	1	20.00%	5	100.00%
Defense Contract Management Agency	36	4	11.11%	15	41.67%	19	52.78%
Defense Finance and Accounting Service	55	22	40.00%	14	25.45%	36	65.45%
Defense Human Resources Activity	6	1	16.67%	3	50.00%	4	66.67%
Defense Information Systems Agency	1	0	0.00%	1	100.00%	1	100.00%

Table B-5 FY 2012 ADR Pre-Complaint Resolutions (Informal Phase)							
Agency or Department	**Number ADR Closures**	**Number ADR Settlements**	**% ADR Settlements**	**Number ADR Withdrawals/ No Complaints Filed**	**% ADR Withdrawals No Complaints Filed**	**Number ADR Resolutions**	**% ADR Resolutions (Resolution Rate)**
Defense Intelligence Agency	23	7	30.43%	12	52.17%	19	82.61%
Defense Joint Task Force National Capital Region Medical	17	6	35.29%	2	11.76%	8	47.06%
Defense Logistics Agency	191	58	30.37%	80	41.88%	138	72.25%
Defense Media Activity	0	0	0.00%	0	0.00%	0	0.00%
Defense Missile Defense Agency	1	0	0.00%	1	100.00%	1	100.00%
Defense National Geospatial-Intelligence Agency	4	2	50.00%	1	25.00%	3	75.00%
Defense National Guard Bureau	47	37	78.72%	6	12.77%	43	91.49%
Defense National Security Agency	11	6	54.55%	2	18.18%	8	72.73%
Defense Nuclear Facilities Safety Board	0	0	0.00%	0	0.00%	0	0.00%
Defense Office of the Inspector General	2	1	50.00%	0	0.00%	1	50.00%
Defense Office of the Secretary - Wash. Hqtrs. Services	9	2	22.22%	2	22.22%	4	44.44%
Defense Security Service	2	2	100.00%	0	0.00%	2	100.00%
Defense Technical Information Center	0	0	0.00%	0	0.00%	0	0.00%
Defense Threat Reduction Agency	7	3	42.86%	3	42.86%	6	85.71%
Defense TRICARE Management Activity	1	0	0.00%	1	100.00%	1	100.00%
Defense Uniformed Services University	0	0	0.00%	0	0.00%	0	0.00%
Department of Agriculture	255	55	21.57%	78	30.59%	133	52.16%
Department of Commerce	37	7	18.92%	12	32.43%	19	51.35%
Department of Defense Education Activity	29	7	24.14%	9	31.03%	16	55.17%
Department of Education	10	1	10.00%	5	50.00%	6	60.00%
Department of Energy	29	5	17.24%	4	13.79%	9	31.03%
Department of Health and Human Services	202	16	7.92%	52	25.74%	68	33.66%
Department of Homeland Security	936	137	14.64%	303	32.37%	440	47.01%
Department of Housing and Urban Development	21	0	0.00%	5	23.81%	5	23.81%
Department of Justice	242	54	22.31%	58	23.97%	112	46.28%
Department of Labor	104	12	11.54%	15	14.42%	27	25.96%
Department of State	65	10	15.38%	16	24.62%	26	40.00%
Department of the Air Force	439	162	36.90%	59	13.44%	221	50.34%
Department of the Army	553	175	31.65%	177	32.01%	352	63.65%
Department of the Interior	155	32	20.65%	43	27.74%	75	48.39%

Table B-5 FY 2012 ADR Pre-Complaint Resolutions (Informal Phase)							
Agency or Department	**Number ADR Closures**	**Number ADR Settlements**	**% ADR Settlements**	**Number ADR Withdrawals/ No Complaints Filed**	**% ADR Withdrawals No Complaints Filed**	**Number ADR Resolutions**	**% ADR Resolutions (Resolution Rate)**
Department of the Navy	774	203	26.23%	262	33.85%	465	60.08%
Department of the Treasury	429	138	32.17%	104	24.24%	242	56.41%
Department of Transportation	242	54	22.31%	71	29.34%	125	51.65%
Department of Veterans Affairs	2,580	319	12.36%	886	34.34%	1,205	46.71%
Election Assistance Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Environmental Protection Agency	28	2	7.14%	2	7.14%	4	14.29%
Equal Employment Opportunity Commission	17	1	5.88%	4	23.53%	5	29.41%
Export-Import Bank of the US	0	0	0.00%	0	0.00%	0	0.00%
Farm Credit Administration	0	0	0.00%	0	0.00%	0	0.00%
Farm Credit System Insurance Corporation	0	0	0.00%	0	0.00%	0	0.00%
Federal Communications Commission	0	0	0.00%	0	0.00%	0	0.00%
Federal Deposit Insurance Corporation	39	9	23.08%	6	15.38%	15	38.46%
Federal Election Commission	0	0	0.00%	0	0.00%	0	0.00%
Federal Energy Regulatory Commission	0	0	0.00%	0	0.00%	0	0.00%
Federal Financial Institutions Examination Council	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Housing Finance Agency	13	2	15.38%	4	30.77%	6	46.15%
Federal Labor Relations Authority	1	0	0.00%	1	100.00%	1	100.00%
Federal Maritime Commission	0	0	0.00%	0	0.00%	0	0.00%
Federal Mediation and Conciliation Service	0	0	0.00%	0	0.00%	0	0.00%
Federal Mine Safety &Health Review Commission	0	0	0.00%	0	0.00%	0	0.00%
Federal Reserve System--Board of Governors	1	0	0.00%	0	0.00%	0	0.00%
Federal Retirement Thrift Investment Board	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Trade Commission	0	0	0.00%	0	0.00%	0	0.00%
General Services Administration	66	5	7.58%	22	33.33%	27	40.91%
Government Printing Office	0	0	0.00%	0	0.00%	0	0.00%
Harry S. Truman Scholarship Foundation	0	0	0.00%	0	0.00%	0	0.00%
Holocaust Memorial Museum U.S.	0	0	0.00%	0	0.00%	0	0.00%
Institute of Museum and Library Services	0	0	0.00%	0	0.00%	0	0.00%
Inter-American Foundation	0	0	0.00%	0	0.00%	0	0.00%
International Boundary and Water Commission	0	0	0.00%	0	0.00%	0	0.00%
International Joint Commission: US and Canada	NRF	NRF	NRF	NRF	NRF	NRF	NRF
International Trade Commission	1	0	0.00%	0	0.00%	0	0.00%

Table B-5 FY 2012 ADR Pre-Complaint Resolutions (Informal Phase)							
Agency or Department	**Number ADR Closures**	**Number ADR Settlements**	**% ADR Settlements**	**Number ADR Withdrawals/ No Complaints Filed**	**% ADR Withdrawals No Complaints Filed**	**Number ADR Resolutions**	**% ADR Resolutions (Resolution Rate)**
James Madison Memorial Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Japan-United States Friendship Commission	0	0	0.00%	0	0.00%	0	0.00%
John F. Kennedy Center for the Performing Arts	0	0	0.00%	0	0.00%	0	0.00%
Marine Mammal Commission	0	0	0.00%	0	0.00%	0	0.00%
Merit Systems Protection Board	3	1	33.33%	0	0.00%	1	33.33%
Millennium Challenge Corporation	0	0	0.00%	0	0.00%	0	0.00%
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Aeronautics and Space Administration	21	6	28.57%	7	33.33%	13	61.90%
National Archives and Records Administration	10	7	70.00%	2	20.00%	9	90.00%
National Capital Planning Commission	0	0	0.00%	0	0.00%	0	0.00%
National Council on Disability	0	0	0.00%	0	0.00%	0	0.00%
National Credit Union Administration	0	0	0.00%	0	0.00%	0	0.00%
National Endowment for the Arts	1	0	0.00%	0	0.00%	0	0.00%
National Endowment for the Humanities	0	0	0.00%	0	0.00%	0	0.00%
National Foundation on the Arts &the Humanities	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Gallery of Art	0	0	0.00%	0	0.00%	0	0.00%
National Indian Gaming Commission	1	1	100.00%	0	0.00%	1	100.00%
National Labor Relations Board	2	0	0.00%	1	50.00%	1	50.00%
National Mediation Board	0	0	0.00%	0	0.00%	0	0.00%
National Reconnaissance Office	2	1	50.00%	1	50.00%	2	100.00%
National Science Foundation	7	2	28.57%	0	0.00%	2	28.57%
National Transportation Safety Board	0	0	0.00%	0	0.00%	0	0.00%
Navajo and Hopi Indian Relocation Commission	0	0	0.00%	0	0.00%	0	0.00%
Nuclear Regulatory Commission	9	5	55.56%	1	11.11%	6	66.67%
Nuclear Waste Technical Review Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Occupational Safety& Health Review Commission	0	0	0.00%	0	0.00%	0	0.00%
Office of Government Ethics	10	0	0.00%	10	100.00%	10	100.00%
Office of Personnel Management	9	1	11.11%	8	88.89%	9	100.00%
Office of Special Counsel	0	0	0.00%	0	0.00%	0	0.00%
Office of the Director of National Intelligence	0	0	0.00%	0	0.00%	0	0.00%
Overseas Private Investment Corporation	0	0	0.00%	0	0.00%	0	0.00%

Table B-5 FY 2012 ADR Pre-Complaint Resolutions (Informal Phase)							
Agency or Department	**Number ADR Closures**	**Number ADR Settlements**	**% ADR Settlements**	**Number ADR Withdrawals/ No Complaints Filed**	**% ADR Withdrawals No Complaints Filed**	**Number ADR Resolutions**	**% ADR Resolutions (Resolution Rate)**
Peace Corps	1	0	0.00%	0	0.00%	0	0.00%
Pension Benefit Guaranty Corporation	1	0	0.00%	0	0.00%	0	0.00%
Postal Regulatory Commission	0	0	0.00%	0	0.00%	0	0.00%
Presidio Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Railroad Retirement Board	2	1	50.00%	1	50.00%	2	100.00%
Securities and Exchange Commission	4	0	0.00%	0	0.00%	0	0.00%
Selective Service System	0	0	0.00%	0	0.00%	0	0.00%
Small Business Administration	8	3	37.50%	2	25.00%	5	62.50%
Smithsonian Institution	33	1	3.03%	10	30.30%	11	33.33%
Social Security Administration	406	62	15.27%	61	15.02%	123	30.30%
Tennessee Valley Authority	20	1	5.00%	0	0.00%	1	5.00%
Trade and Development Agency	0	0	0.00%	0	0.00%	0	0.00%
U.S. Postal Service	9,180	3,119	33.98%	3,786	41.24%	6,905	75.22%
Utah Reclamation Mitigation and Conservation Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Valles Caldera Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Cabinet Level Subtotal	16,898	4,688	27.74%	6,155	36.42%	10,843	64.17%
Midsize Agencies Subtotal	637	92	14.44%	119	18.68%	211	33.12%
Small Agencies Subtotal	98	24	24.49%	26	26.53%	50	51.02%
Micro Agencies Subtotal	10	0	0.00%	10	100.00%	10	100.00%
Government-wide	17,643	4,804	27.23%	6,310	35.76%	11,114	62.99%

NRF = No Report Filed

Table B-6 FY 2012 Benefits Provided in All Pre-Complaint Settlements									
Agency or Department	**Total Number Completed/ Ended Counselings**	**Total Number Settlements**	**Number Completed/ Ended Counselings with Non-Monetary Benefits**	**% Completed/ Ended Counselings with Non-Monetary Benefits**	**Number Completed/ Ended Counselings with Monetary Benefits**	**% Completed/ Ended Counselings with Monetary Benefits**	**Total Amount of Monetary Benefits**	**Average Monetary Benefits Per Total Settlements**	**Ave Monetary Benefits Per Settlements With Monetary Benefits**
Advisory Council on Historic Preservation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
African Development Foundation	0	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Agency for International Development	34	1	1	100.00%	1	100.00%	$6,000.00	$6,000.00	$6,000.00
American Battle Monuments Commission	1	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Appalachian Regional Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Architectural and Transportation Barriers Compliance Board	0	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Arctic Research Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Armed Forces Retirement Home	5	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Barry Goldwater Scholarship and Excellence in Education Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Broadcasting Board of Governors	53	5	5	100.00%	1	20.00%	$1,000.00	$200.00	$1,000.00
Central Intelligence Agency	42	1	1	100.00%	0	0.00%	$0.00	$0.00	$0.00
Chemical Safety and Hazard Investigation Board	2	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Christopher Columbus Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission of Fine Arts	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission on Civil Rights	0	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Committee for Purchase from People Who Are Blind or Severely Disabled	0	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Commodity Futures Trading Commission	1	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Consumer Financial Protection Bureau	15	2	2	100.00%	0	0.00%	$0.00	$0.00	$0.00
Consumer Product Safety Commission	3	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Corporation for National and Community Service	7	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Court Services and Offender Supervision Agency for the District of Columbia	24	3	3	100.00%	0	0.00%	$0.00	$0.00	$0.00
Defense Army and Air Force Exchange	336	26	23	88.46%	3	11.54%	$2,569.06	$98.81	$856.35
Defense Commissary Agency	227	10	10	100.00%	0	0.00%	$0.00	$0.00	$0.00
Defense Contract Audit Agency	45	4	4	100.00%	0	0.00%	$0.00	$0.00	$0.00
Defense Contract Management Agency	85	6	5	83.33%	2	33.33%	$11,900.00	$1,983.33	$5,950.00
Defense Finance and Accounting Service	92	23	23	100.00%	1	4.35%	$340.00	$14.78	$340.00
Defense Human Resources Activity	8	1	1	100.00%	0	0.00%	$0.00	$0.00	$0.00
Defense Information Systems Agency	30	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Defense Intelligence Agency	89	7	7	100.00%	2	28.57%	$15,000.00	$2,142.86	$7,500.00
Defense Joint Task Force National Capital Region Medical	84	6	6	100.00%	0	0.00%	$0.00	$0.00	$0.00

Table B-6 FY 2012 Benefits Provided in All Pre-Complaint Settlements									
Agency or Department	**Total Number Completed/ Ended Counselings**	**Total Number Settlements**	**Number Completed/ Ended Counselings with Non-Monetary Benefits**	**% Completed/ Ended Counselings with Non-Monetary Benefits**	**Number Completed/ Ended Counselings with Monetary Benefits**	**% Completed/ Ended Counselings with Monetary Benefits**	**Total Amount of Monetary Benefits**	**Average Monetary Benefits Per Total Settlements**	**Ave Monetary Benefits Per Settlements With Monetary Benefits**
Defense Logistics Agency	312	60	58	96.67%	5	8.33%	$9,052.64	$150.88	$1,810.53
Defense Media Activity	3	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Defense Missile Defense Agency	11	1	1	100.00%	0	0.00%	$0.00	$0.00	$0.00
Defense National Geospatial-Intelligence Agency	31	6	6	100.00%	3	50.00%	$35,203.80	$5,867.30	$11,734.60
Defense National Guard Bureau	113	47	47	100.00%	0	0.00%	$0.00	$0.00	$0.00
Defense National Security Agency	69	6	5	83.33%	1	16.67%	$500.00	$83.33	$500.00
Defense Nuclear Facilities Safety Board	0	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Defense Office of the Inspector General	9	2	1	50.00%	1	50.00%	$15,000.00	$7,500.00	$15,000.00
Defense Office of the Secretary - Wash. Hqtrs. Services	45	2	2	100.00%	0	0.00%	$0.00	$0.00	$0.00
Defense Security Service	18	2	2	100.00%	0	0.00%	$0.00	$0.00	$0.00
Defense Technical Information Center	1	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Defense Threat Reduction Agency	19	3	2	66.67%	1	33.33%	$2,000.00	$666.67	$2,000.00
Defense TRICARE Management Activity	18	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Defense Uniformed Services University	5	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Department of Agriculture	975	97	87	89.69%	29	29.90%	$341,933.32	$3,525.09	$11,790.80
Department of Commerce	325	11	11	100.00%	1	9.09%	$25,000.00	$2,272.73	$25,000.00
Department of Defense Education Activity	136	10	9	90.00%	1	10.00%	$1,380.20	$138.02	$1,380.20
Department of Education	48	2	2	100.00%	0	0.00%	$0.00	$0.00	$0.00
Department of Energy	124	12	11	91.67%	1	8.33%	$5,418.00	$451.50	$5,418.00
Department of Health and Human Services	674	26	24	92.31%	2	7.69%	$60,583.75	$2,330.14	$30,291.88
Department of Homeland Security	2,031	155	152	98.06%	19	12.26%	$544,996.21	$3,516.10	$28,684.01
Department of Housing and Urban Development	106	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Department of Justice	1,372	82	73	89.02%	22	26.83%	$315,868.64	$3,852.06	$14,357.67
Department of Labor	206	12	10	83.33%	2	16.67%	$23,500.00	$1,958.33	$11,750.00
Department of State	271	18	18	100.00%	0	0.00%	$0.00	$0.00	$0.00
Department of the Air Force	1,002	186	186	100.00%	18	9.68%	$172,541.20	$927.64	$9,585.62
Department of the Army	2,301	264	248	93.94%	41	15.53%	$208,167.58	$788.51	$5,077.26
Department of the Interior	592	59	49	83.05%	17	28.81%	$109,994.37	$1,864.31	$6,470.26
Department of the Navy	1,531	228	213	93.42%	25	10.96%	$161,418.00	$707.97	$6,456.72
Department of the Treasury	746	152	151	99.34%	10	6.58%	$65,250.00	$429.28	$6,525.00
Department of Transportation	541	63	62	98.41%	4	6.35%	$9,950.00	$157.94	$2,487.50
Department of Veterans Affairs	4,484	353	321	90.93%	48	13.60%	$485,766.66	$1,376.11	$10,120.14
Election Assistance Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF

Table B-6 FY 2012 Benefits Provided in All Pre-Complaint Settlements									
Agency or Department	**Total Number Completed/ Ended Counselings**	**Total Number Settlements**	**Number Completed/ Ended Counselings with Non-Monetary Benefits**	**% Completed/ Ended Counselings with Non-Monetary Benefits**	**Number Completed/ Ended Counselings with Monetary Benefits**	**% Completed/ Ended Counselings with Monetary Benefits**	**Total Amount of Monetary Benefits**	**Average Monetary Benefits Per Total Settlements**	**Ave Monetary Benefits Per Settlements With Monetary Benefits**
Environmental Protection Agency	98	4	4	100.00%	0	0.00%	$0.00	$0.00	$0.00
Equal Employment Opportunity Commission	41	2	2	100.00%	0	0.00%	$0.00	$0.00	$0.00
Export-Import Bank of the US	2	1	1	100.00%	0	0.00%	$0.00	$0.00	$0.00
Farm Credit Administration	1	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Farm Credit System Insurance Corporation	0	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Federal Communications Commission	15	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Federal Deposit Insurance Corporation	82	11	11	100.00%	1	9.09%	$1,750.00	$159.09	$1,750.00
Federal Election Commission	4	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Federal Energy Regulatory Commission	13	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Federal Financial Institutions Examination Council	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Housing Finance Agency	17	2	2	100.00%	1	50.00%	$11,920.00	$5,960.00	$11,920.00
Federal Labor Relations Authority	3	1	1	100.00%	0	0.00%	$0.00	$0.00	$0.00
Federal Maritime Commission	3	1	1	100.00%	0	0.00%	$0.00	$0.00	$0.00
Federal Mediation and Conciliation Service	2	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Federal Mine Safety & Health Review Commission	0	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Federal Reserve System--Board of Governors	54	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Federal Retirement Thrift Investment Board	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Trade Commission	10	1	1	100.00%	0	0.00%	$0.00	$0.00	$0.00
General Services Administration	158	9	8	88.89%	1	11.11%	$628.38	$69.82	$628.38
Government Printing Office	70	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Harry S. Truman Scholarship Foundation	0	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Holocaust Memorial Museum U.S.	0	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Institute of Museum and Library Services	0	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Inter-American Foundation	0	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
International Boundary and Water Commission	2	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
International Joint Commission: US and Canada	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
International Trade Commission	2	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
James Madison Memorial Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Japan-United States Friendship Commission	0	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
John F. Kennedy Center for the Performing Arts	2	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Marine Mammal Commission	0	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Merit Systems Protection Board	3	1	1	100.00%	0	0.00%	$0.00	$0.00	$0.00
Millennium Challenge Corporation	0	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00

Table B-6 FY 2012 Benefits Provided in All Pre-Complaint Settlements									
Agency or Department	**Total Number Completed/ Ended Counselings**	**Total Number Settlements**	**Number Completed/ Ended Counselings with Non-Monetary Benefits**	**% Completed/ Ended Counselings with Non-Monetary Benefits**	**Number Completed/ Ended Counselings with Monetary Benefits**	**% Completed/ Ended Counselings with Monetary Benefits**	**Total Amount of Monetary Benefits**	**Average Monetary Benefits Per Total Settlements**	**Ave Monetary Benefits Per Settlements With Monetary Benefits**
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Aeronautics and Space Administration	77	8	5	62.50%	4	50.00%	$44,000.00	$5,500.00	$11,000.00
National Archives and Records Administration	33	13	13	100.00%	1	7.69%	$1,650.00	$126.92	$1,650.00
National Capital Planning Commission	0	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
National Council on Disability	0	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
National Credit Union Administration	7	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
National Endowment for the Arts	8	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
National Endowment for the Humanities	0	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
National Foundation on the Arts & the Humanities	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Gallery of Art	3	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
National Indian Gaming Commission	1	1	1	100.00%	0	0.00%	$0.00	$0.00	$0.00
National Labor Relations Board	19	1	1	100.00%	0	0.00%	$0.00	$0.00	$0.00
National Mediation Board	0	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
National Reconnaissance Office	7	1	0	0.00%	1	100.00%	$20,000.00	$20,000.00	$20,000.00
National Science Foundation	15	2	2	100.00%	0	0.00%	$0.00	$0.00	$0.00
National Transportation Safety Board	3	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Navajo and Hopi Indian Relocation Commission	0	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Nuclear Regulatory Commission	35	9	5	55.56%	4	44.44%	$29,500.00	$3,277.78	$7,375.00
Nuclear Waste Technical Review Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Occupational Safety & Health Review Commission	0	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Office of Government Ethics	10	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Office of Personnel Management	88	1	0	0.00%	1	100.00%	$11,000.00	$11,000.00	$11,000.00
Office of Special Counsel	0	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Office of the Director of National Intelligence	5	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Overseas Private Investment Corporation	2	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Peace Corps	6	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Pension Benefit Guaranty Corporation	20	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Postal Regulatory Commission	1	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Presidio Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Railroad Retirement Board	6	1	1	100.00%	0	0.00%	$0.00	$0.00	$0.00
Securities and Exchange Commission	30	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Selective Service System	2	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Small Business Administration	75	4	4	100.00%	1	25.00%	$9,788.00	$2,447.00	$9,788.00

Table B-6 FY 2012 Benefits Provided in All Pre-Complaint Settlements

Agency or Department	Total Number Completed/ Ended Counselings	Total Number Settlements	Number Completed/ Ended Counselings with Non-Monetary Benefits	% Completed/ Ended Counselings with Non-Monetary Benefits	Number Completed/ Ended Counselings with Monetary Benefits	% Completed/ Ended Counselings with Monetary Benefits	Total Amount of Monetary Benefits	Average Monetary Benefits Per Total Settlements	Ave Monetary Benefits Per Settlements With Monetary Benefits
Smithsonian Institution	38	1	0	0.00%	1	100.00%	$618.49	$618.49	$618.49
Social Security Administration	917	77	77	100.00%	2	2.60%	$28,500.00	$370.13	$14,250.00
Tennessee Valley Authority	86	8	8	100.00%	6	75.00%	$94,279.96	$11,785.00	$15,713.33
Trade and Development Agency	0	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
U.S. Postal Service	13,143	3,239	3,031	93.58%	455	14.05%	$558,750.39	$172.51	$1,228.02
Utah Reclamation Mitigation and Conservation Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Valles Caldera Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Cabinet Level Subtotal	32,258	5,181	4,861	93.82%	714	13.78%	$3,182,083.82	$614.18	$4,456.70
Midsize Agencies Subtotal	1,634	125	119	95.20%	17	13.60%	$190,564.83	$1,524.52	$11,209.70
Small Agencies Subtotal	615	47	42	89.36%	9	19.15%	$70,070.00	$1,490.85	$7,785.56
Micro Agencies Subtotal	15	0	0	0.00%	0	0.00%	$0.00	$0.00	$0.00
Government-wide	34,521	5,353	5,022	93.82%	740	13.82%	$3,442,718.65	$643.14	$4,652.32

NRF = No Report Filed

Table B-7 FY 2012 Profile Agency Timeliness Indicators (totals with and without USPS data)														
Agency or Department	Total Number Completed / Ended Counselings (excluding remands)	Total Number Timely Completed / Ended Counselings	% Timely Completed / Ended Counselings	Total Number Completed Investigations	Total Number Timely Completed Investigations	% Investigations Timely Completed	APD All Completed Investigations From Date Complaint Filed	Total Number Complaint Closures	APD All Complaint Closures from Date Complaint Filed	Total Number Merit FADs (No AJ Decision)	Total Number Timely Merit FADs (No AJ Decision)	% Timely Merit FADs (No AJ Decision)	APD Merit FADs (No AJ Decision) from Date FAD Required	APD Merit FADs (No AJ Dec) from Date Complaint Filed / Remanded
Advisory Council on Historic Preservation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
African Development Foundation	0	0	0.00%	0	0	0.00%	0	3	845	0	0	0.00%	0	0
Agency for International Development	34	23	67.65%	13	1	7.69%	282.38	16	398.81	1	0	0.00%	62	830
American Battle Monuments Commission	1	1	100.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Appalachian Regional Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Architectural and Transportation Barriers Compliance Board	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Arctic Research Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Armed Forces Retirement Home	5	4	80.00%	0	0	0.00%	0	4	243.5	4	4	100.00%	48.25	243.5
Barry Goldwater Scholarship and Excellence in Education Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Broadcasting Board of Governors	53	51	96.23%	5	5	100.00%	161.2	14	356.29	2	2	100.00%	51	326
Central Intelligence Agency	42	33	78.57%	14	1	7.14%	345.57	39	585.38	6	4	66.67%	59.67	590.33
Chemical Safety and Hazard Investigation Board	2	2	100.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Christopher Columbus Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission of Fine Arts	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission on Civil Rights	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Committee for Purchase from People Who Are Blind or Severely Disabled	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Commodity Futures Trading Commission	1	1	100.00%	1	1	100.00%	110	2	314	2	1	50.00%	68.5	314
Consumer Financial Protection Bureau	15	11	73.33%	3	3	100.00%	209	7	181.29	3	3	100.00%	57	301
Consumer Product Safety Commission	3	2	66.67%	4	4	100.00%	142.25	2	380	1	1	100.00%	25	416
Corporation for National and Community Service	7	3	42.86%	6	6	100.00%	108.67	3	431.67	3	0	0.00%	169.33	431.67
Court Services and Offender Supervision Agency for the District of Columbia	24	13	54.17%	6	4	66.67%	165	15	756.93	2	2	100.00%	46	393
Defense Army and Air Force Exchange	336	255	75.89%	38	5	13.16%	234.79	89	318.17	14	13	92.86%	59.07	346.29
Defense Commissary Agency	227	198	87.22%	58	14	24.14%	256.97	120	318.85	27	26	96.30%	29.81	349.44
Defense Contract Audit Agency	45	26	57.78%	12	3	25.00%	264	32	252.25	7	5	71.43%	67.71	357.57
Defense Contract Management Agency	85	85	100.00%	3	0	0.00%	328.67	38	345.03	8	8	100.00%	21.88	496.63
Defense Finance and Accounting Service	92	92	100.00%	20	11	55.00%	244.55	39	352.74	8	8	100.00%	37.75	309.25
Defense Human Resources Activity	8	6	75.00%	0	0	0.00%	0	5	149	0	0	0.00%	0	0
Defense Information Systems Agency	29	29	100.00%	4	0	0.00%	260.75	8	686.75	0	0	0.00%	0	0
Defense Intelligence Agency	89	83	93.26%	14	5	35.71%	314.36	34	518.88	7	1	14.29%	239.57	681.29
Defense Joint Task Force National Capital Region Medical	84	53	63.10%	1	0	0.00%	315	7	92	0	0	0.00%	0	0
Defense Logistics Agency	312	276	88.46%	52	12	23.08%	272.19	136	463.1	38	3	7.89%	195.84	493.92
Defense Media Activity	3	3	100.00%	0	0	0.00%	0	3	453	0	0	0.00%	0	0
Defense Missile Defense Agency	11	3	27.27%	1	0	0.00%	237	0	0	0	0	0.00%	0	0
Defense National Geospatial-Intelligence Agency	31	27	87.10%	17	17	100.00%	179.47	20	427.3	4	4	100.00%	42.25	666.75
Defense National Guard Bureau	113	97	85.84%	0	0	0.00%	0	33	327.39	3	0	0.00%	321.67	361.67
Defense National Security Agency	69	66	95.65%	30	21	70.00%	332.5	17	636.29	5	5	100.00%	60	376.4
Defense Nuclear Facilities Safety Board	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Defense Office of the Inspector General	9	9	100.00%	1	1	100.00%	255	3	468.67	0	0	0.00%	0	0
Defense Office of the Secretary - Wash. Hqtrs. Services	45	45	100.00%	19	15	78.95%	247.68	45	569.62	6	0	0.00%	157.5	663.5

Table B-7 FY 2012 Profile Agency Timeliness Indicators (totals with and without USPS data)														
Agency or Department	Total Number Completed / Ended Counselings (excluding remands)	Total Number Timely Completed / Ended Counselings	% Timely Completed / Ended Counselings	Total Number Completed Investigations	Total Number Timely Completed Investigations	% Investigations Timely Completed	APD All Completed Investigations From Date Complaint Filed	Total Number Complaint Closures	APD All Complaint Closures from Date Complaint Filed	Total Number Merit FADs (No AJ Decision)	Total Number Timely Merit FADs (No AJ Decision)	% Timely Merit FADs (No AJ Decision)	APD Merit FADs (No AJ Decision) from Date FAD Required	APD Merit FADs (No AJ Dec) from Date Complaint Filed / Remanded
Defense Security Service	18	18	100.00%	5	0	0.00%	193	6	166.67	3	3	100.00%	57.67	200
Defense Technical Information Center	1	0	0.00%	0	0	0.00%	0	1	599	0	0	0.00%	0	0
Defense Threat Reduction Agency	19	18	94.74%	0	0	0.00%	0	8	742.75	0	0	0.00%	0	0
Defense TRICARE Management Activity	18	7	38.89%	2	1	50.00%	368.5	7	217.29	0	0	0.00%	0	0
Defense Uniformed Services University	5	5	100.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Department of Agriculture	975	713	73.13%	437	217	49.66%	241.59	453	633.2	151	42	27.81%	244.41	638.32
Department of Commerce	325	275	84.62%	183	166	90.71%	188.25	432	465.11	189	26	13.76%	242.79	569.24
Department of Defense Education Activity	136	134	98.53%	54	50	92.59%	176.35	55	405.89	12	7	58.33%	58.33	385.67
Department of Education	48	47	97.92%	26	26	100.00%	179	46	565.93	17	17	100.00%	36.12	358.24
Department of Energy	124	66	53.23%	51	42	82.35%	178.84	63	344.75	18	5	27.78%	91.72	371.67
Department of Health and Human Services	674	613	90.95%	288	269	93.40%	153.41	409	340.52	96	54	56.25%	63.85	404.14
Department of Homeland Security	2,031	1,718	84.59%	1,046	596	56.98%	229.94	1,097	461.88	337	163	48.37%	142.91	493.66
Department of Housing and Urban Development	106	68	64.15%	77	26	33.77%	285.31	73	594.14	25	2	8.00%	190.32	624.24
Department of Justice	1,372	1,242	90.52%	614	483	78.66%	202.46	857	591.89	362	28	7.73%	382.55	775.83
Department of Labor	206	193	93.69%	85	83	97.65%	204.12	134	505.19	44	38	86.36%	59.48	357.14
Department of State	270	199	73.70%	97	52	53.61%	245.01	110	413.4	40	1	2.50%	167.78	460.58
Department of the Air Force	996	897	90.06%	305	53	17.38%	263.15	500	482.59	96	12	12.50%	455.29	839.44
Department of the Army	2,299	2,008	87.34%	484	114	23.55%	258.31	1,116	324.63	181	21	11.60%	108.17	528.11
Department of the Interior	592	473	79.90%	238	123	51.68%	270.06	307	487.03	104	12	11.54%	173.24	574.44
Department of the Navy	1,530	1,394	91.11%	409	162	39.61%	276.71	904	332.14	117	117	100.00%	53.45	477.23
Department of the Treasury	746	721	96.65%	285	248	87.02%	197.5	407	468.29	123	108	87.80%	41.02	355.41
Department of Transportation	541	506	93.53%	216	214	99.07%	136.06	335	411.26	89	47	52.81%	75.36	413.53
Department of Veterans Affairs	4,484	4,407	98.28%	1,583	1,391	87.87%	164.52	2,123	393.83	597	30	5.03%	177.88	464.04
Election Assistance Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Environmental Protection Agency	98	68	69.39%	61	9	14.75%	354.98	49	712.04	13	0	0.00%	476.77	899.31
Equal Employment Opportunity Commission	41	40	97.56%	13	12	92.31%	239.69	20	329.05	5	0	0.00%	155.4	529.8
Export-Import Bank of the US	2	2	100.00%	1	1	100.00%	240	1	330	0	0	0.00%	0	0
Farm Credit Administration	1	1	100.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Farm Credit System Insurance Corporation	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Federal Communications Commission	15	10	66.67%	10	10	100.00%	39	2	90	0	0	0.00%	0	0
Federal Deposit Insurance Corporation	82	80	97.56%	29	29	100.00%	224.21	42	291.31	12	12	100.00%	49.83	407.42
Federal Election Commission	4	4	100.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Federal Energy Regulatory Commission	13	13	100.00%	6	6	100.00%	180	10	152.3	6	6	100.00%	60	200
Federal Financial Institutions Examination Council	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Housing Finance Agency	16	15	93.75%	3	2	66.67%	225	6	199.83	0	0	0.00%	0	0
Federal Labor Relations Authority	3	3	100.00%	1	1	100.00%	248	0	0	0	0	0.00%	0	0
Federal Maritime Commission	3	3	100.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Federal Mediation and Conciliation Service	2	2	100.00%	0	0	0.00%	0	2	15	0	0	0.00%	0	0
Federal Mine Safety & Health Review Commission	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Federal Reserve System--Board of Governors	54	54	100.00%	5	5	100.00%	151	6	310.17	0	0	0.00%	0	0
Federal Retirement Thrift Investment Board	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Trade Commission	10	10	100.00%	0	0	0.00%	0	1	1,115.00	0	0	0.00%	0	0
General Services Administration	158	156	98.73%	77	44	57.14%	265.82	85	425.05	21	15	71.43%	59.19	397.57
Government Printing Office	70	66	94.29%	26	12	46.15%	274.27	29	329.86	11	3	27.27%	158.55	358.45
Harry S. Truman Scholarship Foundation	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0

Table B-7 FY 2012 Profile Agency Timeliness Indicators (totals with and without USPS data)														
Agency or Department	Total Number Completed / Ended Counselings (excluding remands)	Total Number Timely Completed / Ended Counselings	% Timely Completed / Ended Counselings	Total Number Completed Investigations	Total Number Timely Completed Investigations	% Investigations Timely Completed	APD All Completed Investigations From Date Complaint Filed	Total Number Complaint Closures	APD All Complaint Closures from Date Complaint Filed	Total Number Merit FADs (No AJ Decision)	Total Number Timely Merit FADs (No AJ Decision)	% Timely Merit FADs (No AJ Decision)	APD Merit FADs (No AJ Decision) from Date FAD Required	APD Merit FADs (No AJ Dec) from Date Complaint Filed / Remanded
Holocaust Memorial Museum U.S.	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Institute of Museum and Library Services	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Inter-American Foundation	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
International Boundary and Water Commission	2	2	100.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
International Joint Commission: US and Canada	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
International Trade Commission	2	2	100.00%	2	1	50.00%	161.5	1	195	0	0	0.00%	0	0
James Madison Memorial Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Japan-United States Friendship Commission	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
John F. Kennedy Center for the Performing Arts	2	2	100.00%	1	1	100.00%	61	0	0	0	0	0.00%	0	0
Marine Mammal Commission	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Merit Systems Protection Board	3	3	100.00%	1	1	100.00%	148	1	231	0	0	0.00%	0	0
Millennium Challenge Corporation	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Aeronautics and Space Administration	77	61	79.22%	21	17	80.95%	193.57	38	565.26	11	0	0.00%	181	516.36
National Archives and Records Administration	33	30	90.91%	3	3	100.00%	170	11	685.27	3	3	100.00%	58.33	636
National Capital Planning Commission	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
National Council on Disability	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
National Credit Union Administration	7	7	100.00%	3	2	66.67%	217	7	424.57	1	0	0.00%	75	541
National Endowment for the Arts	8	8	100.00%	0	0	0.00%	0	3	324.33	0	0	0.00%	0	0
National Endowment for the Humanities	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
National Foundation on the Arts&the Humanities	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Gallery of Art	3	3	100.00%	0	0	0.00%	0	6	817.33	3	0	0.00%	89.33	760.67
National Indian Gaming Commission	1	0	0.00%	2	1	50.00%	266	1	304	0	0	0.00%	0	0
National Labor Relations Board	19	15	78.95%	3	3	100.00%	167.33	8	288.88	2	2	100.00%	55.5	234.5
National Mediation Board	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
National Reconnaissance Office	7	7	100.00%	0	0	0.00%	0	7	542.14	2	1	50.00%	84.5	333.5
National Science Foundation	15	14	93.33%	4	0	0.00%	371.75	6	364	0	0	0.00%	0	0
National Transportation Safety Board	3	3	100.00%	2	2	100.00%	111	2	176	1	1	100.00%	40	276
Navajo and Hopi Indian Relocation Commission	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Nuclear Regulatory Commission	35	33	94.29%	9	7	77.78%	209.44	16	298.19	0	0	0.00%	0	0
Nuclear Waste Technical Review Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Occupational Safety & Health Review Commission	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Office of Government Ethics	10	10	100.00%	0	0	0.00%	0	2	15	0	0	0.00%	0	0
Office of Personnel Management	88	87	98.86%	25	25	100.00%	103.4	28	504.64	8	0	0.00%	353.88	1,128.25
Office of Special Counsel	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Office of the Director of National Intelligence	5	5	100.00%	0	0	0.00%	0	4	474	1	1	100.00%	27	269
Overseas Private Investment Corporation	2	2	100.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Peace Corps	6	6	100.00%	4	4	100.00%	156.75	4	508.75	3	1	33.33%	130	367
Pension Benefit Guaranty Corporation	20	13	65.00%	7	6	85.71%	194.14	20	437.2	5	5	100.00%	40.4	361.8
Postal Regulatory Commission	1	1	100.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Presidio Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Railroad Retirement Board	6	6	100.00%	4	4	100.00%	178	1	660	0	0	0.00%	0	0
Securities and Exchange Commission	30	25	83.33%	10	8	80.00%	259.7	4	308.25	2	1	50.00%	66.5	334.5
Selective Service System	2	2	100.00%	2	2	100.00%	288	2	288	0	0	0.00%	0	0

Table B-7 FY 2012 Profile Agency Timeliness Indicators (totals with and without USPS data)														
Agency or Department	Total Number Completed / Ended Counselings (excluding remands)	Total Number Timely Completed / Ended Counselings	% Timely Completed / Ended Counselings	Total Number Completed Investigations	Total Number Timely Completed Investigations	% Investigations Timely Completed	APD All Completed Investigations From Date Complaint Filed	Total Number Complaint Closures	APD All Complaint Closures from Date Complaint Filed	Total Number Merit FADs (No AJ Decision)	Total Number Timely Merit FADs (No AJ Decision)	% Timely Merit FADs (No AJ Decision)	APD Merit FADs (No AJ Decision) from Date FAD Required	APD Merit FADs (No AJ Dec) from Date Complaint Filed / Remanded
Small Business Administration	75	50	66.67%	33	30	90.91%	204.09	38	313.29	7	6	85.71%	25.14	329
Smithsonian Institution	38	38	100.00%	8	8	100.00%	173.5	15	500.27	5	5	100.00%	41.4	213.2
Social Security Administration	916	871	95.09%	339	279	82.30%	194.84	414	506.13	136	36	26.47%	175.1	459.63
Tennessee Valley Authority	86	85	98.84%	44	44	100.00%	138.2	58	330.36	20	20	100.00%	56.2	236.25
Trade and Development Agency	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
U.S. Postal Service	13,121	12,906	98.36%	2,660	2,636	99.10%	112.86	4,579	275.45	1,088	1,062	97.61%	32.41	277.48
Utah Reclamation Mitigation and Conservation Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Valles Caldera Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Cabinet Level Subtotal Including USPS	32,225	29,981	93.04%	9,415	7,056	74.94%	184.54	14,651	382.46	3,816	1,868	48.95%	143.51	462.61
Midsize Agencies Subtotal	1,633	1,507	92.28%	640	488	76.25%	212.74	774	475.76	236	97	41.10%	162.51	470.94
Small Agencies Subtotal	614	541	88.11%	171	116	67.84%	219.08	276	424.89	66	38	57.58%	90.12	407.67
Micro Agencies Subtotal	14	14	100.00%	0	0	0.00%	0	5	513	0	0	0.00%	0	0
Government-wide Including USPS	34,486	32,043	92.92%	10,226	7,660	74.91%	186.89	15,706	387.84	4,118	2,003	48.64%	143.74	462.21
USPS Percentage of Cabinet Sub Total	40.72%	43.05%		28.25%	37.36%			31.25%		28.51%	56.85%			
USPS Percentage of Government-wide	38.05%	40.28%		26.01%	34.41%			29.15%		26.42%	53.02%			
Cabinet Level Subtotal Minus USPS	19,104	17,075	89.38%	6,755	4,420	65.43%	212.77	10,072	431.1	2,728	806	29.55%	187.82	647.11
Government-wide Minus USPS	21,365	19,138	89.57%	7,566	5,024	66.40%	212.91	11,127	434.09	3,030	941	31.06%	183.72	628.17

NRF = No Report Filed

Table B-7a FY 2012 Profile Agency Timeliness Indicators														
Agency or Department	Total Number Completed / Ended Counselings (excluding remands)	Total Number Timely Completed / Ended Counselings	% Timely Completed / Ended Counselings	Total Number Completed Investigations	Total Number Timely Completed Investigations	% Investigations Timely Completed	APD All Completed Investigations From Date Complaint Filed	Total Number Complaint Closures	APD All Complaint Closures from Date Complaint Filed	Total Number Merit FADs (No AJ Decision)	Total Number Timely Merit FADs (No AJ Decision)	% Timely Merit FADs (No AJ Decision)	APD Merit FADs (No AJ Decision) from Date FAD Required	APD Merit FADs (No AJ Dec) from Date Complaint Filed / Remanded
Defense Logistics Agency Wide	**312**	**276**	**88.46%**	**52**	**12**	**23.08%**	**272.19**	**136**	**463.1**	**38**	**3**	**7.89%**	**195.84**	**493.92**
DLA Aviation	54	48	88.89%	10	2	20.00%	238.8	20	398.8	7	1	14.29%	160.86	452.71
DLA Disposition Services	10	7	70.00%	5	0	0.00%	328.8	9	638.56	6	1	16.67%	214.33	576.17
DLA Distribution	151	140	92.72%	19	6	31.58%	276.42	56	416.79	14	1	7.14%	249.86	549.14
DLA Headquarters Operations Division	53	43	81.13%	7	2	28.57%	264.14	22	586.32	1	0	0.00%	163	419
DLA Land and Maritime	20	15	75.00%	6	0	0.00%	321	16	450.06	3	0	0.00%	156.33	432.67
DLA Logistics Information Service	2	2	100.00%	2	0	0.00%	288.5	4	454.25	4	0	0.00%	156.25	454.25
DLA Troop Support	22	21	95.45%	3	2	66.67%	172.67	9	444.56	3	0	0.00%	91.67	307
Defense National Guard Bureau Wide	**113**	**97**	**85.84%**	**0**	**0**	**0.00%**	**0**	**33**	**327.39**	**3**	**0**	**0.00%**	**321.67**	**361.67**
Alabama National Guard	1	1	100.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Alaska National Guard	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Arizona National Guard	6	6	100.00%	0	0	0.00%	0	3	103	0	0	0.00%	0	0
Arkansas National Guard	3	3	100.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
California National Guard	17	12	70.59%	0	0	0.00%	0	7	307.43	0	0	0.00%	0	0
Colorado National Guard	1	1	100.00%	0	0	0.00%	0	1	180	0	0	0.00%	0	0
Connecticut National Guard	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
DC National Guard	1	1	100.00%	0	0	0.00%	0	1	30	0	0	0.00%	0	0
Delaware National Guard	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Florida National Guard	1	1	100.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Georgia National Guard	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Guam National Guard	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Hawaii National Guard	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Idaho National Guard	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Illinois National Guard	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Indiana National Guard	1	1	100.00%	0	0	0.00%	0	1	400	0	0	0.00%	0	0
Iowa National Guard	34	33	97.06%	0	0	0.00%	0	1	458	0	0	0.00%	0	0
Kansas National Guard	1	1	100.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Kentucky National Guard	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Louisiana National Guard	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Maine National Guard	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Maryland National Guard	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Massachusetts National Guard	4	4	100.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Michigan National Guard	5	3	60.00%	0	0	0.00%	0	1	315	0	0	0.00%	0	0
Minnesota National Guard	1	1	100.00%	0	0	0.00%	0	1	444	0	0	0.00%	0	0
Mississippi National Guard	1	1	100.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Missouri National Guard	1	1	100.00%	0	0	0.00%	0	2	410.5	0	0	0.00%	0	0
Montana National Guard	1	1	100.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Nebraska National Guard	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Nevada National Guard	2	1	50.00%	0	0	0.00%	0	1	500	0	0	0.00%	0	0
New Hampshire National Guard	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
New Jersey National Guard	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
New Mexico National Guard	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
New York National Guard	6	0	0.00%	0	0	0.00%	0	3	121.67	0	0	0.00%	0	0

Table B-7a FY 2012 Profile Agency Timeliness Indicators														
Agency or Department	Total Number Completed / Ended Counselings (excluding remands)	Total Number Timely Completed / Ended Counselings	% Timely Completed / Ended Counselings	Total Number Completed Investigations	Total Number Timely Completed Investigations	% Investigations Timely Completed	APD All Completed Investigations From Date Complaint Filed	Total Number Complaint Closures	APD All Complaint Closures from Date Complaint Filed	Total Number Merit FADs (No AJ Decision)	Total Number Timely Merit FADs (No AJ Decision)	% Timely Merit FADs (No AJ Decision)	APD Merit FADs (No AJ Decision) from Date FAD Required	APD Merit FADs (No AJ Dec) from Date Complaint Filed / Remanded
North Carolina National Guard	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
North Dakota National Guard	1	1	100.00%	0	0	0.00%	0	1	239	0	0	0.00%	0	0
Ohio National Guard	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Oklahoma National Guard	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Oregon National Guard	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Pennsylvania National Guard	1	1	100.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Puerto Rico National Guard	6	6	100.00%	0	0	0.00%	0	1	731	0	0	0.00%	0	0
Rhode Island National Guard	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
South Carolina National Guard	1	1	100.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
South Dakota National Guard	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Tennessee National Guard	1	1	100.00%	0	0	0.00%	0	3	361.67	3	0	0.00%	321.67	361.67
Texas National Guard	1	1	100.00%	0	0	0.00%	0	5	468.8	0	0	0.00%	0	0
Utah National Guard	4	4	100.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Vermont National Guard	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Virgin Islands National Guard	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Virginia National Guard	2	2	100.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Washington State National Guard	3	3	100.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
West Virginia National Guard	4	4	100.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Wisconsin National Guard	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Wyoming National Guard	2	1	50.00%	0	0	0.00%	0	1	431	0	0	0.00%	0	0
Department of Agriculture Wide	**975**	**713**	**73.13%**	**437**	**217**	**49.66%**	**241.59**	**453**	**633.2**	**151**	**42**	**27.81%**	**244.41**	**638.32**
USDA - Office Of Inspector General	10	7	70.00%	6	6	100.00%	154.17	2	1,188.50	2	0	0.00%	269	1,188.50
USDA Agricultural Marketing Service	26	26	100.00%	15	13	86.67%	146.8	21	1,152.76	5	0	0.00%	115.6	298.2
USDA Agricultural Research Service	40	38	95.00%	21	11	52.38%	286.29	27	438.19	9	0	0.00%	337.56	486.33
USDA Agriculture Headquarters	51	15	29.41%	14	4	28.57%	259.79	23	710.09	7	7	100.00%	44	1,243.57
USDA Animal and Plant Health Inspection Service	87	31	35.63%	39	21	53.85%	195.41	43	470.88	17	7	41.18%	276.76	602.76
USDA Economic Research Service	1	1	100.00%	3	1	33.33%	534	1	1,264.00	0	0	0.00%	0	0
USDA Farm Service Agency	47	45	95.74%	23	23	100.00%	95.87	28	804.89	9	2	22.22%	637.11	931.33
USDA Food and Nutrition Service	12	12	100.00%	3	2	66.67%	190.33	8	557.38	2	0	0.00%	126.5	356
USDA Food Safety And Inspection Service	180	171	95.00%	70	33	47.14%	247.21	77	906.78	19	6	31.58%	130.47	525.11
USDA Foreign Agricultural Service	13	6	46.15%	3	2	66.67%	182.33	4	312.75	1	1	100.00%	55	499
USDA Forest Service	302	249	82.45%	137	72	52.55%	210.57	128	453.45	45	11	24.44%	215.71	570.91
USDA Grain Inspection, Packers& Stockyards Admin	15	6	40.00%	6	5	83.33%	149.5	7	543.14	3	0	0.00%	373.33	761.67
USDA National Agricultural Statistics Service	4	4	100.00%	2	1	50.00%	215.5	1	181	0	0	0.00%	0	0
USDA National Appeals Division	0	0	0.00%	0	0	0.00%	0	1	718	0	0	0.00%	0	0
USDA National Institute of Food and Agriculture	2	2	100.00%	0	0	0.00%	0	2	309	0	0	0.00%	0	0
USDA Natural Resources Conservation Service	74	55	74.32%	22	16	72.73%	188.73	22	488.55	8	4	50.00%	295.88	602.75
USDA Office Of The Chief Financial Officer	41	28	68.29%	22	3	13.64%	384.95	14	449.5	6	0	0.00%	527.67	527.67
USDA Risk Management Agency	14	9	64.29%	7	1	14.29%	396.14	6	513.5	3	3	100.00%	43.67	755.33
USDA Rural Development	56	8	14.29%	44	3	6.82%	394.91	38	763.87	15	1	6.67%	181.8	759.27

Table B-7a FY 2012 Profile Agency Timeliness Indicators														
Agency or Department	Total Number Completed / Ended Counselings (excluding remands)	Total Number Timely Completed / Ended Counselings	% Timely Completed / Ended Counselings	Total Number Completed Investigations	Total Number Timely Completed Investigations	% Investigations Timely Completed	APD All Completed Investigations From Date Complaint Filed	Total Number Complaint Closures	APD All Complaint Closures from Date Complaint Filed	Total Number Merit FADs (No AJ Decision)	Total Number Timely Merit FADs (No AJ Decision)	% Timely Merit FADs (No AJ Decision)	APD Merit FADs (No AJ Decision) from Date FAD Required	APD Merit FADs (No AJ Dec) from Date Complaint Filed / Remanded
Department of Commerce Wide	**325**	**275**	**84.62%**	**183**	**166**	**90.71%**	**188.25**	**432**	**465.11**	**189**	**26**	**13.76%**	**242.79**	**569.24**
DOC All Other Commerce Bureaus	30	9	30.00%	21	21	100.00%	185.57	26	352	7	2	28.57%	176.71	461.29
DOC Bureau of the Census	114	105	92.11%	66	60	90.91%	181.77	52	314.9	22	3	13.64%	214.27	476.36
DOC Decennial Census	5	5	100.00%	3	3	100.00%	192	249	567.55	125	9	7.20%	278.11	631.04
DOC International Trade Administration	11	7	63.64%	7	6	85.71%	206.71	6	211.33	2	0	0.00%	156.5	360
DOC National Institute of Standards & Technology	24	23	95.83%	8	7	87.50%	197.63	14	279.71	5	1	20.00%	202.6	457
DOC National Oceanic & Atmospheric Administration	82	71	86.59%	61	52	85.25%	191.23	53	324.3	19	2	10.53%	176.47	409.37
DOC U. S. Patent and Trademark Office	59	55	93.22%	17	17	100.00%	193.29	32	365.91	9	9	100.00%	54.78	468.22
Department of Energy Wide	**124**	**66**	**53.23%**	**51**	**42**	**82.35%**	**178.84**	**63**	**344.75**	**18**	**5**	**27.78%**	**91.72**	**371.67**
DOE Bonneville Power Administration	28	7	25.00%	6	1	16.67%	228.17	13	234.77	3	0	0.00%	146.33	354
DOE Chicago Operations Office	1	1	100.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
DOE EM Consolidated Business Center	4	1	25.00%	1	0	0.00%	398	1	300	0	0	0.00%	0	0
DOE Golden Field Office	5	5	100.00%	1	0	0.00%	330	1	229	0	0	0.00%	0	0
DOE Headquarters	32	11	34.38%	12	12	100.00%	219.42	18	473.94	5	0	0.00%	121.2	525.2
DOE Idaho Operations Office	3	3	100.00%	1	1	100.00%	91	0	0	0	0	0.00%	0	0
DOE National Energy Technology Lab	2	1	50.00%	1	0	0.00%	207	1	87	0	0	0.00%	0	0
DOE NNSA Service Center	21	12	57.14%	19	18	94.74%	122.63	9	266.56	3	1	33.33%	75	294.33
DOE Oak Ridge Operations	2	2	100.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
DOE OSTI	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
DOE Richland Operations Office	1	1	100.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
DOE Savannah River Operations	6	5	83.33%	0	0	0.00%	0	2	352	2	2	100.00%	38	352
DOE Southeastern Power Administration	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
DOE Southwestern Power Administration	3	3	100.00%	0	0	0.00%	0	3	153.33	1	1	100.00%	60	400
DOE Strategic Petroleum Reserve	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
DOE Western Area Power Administration	16	14	87.50%	10	10	100.00%	176.3	15	397.13	4	1	25.00%	61.25	253.75
Department of Health and Human Services Wide	**674**	**613**	**90.95%**	**288**	**269**	**93.40%**	**153.41**	**409**	**340.52**	**96**	**54**	**56.25%**	**63.85**	**404.14**
HHS Administration for Children and Families	12	8	66.67%	4	2	50.00%	197.25	5	593.8	3	2	66.67%	94.67	920
HHS Agency for Healthcare Research and Quality	3	3	100.00%	3	3	100.00%	141	0	0	0	0	0.00%	0	0
HHS Centers for Disease Control and Prevention	127	121	95.28%	47	42	89.36%	157.83	69	263.43	11	8	72.73%	64.09	423.27
HHS Centers for Medicare & Medicaid Services	38	36	94.74%	24	24	100.00%	136.17	38	531.18	8	5	62.50%	61	518.5
HHS Food and Drug Administration	123	122	99.19%	58	56	96.55%	176.79	60	398.6	5	0	0.00%	122.8	557.6
HHS Health Resources and Services Administration	20	20	100.00%	7	7	100.00%	127.43	13	404.92	7	6	85.71%	31.14	341.71
HHS Indian Health Service	198	172	86.87%	57	56	98.25%	116.07	105	208.22	29	22	75.86%	28	268.59
HHS National Institutes of Health	99	88	88.89%	51	46	90.20%	162.88	82	379.46	21	3	14.29%	101.9	404.95
HHS Office of the Secretary of Health &Human Srvcs	44	34	77.27%	30	27	90.00%	174.23	30	483.13	11	8	72.73%	72.27	493.27
HHS Program Support Center	7	6	85.71%	3	3	100.00%	120.33	1	26	0	0	0.00%	0	0
HHS Substance Abuse& Mental Health Srvcs Admin	3	3	100.00%	4	3	75.00%	157	6	210.67	1	0	0.00%	74	334

Table B-7a FY 2012 Profile Agency Timeliness Indicators														
Agency or Department	Total Number Completed / Ended Counselings (excluding remands)	Total Number Timely Completed / Ended Counselings	% Timely Completed / Ended Counselings	Total Number Completed Investigations	Total Number Timely Completed Investigations	% Investigations Timely Completed	APD All Completed Investigations From Date Complaint Filed	Total Number Complaint Closures	APD All Complaint Closures from Date Complaint Filed	Total Number Merit FADs (No AJ Decision)	Total Number Timely Merit FADs (No AJ Decision)	% Timely Merit FADs (No AJ Decision)	APD Merit FADs (No AJ Decision) from Date FAD Required	APD Merit FADs (No AJ Dec) from Date Complaint Filed / Remanded
Department of Homeland Security Wide	**2,031**	**1,718**	**84.59%**	**1,046**	**596**	**56.98%**	**229.94**	**1,097**	**461.88**	**337**	**163**	**48.37%**	**142.91**	**493.66**
DHS Federal Emergency Management Agency	242	182	75.21%	110	13	11.82%	360.8	96	674.99	36	8	22.22%	233.78	811.06
DHS Federal Law Enforcement Training Center	18	18	100.00%	9	8	88.89%	222.33	16	403.75	1	0	0.00%	78	292
DHS Headquarters	77	54	70.13%	24	21	87.50%	226.13	24	379.33	10	5	50.00%	100.7	455.5
DHS Transportation Security Administration	658	558	84.80%	429	190	44.29%	224.57	373	442.47	109	55	50.46%	111.5	461.31
DHS U.S. Citizenship and Immigration Services	186	185	99.46%	74	73	98.65%	141.64	78	435.5	19	11	57.89%	75.84	383.42
DHS U.S. Coast Guard	96	94	97.92%	39	39	100.00%	205.79	51	391.43	17	13	76.47%	60.29	313.53
DHS U.S. Customs and Border Protection	464	464	100.00%	252	241	95.63%	175.54	294	395.88	91	54	59.34%	157.2	400.19
DHS U.S. Immigration and Customs Enforcement	242	116	47.93%	81	6	7.41%	301.32	133	580.21	42	13	30.95%	212.33	638.21
DHS U.S. Secret Service	48	47	97.92%	28	5	17.86%	354.07	32	430.88	12	4	33.33%	68	516.42
Department of Justice Wide	**1,372**	**1,242**	**90.52%**	**614**	**483**	**78.66%**	**202.46**	**857**	**591.89**	**362**	**28**	**7.73%**	**382.55**	**775.83**
DOJ Alcohol, Tobacco, Firearms and Explosives	67	53	79.10%	34	9	26.47%	314.74	52	454.65	19	2	10.53%	217.63	362.11
DOJ Bureau of Prisons	838	820	97.85%	350	309	88.29%	160.57	412	555.18	143	8	5.59%	491.06	737.02
DOJ Drug Enforcement Administration	44	27	61.36%	23	8	34.78%	313.35	32	551.97	17	0	0.00%	382	769.29
DOJ Executive Office for Immigration Review	16	16	100.00%	10	9	90.00%	215.8	11	485.64	9	0	0.00%	130.33	526.44
DOJ Executive Office for U.S. Attorneys	37	37	100.00%	22	21	95.45%	208.91	42	638.4	19	2	10.53%	384.89	812.11
DOJ Federal Bureau of Investigation	221	150	67.87%	128	98	76.56%	239.77	203	704.71	115	10	8.70%	312.7	916.68
DOJ Office of Justice Programs	18	18	100.00%	9	9	100.00%	227.22	9	193.33	1	1	100.00%	60	376
DOJ Offices, Boards, and Divisions	46	37	80.43%	14	6	42.86%	280.57	34	475.24	8	1	12.50%	85	400
DOJ U.S. Marshals Service	85	84	98.82%	24	14	58.33%	282.67	62	711.35	31	4	12.90%	401.45	849.52
Department of Labor Wide	**206**	**193**	**93.69%**	**85**	**83**	**97.65%**	**204.12**	**134**	**505.19**	**44**	**38**	**86.36%**	**59.48**	**357.14**
DOL (DM and others)	73	69	94.52%	28	27	96.43%	196	51	319.92	17	13	76.47%	61.82	335.35
DOL Bureau of Labor Statistics	6	6	100.00%	1	1	100.00%	176	4	535.5	0	0	0.00%	0	0
DOL Employment and Training Administration	17	16	94.12%	10	10	100.00%	180.2	18	360.94	8	8	100.00%	58.63	441.38
DOL Mine Safety and Health Administration	31	28	90.32%	9	9	100.00%	196.44	15	392.53	4	3	75.00%	66.25	296
DOL Occupational Safety and Health Administration	22	20	90.91%	14	14	100.00%	188.86	18	1,594.89	4	3	75.00%	54.25	295.5
DOL Office of Workers Compensation Programs	25	23	92.00%	9	9	100.00%	228.22	15	277.4	8	8	100.00%	54.38	356.63
DOL Wage and Hour Division	32	31	96.88%	14	13	92.86%	244.14	13	306.46	3	3	100.00%	60	421
Department of the Army Wide	**2,299**	**2,008**	**87.34%**	**484**	**114**	**23.55%**	**258.31**	**1,116**	**324.63**	**181**	**21**	**11.60%**	**108.17**	**528.11**
Eighth U.S. Army (KOREA)	2	0	0.00%	2	0	0.00%	324.5	5	236	1	0	0.00%	101	364
Headquarters, Department of Army	171	151	88.30%	41	3	7.32%	292.93	66	363.88	14	1	7.14%	108.14	468.43
U.S. Army Corps of Engineers	248	216	87.10%	57	14	24.56%	262.04	135	292.41	20	4	20.00%	92.25	487.8
U.S. Army Europe	18	18	100.00%	1	1	100.00%	197	4	85.25	0	0	0.00%	0	0
U.S. Army Forces Command	175	171	97.71%	24	8	33.33%	233.13	85	250.75	11	2	18.18%	113.09	357.36
U.S. Army Installation Management Command	544	482	88.60%	112	29	25.89%	240.04	279	371.59	39	3	7.69%	111.44	537.59
U.S. Army Intelligence and Security Command	22	18	81.82%	9	2	22.22%	241.56	12	299.75	4	1	25.00%	87.5	337.75
U.S. Army Material Command	507	448	88.36%	103	26	25.24%	256.47	259	287.01	34	3	8.82%	106.68	529.79
U.S. Army Medical Command	424	356	83.96%	86	18	20.93%	268	175	329.58	34	5	14.71%	108.06	608.35
U.S. Army Network Enterprise Technology Command	26	20	76.92%	11	5	45.45%	270.73	10	302.9	2	0	0.00%	132	379

Table B-7a FY 2012 Profile Agency Timeliness Indicators

Agency or Department	Total Number Completed / Ended Counselings (excluding remands)	Total Number Timely Completed / Ended Counselings	% Timely Completed / Ended Counselings	Total Number Completed Investigations	Total Number Timely Completed Investigations	% Investigations Timely Completed	APD All Completed Investigations From Date Complaint Filed	Total Number Complaint Closures	APD All Complaint Closures from Date Complaint Filed	Total Number Merit FADs (No AJ Decision)	Total Number Timely Merit FADs (No AJ Decision)	% Timely Merit FADs (No AJ Decision)	APD Merit FADs (No AJ Decision) from Date FAD Required	APD Merit FADs (No AJ Dec) from Date Complaint Filed / Remanded
U.S. Army Pacific (USARPAC)	2	2	100.00%	0	0	0.00%	0	1	6	0	0	0.00%	0	0
U.S. Army Space and Missile Defense Command	1	1	100.00%	4	1	25.00%	269.75	5	893.2	0	0	0.00%	0	0
U.S. Army Special Operations Command (USASOC)	16	12	75.00%	0	0	0.00%	0	7	237.29	0	0	0.00%	0	0
U.S. Army Test and Evaluation Command	16	12	75.00%	10	3	30.00%	262.7	12	357.08	3	0	0.00%	104.33	817.67
U.S. Army Training and Doctrine Command	127	101	79.53%	24	4	16.67%	267.83	61	380.93	19	2	10.53%	121.05	566
Department of the Interior Wide	**592**	**473**	**79.90%**	**238**	**123**	**51.68%**	**270.06**	**307**	**487.03**	**104**	**12**	**11.54%**	**173.24**	**574.44**
Bureau of Ocean Energy Management	7	4	57.14%	2	2	100.00%	245.5	0	0	0	0	0.00%	0	0
Bureau of Safety and Environmental Enforcement	7	2	28.57%	3	2	66.67%	193	0	0	0	0	0.00%	0	0
DOI Bureau Of Indian Affairs	56	56	100.00%	52	13	25.00%	369.54	49	686.98	20	5	25.00%	197.5	873.95
DOI Bureau Of Land Management	81	65	80.25%	33	30	90.91%	158.15	36	367.47	12	2	16.67%	158	389.33
DOI Bureau Of Reclamation	78	63	80.77%	28	25	89.29%	150.96	49	345.53	16	0	0.00%	150.63	378.94
DOI Fish And Wildlife Service	56	50	89.29%	22	22	100.00%	178.18	27	279.11	11	0	0.00%	122.45	317.55
DOI Geological Survey	22	22	100.00%	6	4	66.67%	279.83	18	285.72	3	0	0.00%	78	337.67
DOI National Park Service	208	137	65.87%	65	7	10.77%	345.51	74	580.51	22	1	4.55%	217.73	724.5
DOI Office Of Surface Mining, Reclamation & Enforce	6	4	66.67%	4	4	100.00%	149	5	420.8	0	0	0.00%	0	0
DOI-Office Of The Secretary	71	70	98.59%	23	14	60.87%	256.04	49	570.49	20	4	20.00%	169.5	554.15
Department of the Navy Wide	**1,530**	**1,394**	**91.11%**	**409**	**162**	**39.61%**	**276.71**	**904**	**332.14**	**117**	**117**	**100.00%**	**53.45**	**477.23**
Chief Of Naval Operations	27	26	96.30%	9	4	44.44%	252	12	325.75	5	5	100.00%	57.8	325.8
Commander Naval Installations Command	270	249	92.22%	40	16	40.00%	256.75	171	233.65	17	17	100.00%	55.65	515.18
Commander Naval Reserve	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Commander Pacific Fleet	124	121	97.58%	28	18	64.29%	262.71	39	393.05	8	8	100.00%	54.25	339.63
DON Assistant for Administration	54	48	88.89%	16	6	37.50%	308.44	20	374.35	6	6	100.00%	51.5	444.67
DON Bureau of Medicine & Surgery	120	103	85.83%	32	12	37.50%	304.59	58	404.72	12	12	100.00%	48.75	519.5
DON SPAWAR	25	17	68.00%	5	2	40.00%	264.2	6	311.33	1	1	100.00%	58	334
DON Strategic Systems Project Office	7	7	100.00%	3	1	33.33%	359	3	421.67	0	0	0.00%	0	0
Fleet Cyber Command	16	15	93.75%	1	1	100.00%	160	1	93	0	0	0.00%	0	0
Fleet Forces Command	88	81	92.05%	22	6	27.27%	282.23	36	357.64	5	5	100.00%	53	428
Marine Corps HQ	233	201	86.27%	64	18	28.13%	287	321	345.67	21	21	100.00%	51.1	501.33
Military Sealift Command	56	55	98.21%	18	6	33.33%	296.5	23	141.35	2	2	100.00%	59	419.5
Naval Air Systems Command	162	153	94.44%	42	19	45.24%	265.95	57	279.51	10	10	100.00%	53.3	490.2
Naval Education & Training Command	31	27	87.10%	11	1	9.09%	446.82	15	339.27	1	1	100.00%	53	307
Naval Sea Systems Command	71	66	92.96%	30	12	40.00%	249.73	36	502.08	7	7	100.00%	52.57	467.71
Naval Special Warfare Command	5	4	80.00%	1	0	0.00%	312	3	72.67	0	0	0.00%	0	0
Naval Supply Systems Command	95	86	90.53%	29	15	51.72%	260	41	387.59	10	10	100.00%	58.5	476.7
Naval Systems Management Activity	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Navy Facilities & Engineering Command	118	110	93.22%	47	19	40.43%	250.98	56	414.5	9	9	100.00%	53.44	617.33
Navy Military Personnel Command	9	7	77.78%	5	2	40.00%	277.6	2	203.5	1	1	100.00%	41	378
Office Of Naval Intelligence	15	14	93.33%	5	3	60.00%	252.2	2	292	1	1	100.00%	56	464
Office Of Naval Research	4	4	100.00%	1	1	100.00%	252	2	191	1	1	100.00%	60	341
Department of the Treasury Wide	**746**	**721**	**96.65%**	**285**	**248**	**87.02%**	**197.5**	**407**	**468.29**	**123**	**108**	**87.80%**	**41.02**	**355.41**
Treas - Alcohol and Tobacco Tax and Trade Bureau	1	1	100.00%	0	0	0.00%	0	3	966.67	0	0	0.00%	0	0

Table B-7a FY 2012 Profile Agency Timeliness Indicators

Agency or Department	Total Number Completed / Ended Counselings (excluding remands)	Total Number Timely Completed / Ended Counselings	% Timely Completed / Ended Counselings	Total Number Completed Investigations	Total Number Timely Completed Investigations	% Investigations Timely Completed	APD All Completed Investigations From Date Complaint Filed	Total Number Complaint Closures	APD All Complaint Closures from Date Complaint Filed	Total Number Merit FADs (No AJ Decision)	Total Number Timely Merit FADs (No AJ Decision)	% Timely Merit FADs (No AJ Decision)	APD Merit FADs (No AJ Decision) from Date FAD Required	APD Merit FADs (No AJ Dec) from Date Complaint Filed / Remanded
Treas - Bureau of Engraving and Printing	31	28	90.32%	13	12	92.31%	160.85	16	478.94	3	2	66.67%	98.33	301.33
Treas - Bureau of the Public Debt	14	14	100.00%	3	2	66.67%	251	2	152.5	1	1	100.00%	55	240
Treas - Departmental Offices	16	15	93.75%	8	8	100.00%	156.75	16	454.94	4	3	75.00%	38.25	242
Treas - Financial Crimes Enforcement Network	5	5	100.00%	1	1	100.00%	173	2	515	2	2	100.00%	32.5	515
Treas - Financial Management Service	15	2	13.33%	6	5	83.33%	149.17	7	647	2	1	50.00%	57	321
Treas - Inspector General For Tax Administration	2	2	100.00%	1	1	100.00%	185	1	917	0	0	0.00%	0	0
Treas - Internal Revenue Service	587	582	99.15%	225	193	85.78%	204.01	283	460.39	95	85	89.47%	39.08	368.08
Treas - Office of the Comptroller of the Currency	17	17	100.00%	5	5	100.00%	100.8	9	278.78	2	2	100.00%	27	185.5
Treas - Special Inspector General for the Trouble Assets Relief Program	0	0	0.00%	0	0	0.00%	0	1	478	0	0	0.00%	0	0
Treas - U. S. Mint	50	47	94.00%	17	16	94.12%	205.47	57	488.35	12	10	83.33%	44.58	341.17
Treas -Internal Revenue Service Office of the Chief	7	7	100.00%	4	4	100.00%	164.25	9	487.22	2	2	100.00%	30.5	249.5
Treas- Office of the Inspector General	1	1	100.00%	2	1	50.00%	189.5	1	472	0	0	0.00%	0	0
Department of Transportation Wide	**541**	**506**	**93.53%**	**216**	**214**	**99.07%**	**136.06**	**335**	**411.26**	**89**	**47**	**52.81%**	**75.36**	**413.53**
DOT Federal Aviation Administration	437	432	98.86%	178	176	98.88%	136.69	268	408.8	75	35	46.67%	79.64	417.48
DOT Federal Highway Administration	27	27	100.00%	7	7	100.00%	117	10	518.4	4	2	50.00%	62.25	426
DOT Federal Motor Carrier Safety Administration	8	8	100.00%	2	2	100.00%	143.5	7	484.14	2	2	100.00%	41.5	221
DOT Federal Railroad Administrataion	4	0	0.00%	2	2	100.00%	133	6	341.5	1	1	100.00%	39	254
DOT Federal Transit Administration	11	10	90.91%	4	4	100.00%	125.75	3	44.67	0	0	0.00%	0	0
DOT Maritime Administration	13	3	23.08%	7	7	100.00%	134.43	11	460.91	1	1	100.00%	48	671
DOT National Highway Traffic Safety Administration	10	7	70.00%	7	7	100.00%	106.29	5	128.2	1	1	100.00%	54	169
DOT Office of Inspector General	3	3	100.00%	1	1	100.00%	175	3	702.67	1	1	100.00%	43	469
DOT Office of the Secretary	11	11	100.00%	1	1	100.00%	128	8	411.88	1	1	100.00%	59	275
DOT Pipeline & Hazardous Materials Safety Admin	8	2	25.00%	1	1	100.00%	177	1	12	0	0	0.00%	0	0
DOT Research & Innovative Technology Admin	9	3	33.33%	6	6	100.00%	170	13	487	3	3	100.00%	53	503
DOT St. Lawrence Development Corporation	0	0	0.00%	0	0	0.00%	0	0	0	0	0	0.00%	0	0
Department of Veterans Affairs Wide	**4,484**	**4,407**	**98.28%**	**1,583**	**1,391**	**87.87%**	**164.52**	**2,123**	**393.83**	**597**	**30**	**5.03%**	**177.88**	**464.04**
VA-HQ and Others	165	163	98.79%	71	58	81.69%	168.08	106	327.84	18	2	11.11%	181	402.39
VA-NCA	50	49	98.00%	18	17	94.44%	162.17	20	441.35	6	0	0.00%	175	593.83
VA-Veterans Benefits Administration	295	291	98.64%	108	101	93.52%	162.39	149	349.44	44	4	9.09%	196.05	468.64
VA-Veterans Health Administration	3,974	3,904	98.24%	1,386	1,215	87.66%	164.54	1,848	400.68	529	24	4.54%	176.3	464.29

Table B-7a FY 2012 Profile Agency Timeliness Indicators

Agency or Department	Total Number Completed / Ended Counselings (excluding remands)	Total Number Timely Completed / Ended Counselings	% Timely Completed / Ended Counselings	Total Number Completed Investigations	Total Number Timely Completed Investigations	% Investigations Timely Completed	APD All Completed Investigations From Date Complaint Filed	Total Number Complaint Closures	APD All Complaint Closures from Date Complaint Filed	Total Number Merit FADs (No AJ Decision)	Total Number Timely Merit FADs (No AJ Decision)	% Timely Merit FADs (No AJ Decision)	APD Merit FADs (No AJ Decision) from Date FAD Required	APD Merit FADs (No AJ Dec) from Date Complaint Filed / Remanded
Federal Housing Finance Agency Wide	**16**	**15**	**93.75%**	**3**	**2**	**66.67%**	**225**	**6**	**199.83**	**0**	**0**	**0.00%**	**0**	**0**
Federal Housing Finance Agency Hqtrs	13	12	92.31%	2	1	50.00%	249	6	199.83	0	0	0.00%	0	0
Federal Housing Finance Agency OIG	3	3	100.00%	1	1	100.00%	177	0	0	0	0	0.00%	0	0
General Services Administration Wide	**158**	**156**	**98.73%**	**77**	**44**	**57.14%**	**265.82**	**85**	**425.05**	**21**	**15**	**71.43%**	**59.19**	**397.57**
GSA Central Office	40	40	100.00%	17	6	35.29%	343.82	15	352.93	6	4	66.67%	67.17	478
GSA National Capital Region	16	16	100.00%	11	6	54.55%	260.36	20	512.9	5	3	60.00%	48	388.8
GSA Region 1	3	3	100.00%	1	1	100.00%	148	0	0	0	0	0.00%	0	0
GSA Region 10	2	2	100.00%	2	2	100.00%	134	2	96.5	0	0	0.00%	0	0
GSA Region 2	19	19	100.00%	9	3	33.33%	249.44	7	706.29	0	0	0.00%	0	0
GSA Region 3	11	11	100.00%	5	1	20.00%	396	9	424.67	5	4	80.00%	66.6	398.2
GSA Region 4	19	17	89.47%	6	3	50.00%	313.67	7	532.71	0	0	0.00%	0	0
GSA Region 5	5	5	100.00%	4	4	100.00%	152	6	515.17	1	0	0.00%	90	285
GSA Region 6	7	7	100.00%	6	5	83.33%	230.33	1	228	1	1	100.00%	58	228
GSA Region 7	6	6	100.00%	0	0	0.00%	0	4	208.25	0	0	0.00%	0	0
GSA Region 8	3	3	100.00%	0	0	0.00%	0	1	21	0	0	0.00%	0	0
GSA Region 9	27	27	100.00%	16	13	81.25%	202.88	13	285.85	3	3	100.00%	39.67	344.33
U.S. Postal Service Wide	**13,121**	**12,906**	**98.36%**	**2,660**	**2,636**	**99.10%**	**112.86**	**4,579**	**275.45**	**1,088**	**1,062**	**97.61%**	**32.41**	**277.48**
USPS Capital Metro Area Operations	1,613	1,596	98.95%	319	314	98.43%	119.84	617	319.67	132	128	96.97%	36.21	307.36
USPS Eastern Area	1,726	1,686	97.68%	406	404	99.51%	108.4	677	320.16	167	156	93.41%	30.74	306.01
USPS Great Lakes Area	1,477	1,454	98.44%	302	298	98.68%	114.29	550	253.35	146	143	97.95%	36.18	311.41
USPS Headquarters	140	135	96.43%	55	55	100.00%	112.6	86	342.92	21	21	100.00%	32.43	281.52
USPS Northeast Area	1,553	1,522	98.00%	271	270	99.63%	116.3	397	293.33	86	86	100.00%	33.33	277.94
USPS Office of Inspector General	21	21	100.00%	7	7	100.00%	105.57	14	365.64	1	1	100.00%	49	153
USPS Pacific Area	1,823	1,804	98.96%	331	329	99.40%	110.13	493	322.28	101	99	98.02%	29.73	257.64
USPS Southern Area	3,275	3,225	98.47%	641	637	99.38%	112.13	1,126	216.11	288	284	98.61%	30.9	246.79
USPS Western Area	1,493	1,463	97.99%	328	322	98.17%	111.83	619	249.9	146	144	98.63%	31.27	258.17

Table B-8 FY 2012 Complaints Filed Bases and Issues - Grand Total

ISSUES OF ALLEGED DISCRIMINATION	BASES OF ALLEGED DISCRIMINATION																				TOTAL BASES BY ISSUE	TOTAL COMPLAINTS BY ISSUE	TOTAL COMPLAINANTS BY ISSUE
	RACE						COLOR	RELIGION	REPRISAL	SEX		PREGNANCY DISCRIMINATION ACT	NATIONAL ORIGIN		EQUAL PAY ACT		AGE	DISABILITY		GINA			
	AMERICAN INDIAN / ALASKA NATIVE	ASIAN	NATIVE HAWAIIAN/ OTHER PACIFIC ISLANDER	BLACK/ AFRICAN AMERICAN	WHITE	TWO OR MORE RACES				MALE	FEMALE		HISPANIC	OTHER	MALE	FEMALE		MENTAL	PHYSICAL				
Appointment/Hire	8	26	3	163	52	8	80	25	235	92	126	4	22	72	0	0	290	52	152	0	1,410	683	668
Assignment Of Duties	18	42	6	459	148	16	220	71	784	200	430	11	67	120	0	0	528	118	337	1	3,576	1,558	1,544
Awards	3	8	0	93	12	0	31	9	154	33	66	0	11	22	0	0	77	15	35	1	570	268	266
Conversion To Full Time	1	2	0	6	2	0	7	0	6	4	9	0	2	1	0	0	13	1	6	0	60	29	29
Disciplinary Action	28	78	5	994	327	34	537	200	2,120	554	865	27	134	262	0	0	1,167	394	953	7	8,685	3,789	3,653
A. Demotion	1	2	0	42	8	2	13	4	63	23	34	0	6	8	0	0	53	9	24	0	292	131	130
B. Reprimand	9	28	2	294	100	12	180	63	717	158	306	3	37	77	0	0	401	103	279	5	2,774	1,207	1,199
C. Suspension	8	22	1	278	99	9	155	75	636	165	240	9	42	90	0	0	346	114	285	2	2,576	1,115	998
D. Removal	7	18	1	203	59	5	117	33	391	110	175	5	31	55	0	0	214	105	228	0	1,757	761	756
5. Other	3	8	1	177	61	6	72	25	313	98	110	5	18	32	0	0	153	63	137	0	1,282	575	570
Duty Hours	6	15	1	193	54	5	85	40	344	92	190	3	25	48	0	0	203	53	206	1	1,564	690	685
Evaluation/Appraisal	18	36	3	398	78	18	175	67	800	157	299	5	61	121	0	0	424	111	242	1	3,014	1,341	1,329
Examination/Test	1	1	0	10	2	0	3	2	14	8	10	0	0	3	0	0	17	1	10	0	82	43	43
Harassment	51	163	14	1,576	441	62	674	298	3,427	775	2,051	25	291	452	0	0	1,750	608	1,414	11	14,083	6,482	6,299
A. Non-Sexual	51	163	14	1,576	441	62	674	298	3,292	690	1,670	24	291	452	0	0	1,750	608	1,414	11	13,481	5,991	5,810
B. Sexual									135	85	381	1									602	491	489
Medical Examination	0	3	0	18	5	0	11	4	49	6	14	0	2	4	0	0	24	24	50	0	214	102	101
Pay Including Overtime	6	18	3	259	80	12	139	50	497	118	241	5	32	69	13	33	293	62	250	1	2,181	968	950
Promotion/Non-Selection	14	53	11	710	189	19	264	82	876	323	504	6	122	172	0	0	1,029	111	355	5	4,845	2,250	2,203
Reassignment	9	30	4	222	74	6	116	27	428	108	226	3	36	77	0	0	312	64	198	2	1,942	859	855
A. Denied	3	16	0	76	31	3	50	13	138	40	89	0	12	32	0	0	105	24	75	2	709	305	303
B. Directed	6	14	4	146	43	3	66	14	290	68	137	3	24	45	0	0	207	40	123	0	1,233	554	552
Reasonable Acommodation								61	534									315	1,004	0	1,914	1,283	1,259
Reinstatement	0	1	0	9	0	1	3	1	15	1	6	1	2	3	0	0	13	8	15	0	79	41	41
Retirement	1	2	0	24	11	0	14	6	57	15	19	0	4	8	0	0	76	18	41	0	296	135	135
Termination	13	36	2	314	69	15	134	66	391	139	234	8	51	104	0	0	280	178	340	2	2,376	1,208	1,203
Terms/Conditions Of Employment	17	53	2	594	229	31	360	110	1,365	345	583	14	88	174	0	0	791	217	684	4	5,661	2,506	2,451
Time And Attendance	14	30	8	354	103	14	179	70	821	162	349	10	54	93	0	0	421	201	529	3	3,415	1,479	1,447
Training	6	17	0	211	39	8	99	29	287	81	147	0	28	46	0	0	184	42	135	2	1,361	571	564
U. Other	3	4	1	137	41	8	55	20	309	67	100	5	24	28	0	0	156	54	150	2	1,164	563	550
Total Issues By Bases	217	618	63	6,744	1,956	257	3,186	1,238	13,513	3,280	6,469	122	1,056	1,879	13	33	8,048	2,647	7,106	43	0	0	0
Total Complaints Filed By Bases	123	381	42	4,042	1,178	167	1,844	672	7,457	1,996	3,841	70	665	1,113	13	33	4,915	1,436	3,950	21			
Total Complainants By Bases	120	373	42	3,886	1,146	161	1,768	647	6,983	1,927	3,751	69	640	1,074	13	33	4,761	1,393	3,802	21			

Table B-8a FY 2012 Complaints Filed Bases and Issues - Cabinet Level Agencies

ISSUES OF ALLEGED DISCRIMINATION	BASES OF ALLEGED DISCRIMINATION																				TOTAL BASES BY ISSUE	TOTAL COMPLAINTS BY ISSUE	TOTAL COMPLAINANTS BY ISSUE
	RACE						COLOR	RELIGION	REPRISAL	SEX			NATIONAL ORIGIN		EQUAL PAY ACT		AGE	DISABILITY		GINA			
	AMERICAN INDIAN / ALASKA NATIVE	ASIAN	NATIVE HAWAIIAN/ OTHER PACIFIC ISLANDER	BLACK/ AFRICAN AMERICAN	WHITE	TWO OR MORE RACES				MALE	FEMALE	PREGNANCY DISCRIMINATION ACT	HISPANIC	OTHER	MALE	FEMALE		MENTAL	PHYSICAL				
Appointment/Hire	6	22	3	137	43	8	66	21	203	82	109	4	22	59	0	0	251	42	136	0	1,214	587	576
Assignment Of Duties	18	37	6	411	125	14	201	63	702	183	384	10	60	101	0	0	462	102	305	1	3,185	1,397	1,386
Awards	3	8	0	73	8	0	27	8	119	22	53	0	9	19	0	0	56	9	26	1	441	215	214
Conversion To Full Time	1	2	0	6	2	0	7	0	6	4	7	0	2	1	0	0	12	1	5	0	56	27	27
Disciplinary Action	28	76	5	936	315	33	518	194	2,028	536	821	27	129	254	0	0	1,111	380	921	7	8,319	3,623	3,490
A. Demotion	1	2	0	32	7	2	11	4	54	21	26	0	6	8	0	0	44	8	22	0	248	114	114
B. Reprimand	9	27	2	276	96	11	170	60	680	153	288	3	34	75	0	0	378	99	268	5	2,634	1,140	1,132
C. Suspension	8	22	1	263	94	9	151	73	610	161	230	9	41	86	0	0	334	108	275	2	2,477	1,068	953
D. Removal	7	17	1	192	57	5	115	33	379	104	171	5	30	53	0	0	206	104	222	0	1,701	740	735
5. Other	3	8	1	173	61	6	71	24	305	97	106	5	18	32	0	0	149	61	134	0	1,254	561	556
Duty Hours	6	15	1	190	52	4	84	36	334	92	182	3	24	44	0	0	197	52	199	1	1,516	672	667
Evaluation/Appraisal	16	31	3	334	62	15	145	55	654	129	253	3	54	96	0	0	337	88	203	1	2,479	1,127	1,118
Examination/Test	1	1	0	8	1	0	2	2	14	8	9	0	0	3	0	0	15	1	10	0	75	40	40
Harassment	46	151	14	1,428	406	60	614	283	3,139	720	1,911	24	268	415	0	0	1,579	544	1,290	10	12,902	5,951	5,793
A. Non-Sexual	46	151	14	1,428	406	60	614	283	3,014	635	1,556	23	268	415	0	0	1,579	544	1,290	10	12,336	5,490	5,334
B. Sexual									125	85	355	1									566	461	459
Medical Examination	0	3	0	17	5	0	10	4	48	6	10	0	2	4	0	0	23	23	50	0	205	96	95
Pay Including Overtime	6	18	3	242	76	11	132	48	475	114	230	5	31	64	11	29	278	54	236	1	2,064	920	903
Promotion/Non-Selection	12	41	9	596	159	16	233	71	743	271	428	6	105	151	0	0	851	95	284	5	4,076	1,921	1,882
Reassignment	9	27	4	205	66	6	111	23	394	99	213	2	33	73	0	0	289	57	181	2	1,794	795	791
A. Denied	3	15	0	65	28	3	48	9	120	37	79	0	10	30	0	0	92	20	68	2	629	271	269
B. Directed	6	12	4	140	38	3	63	14	274	62	134	2	23	43	0	0	197	37	113	0	1,165	524	522
Reasonable Acommodation								57	498									276	927	0	1,758	1,176	1,156
Reinstatement	0	0	0	8	0	0	2	1	14	1	6	1	2	2	0	0	13	8	15	0	73	38	38
Retirement	1	1	0	21	10	0	10	4	51	13	16	0	3	8	0	0	68	14	36	0	256	119	119
Termination	13	32	2	295	63	15	126	60	367	130	218	6	48	96	0	0	262	163	320	1	2,217	1,130	1,125
Terms/Conditions Of Employment	15	49	2	544	215	27	345	99	1,271	331	545	14	84	159	0	0	731	196	636	4	5,267	2,351	2,301
Time And Attendance	14	29	7	320	95	12	165	63	763	153	327	10	50	87	0	0	386	178	495	3	3,157	1,369	1,342
Training	6	14	0	189	33	7	89	27	252	69	132	0	28	40	0	0	158	34	116	2	1,196	504	497
U. Other	2	4	1	128	38	7	52	18	286	65	96	4	24	27	0	0	143	48	139	1	1,083	520	509
Total Issues By Bases	203	561	60	6,088	1,774	235	2,939	1,137	12,361	3,028	5,950	114	978	1,703	11	29	7,222	2,365	6,530	40	0	0	0
Total Complaints Filed By Bases	115	345	39	3,675	1,078	146	1,705	617	6,866	1,849	3,565	64	614	1,026	11	29	4,441	1,300	3,664	19			
Total Complainants By Bases	112	338	39	3,545	1,050	146	1,647	598	6,447	1,788	3,484	64	591	997	11	29	4,310	1,265	3,538	19			

Table B-8b FY 2012 Complaints Filed Bases and Issues - Medium Size Agencies

ISSUES OF ALLEGED DISCRIMINATION	BASES OF ALLEGED DISCRIMINATION																				TOTAL BASES BY ISSUE	TOTAL COMPLAINTS BY ISSUE	TOTAL COMPLAINANTS BY ISSUE
	RACE						COLOR	RELIGION	REPRISAL	SEX		PREGNANCY DISCRIMINATION ACT	NATIONAL ORIGIN		EQUAL PAY ACT		AGE	DISABILITY		GINA			
	AMERICAN INDIAN / ALASKA NATIVE	ASIAN	NATIVE HAWAIIAN/ OTHER PACIFIC ISLANDER	BLACK/ AFRICAN AMERICAN	WHITE	TWO OR MORE RACES				MALE	FEMALE		HISPANIC	OTHER	MALE	FEMALE		MENTAL	PHYSICAL				
Appointment/Hire	1	3	0	20	5	0	9	2	22	6	13	0	0	6	0	0	29	8	10	0	134	57	54
Assignment Of Duties	0	4	0	36	13	2	12	5	64	10	33	0	5	13	0	0	46	13	26	0	282	110	109
Awards	0	0	0	13	4	0	3	1	28	7	9	0	2	2	0	0	15	3	9	0	96	37	36
Conversion To Full Time	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	1	0	1	0	4	2	2
Disciplinary Action	0	1	0	34	7	0	14	3	70	11	27	0	3	5	0	0	37	11	24	0	247	107	105
A. Demotion	0	0	0	7	1	0	2	0	6	1	7	0	0	0	0	0	8	1	2	0	35	14	13
B. Reprimand	0	0	0	9	3	0	8	2	27	3	10	0	1	2	0	0	13	3	6	0	87	36	36
C. Suspension	0	0	0	9	2	0	2	0	19	3	4	0	1	1	0	0	6	4	9	0	60	31	30
D. Removal	0	1	0	7	1	0	1	0	11	4	4	0	1	2	0	0	6	1	4	0	43	16	16
5. Other	0	0	0	2	0	0	1	1	7	0	2	0	0	0	0	0	4	2	3	0	22	10	10
Duty Hours	0	0	0	2	2	1	1	3	9	0	8	0	1	4	0	0	6	1	6	0	44	14	14
Evaluation/Appraisal	1	4	0	47	12	1	22	9	115	20	38	0	5	18	0	0	68	14	30	0	404	161	159
Examination/Test	0	0	0	1	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	4	2	2
Harassment	3	8	0	111	25	2	49	12	228	37	109	1	20	30	0	0	130	48	97	0	910	400	379
A. Non-Sexual	3	8	0	111	25	2	49	12	218	37	88	1	20	30	0	0	130	48	97	0	879	375	354
B. Sexual									10	0	21	0									31	25	25
Medical Examination	0	0	0	1	0	0	1	0	1	0	3	0	0	0	0	0	0	0	0	0	6	4	4
Pay Including Overtime	0	0	0	16	3	0	7	2	19	3	10	0	1	5	0	1	13	7	12	0	99	35	34
Promotion/Non-Selection	2	12	2	91	28	1	27	9	116	39	62	0	14	18	0	0	154	16	66	0	657	275	267
Reassignment	0	3	0	10	8	0	3	1	26	5	10	0	2	3	0	0	15	6	13	0	105	45	45
A. Denied	0	1	0	8	3	0	2	1	15	1	9	0	2	2	0	0	10	4	6	0	64	26	26
B. Directed	0	2	0	2	5	0	1	0	11	4	1	0	0	1	0	0	5	2	7	0	41	19	19
Reasonable Acommodation								2	23									23	61	0	109	78	76
Reinstatement	0	1	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	4	2	2
Retirement	0	1	0	3	1	0	4	2	6	2	3	0	1	0	0	0	7	4	5	0	39	15	15
Termination	0	2	0	12	2	0	3	3	20	6	12	2	3	5	0	0	12	14	16	0	112	56	56
Terms/Conditions Of Employment	0	2	0	35	11	2	12	8	74	12	29	0	4	14	0	0	44	15	38	0	300	106	103
Time And Attendance	0	1	1	25	7	1	11	5	49	8	17	0	4	6	0	0	28	19	29	0	211	92	89
Training	0	2	0	17	5	0	7	2	29	10	11	0	0	6	0	0	18	8	16	0	131	50	50
U. Other	1	0	0	5	1	0	1	1	18	1	2	0	0	1	0	0	6	5	9	0	51	25	23
Total Issues By Bases	8	44	3	480	135	10	186	70	918	177	399	3	65	137	0	1	630	215	468	0	0	0	0
Total Complaints Filed By Bases	5	28	3	271	72	10	109	40	465	102	207	3	44	64	0	1	374	98	233	0			
Total Complainants By Bases	5	27	3	251	70	4	91	35	417	95	201	3	42	56	0	1	355	92	216	0			

Table B-8c FY 2012 Complaints Filed Bases and Issues - Small Size Agencies

ISSUES OF ALLEGED DISCRIMINATION	BASES OF ALLEGED DISCRIMINATION																				TOTAL BASES BY ISSUE	TOTAL COMPLAINTS BY ISSUE	TOTAL COMPLAINANTS BY ISSUE
	RACE						COLOR	RELIGION	REPRISAL	SEX			NATIONAL ORIGIN		EQUAL PAY ACT		AGE	DISABILITY		GINA			
	AMERICAN INDIAN / ALASKA NATIVE	ASIAN	NATIVE HAWAIIAN/ OTHER PACIFIC ISLANDER	BLACK/ AFRICAN AMERICAN	WHITE	TWO OR MORE RACES				MALE	FEMALE	PREGNANCY DISCRIMINATION ACT	HISPANIC	OTHER	MALE	FEMALE		MENTAL	PHYSICAL				
Appointment/Hire	1	1	0	6	4	0	5	2	10	4	4	0	0	7	0	0	10	2	6	0	62	39	38
Assignment Of Duties	0	1	0	12	10	0	7	3	18	7	13	1	1	6	0	0	19	3	6	0	107	50	48
Awards	0	0	0	7	0	0	1	0	7	4	4	0	0	1	0	0	6	3	0	0	33	16	16
Conversion To Full Time	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Disciplinary Action	0	1	0	24	5	1	5	3	22	7	17	0	1	3	0	0	18	3	8	0	118	58	57
A. Demotion	0	0	0	3	0	0	0	0	3	1	1	0	0	0	0	0	1	0	0	0	9	3	3
B. Reprimand	0	1	0	9	1	1	2	1	10	2	8	0	1	0	0	0	9	1	5	0	51	30	30
C. Suspension	0	0	0	6	3	0	2	2	7	1	6	0	0	3	0	0	6	2	1	0	39	16	15
D. Removal	0	0	0	4	1	0	1	0	1	2	0	0	0	0	0	0	2	0	2	0	13	5	5
5. Other	0	0	0	2	0	0	0	0	1	1	2	0	0	0	0	0	0	0	0	0	6	4	4
Duty Hours	0	0	0	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	1	0	4	4	4
Evaluation/Appraisal	1	1	0	17	4	2	8	3	31	8	8	2	1	7	0	0	17	9	9	0	128	51	50
Examination/Test	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	3	1	1
Harassment	2	4	0	37	10	0	11	3	60	18	31	0	3	7	0	0	41	16	27	1	271	131	127
A. Non-Sexual	2	4	0	37	10	0	11	3	60	18	26	0	3	7	0	0	41	16	27	1	266	126	122
B. Sexual									0	0	5	0									5	5	5
Medical Examination	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1	0	0	3	2	2
Pay Including Overtime	0	0	0	1	1	1	0	0	3	1	1	0	0	0	2	3	2	1	2	0	18	13	13
Promotion/Non-Selection	0	0	0	23	2	2	4	2	17	13	14	0	2	3	0	0	24	0	5	0	111	53	53
Reassignment	0	0	0	7	0	0	2	3	8	4	3	1	1	1	0	0	8	1	4	0	43	19	19
A. Denied	0	0	0	3	0	0	0	3	3	2	1	0	0	0	0	0	3	0	1	0	16	8	8
B. Directed	0	0	0	4	0	0	2	0	5	2	2	1	1	1	0	0	5	1	3	0	27	11	11
Reasonable Acommodation								2	13									16	16	0	47	29	27
Reinstatement	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	2	1	1
Retirement	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	1	1
Termination	0	2	0	7	4	0	5	3	4	3	4	0	0	3	0	0	6	1	4	1	47	22	22
Terms/Conditions Of Employment	2	2	0	15	3	2	3	3	20	2	9	0	0	1	0	0	16	6	10	0	94	49	47
Time And Attendance	0	0	0	9	1	1	3	2	9	1	5	0	0	0	0	0	7	4	5	0	47	18	16
Training	0	1	0	5	1	1	3	0	6	2	4	0	0	0	0	0	8	0	3	0	34	17	17
U. Other	0	0	0	4	2	1	2	1	5	1	2	1	0	0	0	0	7	1	2	1	30	18	18
Total Issues By Bases	6	13	0	176	47	12	61	31	234	75	120	5	9	39	2	3	192	67	108	3	0	0	0
Total Complaints Filed By Bases	3	8	0	96	28	11	30	15	126	45	69	3	6	23	2	3	98	38	53	2			
Total Complainants By Bases	3	8	0	90	26	11	30	14	119	44	66	2	6	21	2	3	94	36	48	2			

Table B-9 FY 2012 Timeliness and Cost of All Completed Complaint Investigations

Agency or Department	Total Number Completed Investigations	Average Processing Days Completed Investigations	Number Timely Completed within 180 Days	Number Timely Completed within 181-360 Days	Total Number Timely Completed Investigations	% Investigations Timely Completed	Total Cost All Completed Investigations	Average Cost All Completed Investigations
Advisory Council on Historic Preservation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
African Development Foundation	0	0	0	0	0	0.00%	$0.00	$0.00
Agency for International Development	13	282.38	1	0	1	7.69%	$30,971.00	$2,382.38
American Battle Monuments Commission	0	0	0	0	0	0.00%	$0.00	$0.00
Appalachian Regional Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Architectural and Transportation Barriers Compliance Board	0	0	0	0	0	0.00%	$0.00	$0.00
Arctic Research Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Armed Forces Retirement Home	0	0	0	0	0	0.00%	$0.00	$0.00
Barry Goldwater Scholarship and Excellence in Education Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Broadcasting Board of Governors	5	161.2	4	1	5	100.00%	$27,000.00	$5,400.00
Central Intelligence Agency	14	345.57	0	1	1	7.14%	$272,714.68	$19,479.62
Chemical Safety and Hazard Investigation Board	0	0	0	0	0	0.00%	$0.00	$0.00
Christopher Columbus Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission of Fine Arts	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission on Civil Rights	0	0	0	0	0	0.00%	$0.00	$0.00
Committee for Purchase from People Who Are Blind or Severely Disabled	0	0	0	0	0	0.00%	$0.00	$0.00
Commodity Futures Trading Commission	1	110	1	0	1	100.00%	$6,750.00	$6,750.00
Consumer Financial Protection Bureau	3	209	0	3	3	100.00%	$23,469.60	$7,823.20
Consumer Product Safety Commission	4	142.25	4	0	4	100.00%	$19,616.00	$4,904.00
Corporation for National and Community Service	6	108.67	5	1	6	100.00%	$27,107.00	$4,517.83
Court Services and Offender Supervision Agency for the District of Columbia	6	165	4	0	4	66.67%	$22,512.00	$3,752.00
Defense Army and Air Force Exchange	38	234.79	2	3	5	13.16%	$446,869.22	$11,759.72
Defense Commissary Agency	58	256.97	12	2	14	24.14%	$257,328.02	$4,436.69
Defense Contract Audit Agency	12	264	0	3	3	25.00%	$53,240.28	$4,436.69
Defense Contract Management Agency	3	328.67	0	0	0	0.00%	$13,310.07	$4,436.69
Defense Finance and Accounting Service	20	244.55	2	9	11	55.00%	$88,733.80	$4,436.69
Defense Human Resources Activity	0	0	0	0	0	0.00%	$0.00	$0.00
Defense Information Systems Agency	4	260.75	0	0	0	0.00%	$28,003.28	$7,000.82
Defense Intelligence Agency	14	314.36	0	5	5	35.71%	$60,876.97	$4,348.36
Defense Joint Task Force National Capital Region Medical	1	315	0	0	0	0.00%	$3,025.00	$3,025.00

Table B-9 FY 2012 Timeliness and Cost of All Completed Complaint Investigations

Agency or Department	Total Number Completed Investigations	Average Processing Days Completed Investigations	Number Timely Completed within 180 Days	Number Timely Completed within 181-360 Days	Total Number Timely Completed Investigations	% Investigations Timely Completed	Total Cost All Completed Investigations	Average Cost All Completed Investigations
Defense Logistics Agency	52	272.19	4	8	12	23.08%	$464,213.36	$8,927.18
Defense Media Activity	0	0	0	0	0	0.00%	$0.00	$0.00
Defense Missile Defense Agency	1	237	0	0	0	0.00%	$4,437.00	$4,437.00
Defense National Geospatial-Intelligence Agency	17	179.47	10	7	17	100.00%	$75,423.73	$4,436.69
Defense National Guard Bureau	0	0	0	0	0	0.00%	$0.00	$0.00
Defense National Security Agency	30	332.5	2	19	21	70.00%	$303,746.90	$10,124.90
Defense Nuclear Facilities Safety Board	0	0	0	0	0	0.00%	$0.00	$0.00
Defense Office of the Inspector General	1	255	0	1	1	100.00%	$9,895.00	$9,895.00
Defense Office of the Secretary - Wash. Hqtrs. Services	19	247.68	3	12	15	78.95%	$172,330.74	$9,070.04
Defense Security Service	5	193	0	0	0	0.00%	$22,185.00	$4,437.00
Defense Technical Information Center	0	0	0	0	0	0.00%	$0.00	$0.00
Defense Threat Reduction Agency	0	0	0	0	0	0.00%	$0.00	$0.00
Defense TRICARE Management Activity	2	368.5	0	1	1	50.00%	$6,094.00	$3,047.00
Defense Uniformed Services University	0	0	0	0	0	0.00%	$0.00	$0.00
Department of Agriculture	437	241.59	187	30	217	49.66%	$1,535,339.78	$3,513.36
Department of Commerce	183	188.25	95	71	166	90.71%	$1,045,662.42	$5,714.00
Department of Defense Education Activity	54	176.35	36	14	50	92.59%	$186,303.89	$3,450.07
Department of Education	26	179	17	9	26	100.00%	$90,427.61	$3,477.99
Department of Energy	51	178.84	23	19	42	82.35%	$133,184.06	$2,611.45
Department of Health and Human Services	288	153.41	232	37	269	93.40%	$1,233,362.06	$4,282.51
Department of Homeland Security	1,046	229.94	427	169	596	56.98%	$4,963,672.94	$4,745.39
Department of Housing and Urban Development	77	285.31	20	6	26	33.77%	$201,354.00	$2,614.99
Department of Justice	614	202.46	302	181	483	78.66%	$2,575,296.36	$4,194.29
Department of Labor	85	204.12	51	32	83	97.65%	$262,000.00	$3,082.35
Department of State	97	245.01	27	25	52	53.61%	$284,655.00	$2,934.59
Department of the Air Force	305	263.15	36	17	53	17.38%	$1,353,190.40	$4,436.69
Department of the Army	484	258.31	66	48	114	23.55%	$3,014,704.36	$6,228.73
Department of the Interior	238	270.06	87	36	123	51.68%	$781,905.60	$3,285.32
Department of the Navy	409	276.71	41	121	162	39.61%	$3,715,910.00	$9,085.35
Department of the Treasury	285	197.5	135	113	248	87.02%	$2,229,613.00	$7,823.20
Department of Transportation	216	136.06	196	18	214	99.07%	$1,376,310.00	$6,371.81
Department of Veterans Affairs	1,583	164.52	1,258	133	1,391	87.87%	$9,137,264.70	$5,772.12
Election Assistance Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Environmental Protection Agency	61	354.98	1	8	9	14.75%	$138,948.50	$2,277.84

Table B-9 FY 2012 Timeliness and Cost of All Completed Complaint Investigations

Agency or Department	Total Number Completed Investigations	Average Processing Days Completed Investigations	Number Timely Completed within 180 Days	Number Timely Completed within 181-360 Days	Total Number Timely Completed Investigations	% Investigations Timely Completed	Total Cost All Completed Investigations	Average Cost All Completed Investigations
Equal Employment Opportunity Commission	13	239.69	4	8	12	92.31%	$84,000.00	$6,461.54
Export-Import Bank of the US	1	240	0	1	1	100.00%	$6,238.58	$6,238.58
Farm Credit Administration	0	0	0	0	0	0.00%	$0.00	$0.00
Farm Credit System Insurance Corporation	0	0	0	0	0	0.00%	$0.00	$0.00
Federal Communications Commission	10	39	0	10	10	100.00%	$36,000.00	$3,600.00
Federal Deposit Insurance Corporation	29	224.21	13	16	29	100.00%	$165,049.44	$5,691.36
Federal Election Commission	0	0	0	0	0	0.00%	$0.00	$0.00
Federal Energy Regulatory Commission	6	180	6	0	6	100.00%	$21,000.00	$3,500.00
Federal Financial Institutions Examination Council	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Housing Finance Agency	3	225	1	1	2	66.67%	$14,509.00	$4,836.33
Federal Labor Relations Authority	1	248	0	1	1	100.00%	$7,649.00	$7,649.00
Federal Maritime Commission	0	0	0	0	0	0.00%	$0.00	$0.00
Federal Mediation and Conciliation Service	0	0	0	0	0	0.00%	$0.00	$0.00
Federal Mine Safety & Health Review Commission	0	0	0	0	0	0.00%	$0.00	$0.00
Federal Reserve System--Board of Governors	5	151	4	1	5	100.00%	$41,956.10	$8,391.22
Federal Retirement Thrift Investment Board	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Trade Commission	0	0	0	0	0	0.00%	$0.00	$0.00
General Services Administration	77	265.82	23	21	44	57.14%	$230,204.61	$2,989.67
Government Printing Office	26	274.27	1	11	12	46.15%	$79,107.00	$3,042.58
Harry S. Truman Scholarship Foundation	0	0	0	0	0	0.00%	$0.00	$0.00
Holocaust Memorial Museum U.S.	0	0	0	0	0	0.00%	$0.00	$0.00
Institute of Museum and Library Services	0	0	0	0	0	0.00%	$0.00	$0.00
Inter-American Foundation	0	0	0	0	0	0.00%	$0.00	$0.00
International Boundary and Water Commission	0	0	0	0	0	0.00%	$0.00	$0.00
International Joint Commission: US & Canada	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
International Trade Commission	2	161.5	1	0	1	50.00%	$10,344.00	$5,172.00
James Madison Memorial Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Japan-United States Friendship Commission	0	0	0	0	0	0.00%	$0.00	$0.00
John F. Kennedy Center for the Performing Arts	1	61	1	0	1	100.00%	$3,974.00	$3,974.00
Marine Mammal Commission	0	0	0	0	0	0.00%	$0.00	$0.00
Merit Systems Protection Board	1	148	1	0	1	100.00%	$5,619.00	$5,619.00
Millennium Challenge Corporation	0	0	0	0	0	0.00%	$0.00	$0.00
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Aeronautics and Space Administration	21	193.57	10	7	17	80.95%	$91,245.88	$4,345.04

Table B-9 FY 2012 Timeliness and Cost of All Completed Complaint Investigations

Agency or Department	Total Number Completed Investigations	Average Processing Days Completed Investigations	Number Timely Completed within 180 Days	Number Timely Completed within 181-360 Days	Total Number Timely Completed Investigations	% Investigations Timely Completed	Total Cost All Completed Investigations	Average Cost All Completed Investigations
National Archives and Records Administration	3	170	2	1	3	100.00%	$11,477.43	$3,825.81
National Capital Planning Commission	0	0	0	0	0	0.00%	$0.00	$0.00
National Council on Disability	0	0	0	0	0	0.00%	$0.00	$0.00
National Credit Union Administration	3	217	1	1	2	66.67%	$15,830.00	$5,276.67
National Endowment for the Arts	0	0	0	0	0	0.00%	$0.00	$0.00
National Endowment for the Humanities	0	0	0	0	0	0.00%	$0.00	$0.00
National Foundation on the Arts & the Humanities	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Gallery of Art	0	0	0	0	0	0.00%	$0.00	$0.00
National Indian Gaming Commission	2	266	0	1	1	50.00%	$9,903.00	$4,951.50
National Labor Relations Board	3	167.33	3	0	3	100.00%	$29,953.00	$9,984.33
National Mediation Board	0	0	0	0	0	0.00%	$0.00	$0.00
National Reconnaissance Office	0	0	0	0	0	0.00%	$0.00	$0.00
National Science Foundation	4	371.75	0	0	0	0.00%	$11,940.00	$2,985.00
National Transportation Safety Board	2	111	2	0	2	100.00%	$5,465.00	$2,732.50
Navajo and Hopi Indian Relocation Commission	0	0	0	0	0	0.00%	$0.00	$0.00
Nuclear Regulatory Commission	9	209.44	6	1	7	77.78%	$45,000.00	$5,000.00
Nuclear Waste Technical Review Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Occupational Safety &Health Review Commission	0	0	0	0	0	0.00%	$0.00	$0.00
Office of Government Ethics	0	0	0	0	0	0.00%	$0.00	$0.00
Office of Personnel Management	25	103.4	25	0	25	100.00%	$191,010.20	$7,640.41
Office of Special Counsel	0	0	0	0	0	0.00%	$0.00	$0.00
Office of the Director of National Intelligence	0	0	0	0	0	0.00%	$0.00	$0.00
Overseas Private Investment Corporation	0	0	0	0	0	0.00%	$0.00	$0.00
Peace Corps	4	156.75	3	1	4	100.00%	$16,786.00	$4,196.50
Pension Benefit Guaranty Corporation	7	194.14	3	3	6	85.71%	$18,000.00	$2,571.43
Postal Regulatory Commission	0	0	0	0	0	0.00%	$0.00	$0.00
Presidio Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Railroad Retirement Board	4	178	4	0	4	100.00%	$8,090.00	$2,022.50
Securities and Exchange Commission	10	259.7	4	4	8	80.00%	$36,258.26	$3,625.83
Selective Service System	2	288	0	2	2	100.00%	$3,864.00	$1,932.00
Small Business Administration	33	204.09	12	18	30	90.91%	$111,641.00	$3,383.06
Smithsonian Institution	8	173.5	7	1	8	100.00%	$19,250.00	$2,406.25
Social Security Administration	339	194.84	222	57	279	82.30%	$1,520,762.08	$4,486.02
Tennessee Valley Authority	44	138.2	44	0	44	100.00%	$83,258.59	$1,892.24
Trade and Development Agency	0	0	0	0	0	0.00%	$0.00	$0.00

Table B-9 FY 2012 Timeliness and Cost of All Completed Complaint Investigations

Agency or Department	Total Number Completed Investigations	Average Processing Days Completed Investigations	Number Timely Completed within 180 Days	Number Timely Completed within 181-360 Days	Total Number Timely Completed Investigations	% Investigations Timely Completed	Total Cost All Completed Investigations	Average Cost All Completed Investigations
U.S. Postal Service	2,660	112.86	2,562	74	2,636	99.10%	$4,395,336.75	$1,652.38
Utah Reclamation Mitigation and Conservation Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Valles Caldera Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Cabinet Level Subtotal Including USPS	9,415	184.54	5,833	1,223	7,056	74.94%	$40,525,205.30	$4,304.32
Midsize Agencies Subtotal	640	212.74	357	131	488	76.25%	$2,574,839.90	$4,023.19
Small Agencies Subtotal	171	219.08	66	50	116	67.84%	$929,634.05	$5,436.46
Micro Agencies Subtotal	0	0	0	0	0	0.00%	$0.00	$0.00
Government-wide Including USPS	10,226	186.89	6,256	1,404	7,660	74.91%	$44,029,679.25	$4,305.66
USPS Percentage of Cabinet Sub Total	28.25%		43.92%	6.05%	37.36%		10.85%	
USPS Percentage of Government-wide	26.01%		40.95%	5.27%	34.41%		9.98%	
Cabinet Level Subtotal Minus USPS	6,755	212.77	3,271	1,149	4,420	65.43%	$36,129,868.55	$5,348.61
Government-wide Minus USPS	7,566	212.91	3,694	1,330	5,024	66.40%	$39,634,342.50	$5,238.48

NRF= No Report Filed

Table B-9a FY 2012 Timeliness and Cost of Complaint Investigations Completed by Agency Investigators								
Agency or Department	Total Number Completed Investigations By Agency	Average Processing Days Completed Investigations By Agency	Number Timely Completed within 180 Days	Number Timely Completed within 181-360 Days	Total Number Timely Completed Investigations By Agency	% Investigations Timely Completed By Agency	Total Cost Completed Investigations By Agency	Average Cost Completed Investigations By Agency
Advisory Council on Historic Preservation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
African Development Foundation	0	0	0	0	0	0.00%	$0.00	$0.00
Agency for International Development	2	350	0	0	0	0.00%	$2,492.00	$1,246.00
American Battle Monuments Commission	0	0	0	0	0	0.00%	$0.00	$0.00
Appalachian Regional Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Architectural and Transportation Barriers Compliance Board	0	0	0	0	0	0.00%	$0.00	$0.00
Arctic Research Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Armed Forces Retirement Home	0	0	0	0	0	0.00%	$0.00	$0.00
Barry Goldwater Scholarship and Excellence in Education Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Broadcasting Board of Governors	0	0	0	0	0	0.00%	$13,500.00	$0.00
Central Intelligence Agency	11	351.91	0	1	1	9.09%	$200,555.20	$18,232.29
Chemical Safety and Hazard Investigation Board	0	0	0	0	0	0.00%	$0.00	$0.00
Christopher Columbus Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission of Fine Arts	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission on Civil Rights	0	0	0	0	0	0.00%	$0.00	$0.00
Committee for Purchase from People Who Are Blind or Severely Disabled	0	0	0	0	0	0.00%	$0.00	$0.00
Commodity Futures Trading Commission	0	0	0	0	0	0.00%	$0.00	$0.00
Consumer Financial Protection Bureau	3	209	0	3	3	100.00%	$23,469.60	$7,823.20
Consumer Product Safety Commission	0	0	0	0	0	0.00%	$9,808.00	$0.00
Corporation for National and Community Service	0	0	0	0	0	0.00%	$0.00	$0.00
Court Services and Offender Supervision Agency for the District of Columbia	2	234.5	0	0	0	0.00%	$4,452.00	$2,226.00
Defense Army and Air Force Exchange	38	234.79	2	3	5	13.16%	$446,869.22	$11,759.72
Defense Commissary Agency	58	256.97	12	2	14	24.14%	$257,328.02	$4,436.69
Defense Contract Audit Agency	12	264	0	3	3	25.00%	$53,240.28	$4,436.69
Defense Contract Management Agency	3	328.67	0	0	0	0.00%	$13,310.07	$4,436.69
Defense Finance and Accounting Service	20	244.55	2	9	11	55.00%	$88,733.80	$4,436.69
Defense Human Resources Activity	0	0	0	0	0	0.00%	$0.00	$0.00
Defense Information Systems Agency	4	260.75	0	0	0	0.00%	$28,003.28	$7,000.82
Defense Intelligence Agency	13	320.77	0	5	5	38.46%	$57,676.97	$4,436.69
Defense Joint Task Force National Capital Region Medical	0	0	0	0	0	0.00%	$0.00	$0.00
Defense Logistics Agency	52	272.19	4	8	12	23.08%	$464,213.36	$8,927.18

Table B-9a FY 2012 Timeliness and Cost of Complaint Investigations Completed by Agency Investigators								
Agency or Department	Total Number Completed Investigations By Agency	Average Processing Days Completed Investigations By Agency	Number Timely Completed within 180 Days	Number Timely Completed within 181-360 Days	Total Number Timely Completed Investigations By Agency	% Investigations Timely Completed By Agency	Total Cost Completed Investigations By Agency	Average Cost Completed Investigations By Agency
Defense Media Activity	0	0	0	0	0	0.00%	$0.00	$0.00
Defense Missile Defense Agency	1	237	0	0	0	0.00%	$4,437.00	$4,437.00
Defense National Geospatial-Intelligence Agency	17	179.47	10	7	17	100.00%	$75,423.73	$4,436.69
Defense National Guard Bureau	0	0	0	0	0	0.00%	$0.00	$0.00
Defense National Security Agency	30	332.5	2	19	21	70.00%	$303,746.90	$10,124.90
Defense Nuclear Facilities Safety Board	0	0	0	0	0	0.00%	$0.00	$0.00
Defense Office of the Inspector General	1	255	0	1	1	100.00%	$9,895.00	$9,895.00
Defense Office of the Secretary - Wash. Hqtrs. Services	19	247.68	3	12	15	78.95%	$172,330.74	$9,070.04
Defense Security Service	0	0	0	0	0	0.00%	$0.00	$0.00
Defense Technical Information Center	0	0	0	0	0	0.00%	$0.00	$0.00
Defense Threat Reduction Agency	0	0	0	0	0	0.00%	$0.00	$0.00
Defense TRICARE Management Activity	0	0	0	0	0	0.00%	$0.00	$0.00
Defense Uniformed Services University	0	0	0	0	0	0.00%	$0.00	$0.00
Department of Agriculture	0	0	0	0	0	0.00%	$0.00	$0.00
Department of Commerce	6	141.5	4	1	5	83.33%	$21,634.92	$3,605.82
Department of Defense Education Activity	11	266.91	0	8	8	72.73%	$48,803.59	$4,436.69
Department of Education	0	0	0	0	0	0.00%	$0.00	$0.00
Department of Energy	0	0	0	0	0	0.00%	$0.00	$0.00
Department of Health and Human Services	7	141.71	7	0	7	100.00%	$14,500.00	$2,071.43
Department of Homeland Security	321	198.7	202	57	259	80.69%	$2,744,124.03	$8,548.67
Department of Housing and Urban Development	0	0	0	0	0	0.00%	$53,032.00	$0.00
Department of Justice	155	234.64	42	81	123	79.35%	$959,092.32	$6,187.69
Department of Labor	0	0	0	0	0	0.00%	$0.00	$0.00
Department of State	7	213	2	4	6	85.71%	$8,400.00	$1,200.00
Department of the Air Force	305	263.15	36	17	53	17.38%	$1,353,190.40	$4,436.69
Department of the Army	484	258.31	66	48	114	23.55%	$3,014,704.36	$6,228.73
Department of the Interior	0	0	0	0	0	0.00%	$0.00	$0.00
Department of the Navy	409	276.71	41	121	162	39.61%	$3,715,910.00	$9,085.35
Department of the Treasury	285	197.5	135	113	248	87.02%	$2,229,613.00	$7,823.20
Department of Transportation	111	142.22	102	8	110	99.10%	$904,650.00	$8,150.00
Department of Veterans Affairs	1,042	169.31	779	109	888	85.22%	$7,457,612.00	$7,157.02
Election Assistance Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Environmental Protection Agency	37	380.84	1	3	4	10.81%	$97,979.50	$2,648.09
Equal Employment Opportunity Commission	13	239.69	4	8	12	92.31%	$84,000.00	$6,461.54

Table B-9a FY 2012 Timeliness and Cost of Complaint Investigations Completed by Agency Investigators								
Agency or Department	Total Number Completed Investigations By Agency	Average Processing Days Completed Investigations By Agency	Number Timely Completed within 180 Days	Number Timely Completed within 181-360 Days	Total Number Timely Completed Investigations By Agency	% Investigations Timely Completed By Agency	Total Cost Completed Investigations By Agency	Average Cost Completed Investigations By Agency
Export-Import Bank of the US	0	0	0	0	0	0.00%	$0.00	$0.00
Farm Credit Administration	0	0	0	0	0	0.00%	$0.00	$0.00
Farm Credit System Insurance Corporation	0	0	0	0	0	0.00%	$0.00	$0.00
Federal Communications Commission	0	0	0	0	0	0.00%	$0.00	$0.00
Federal Deposit Insurance Corporation	0	0	0	0	0	0.00%	$0.00	$0.00
Federal Election Commission	0	0	0	0	0	0.00%	$0.00	$0.00
Federal Energy Regulatory Commission	0	0	0	0	0	0.00%	$0.00	$0.00
Federal Financial Institutions Examination Council	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Housing Finance Agency	0	0	0	0	0	0.00%	$0.00	$0.00
Federal Labor Relations Authority	0	0	0	0	0	0.00%	$0.00	$0.00
Federal Maritime Commission	0	0	0	0	0	0.00%	$0.00	$0.00
Federal Mediation and Conciliation Service	0	0	0	0	0	0.00%	$0.00	$0.00
Federal Mine Safety & Health Review Commission	0	0	0	0	0	0.00%	$0.00	$0.00
Federal Reserve System--Board of Governors	0	0	0	0	0	0.00%	$0.00	$0.00
Federal Retirement Thrift Investment Board	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Trade Commission	0	0	0	0	0	0.00%	$0.00	$0.00
General Services Administration	0	0	0	0	0	0.00%	$0.00	$0.00
Government Printing Office	0	0	0	0	0	0.00%	$0.00	$0.00
Harry S. Truman Scholarship Foundation	0	0	0	0	0	0.00%	$0.00	$0.00
Holocaust Memorial Museum U.S.	0	0	0	0	0	0.00%	$0.00	$0.00
Institute of Museum and Library Services	0	0	0	0	0	0.00%	$0.00	$0.00
Inter-American Foundation	0	0	0	0	0	0.00%	$0.00	$0.00
International Boundary and Water Commission	0	0	0	0	0	0.00%	$0.00	$0.00
International Joint Commission: US and Canada	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
International Trade Commission	0	0	0	0	0	0.00%	$0.00	$0.00
James Madison Memorial Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Japan-United States Friendship Commission	0	0	0	0	0	0.00%	$0.00	$0.00
John F. Kennedy Center for the Performing Arts	0	0	0	0	0	0.00%	$0.00	$0.00
Marine Mammal Commission	0	0	0	0	0	0.00%	$0.00	$0.00
Merit Systems Protection Board	0	0	0	0	0	0.00%	$0.00	$0.00
Millennium Challenge Corporation	0	0	0	0	0	0.00%	$0.00	$0.00
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Aeronautics and Space Administration	0	0	0	0	0	0.00%	$0.00	$0.00

Table B-9a FY 2012 Timeliness and Cost of Complaint Investigations Completed by Agency Investigators								
Agency or Department	Total Number Completed Investigations By Agency	Average Processing Days Completed Investigations By Agency	Number Timely Completed within 180 Days	Number Timely Completed within 181-360 Days	Total Number Timely Completed Investigations By Agency	% Investigations Timely Completed By Agency	Total Cost Completed Investigations By Agency	Average Cost Completed Investigations By Agency
National Archives and Records Administration	0	0	0	0	0	0.00%	$0.00	$0.00
National Capital Planning Commission	0	0	0	0	0	0.00%	$0.00	$0.00
National Council on Disability	0	0	0	0	0	0.00%	$0.00	$0.00
National Credit Union Administration	0	0	0	0	0	0.00%	$0.00	$0.00
National Endowment for the Arts	0	0	0	0	0	0.00%	$0.00	$0.00
National Endowment for the Humanities	0	0	0	0	0	0.00%	$0.00	$0.00
National Foundation on the Arts & the Humanities	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Gallery of Art	0	0	0	0	0	0.00%	$0.00	$0.00
National Indian Gaming Commission	0	0	0	0	0	0.00%	$0.00	$0.00
National Labor Relations Board	3	167.33	3	0	3	100.00%	$29,953.00	$9,984.33
National Mediation Board	0	0	0	0	0	0.00%	$0.00	$0.00
National Reconnaissance Office	0	0	0	0	0	0.00%	$0.00	$0.00
National Science Foundation	0	0	0	0	0	0.00%	$0.00	$0.00
National Transportation Safety Board	0	0	0	0	0	0.00%	$0.00	$0.00
Navajo and Hopi Indian Relocation Commission	0	0	0	0	0	0.00%	$0.00	$0.00
Nuclear Regulatory Commission	0	0	0	0	0	0.00%	$0.00	$0.00
Nuclear Waste Technical Review Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Occupational Safety &Health Review Commission	0	0	0	0	0	0.00%	$0.00	$0.00
Office of Government Ethics	0	0	0	0	0	0.00%	$0.00	$0.00
Office of Personnel Management	23	101.96	23	0	23	100.00%	$185,510.20	$8,065.66
Office of Special Counsel	0	0	0	0	0	0.00%	$0.00	$0.00
Office of the Director of National Intelligence	0	0	0	0	0	0.00%	$0.00	$0.00
Overseas Private Investment Corporation	0	0	0	0	0	0.00%	$0.00	$0.00
Peace Corps	0	0	0	0	0	0.00%	$0.00	$0.00
Pension Benefit Guaranty Corporation	0	0	0	0	0	0.00%	$0.00	$0.00
Postal Regulatory Commission	0	0	0	0	0	0.00%	$0.00	$0.00
Presidio Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Railroad Retirement Board	0	0	0	0	0	0.00%	$0.00	$0.00
Securities and Exchange Commission	0	0	0	0	0	0.00%	$0.00	$0.00
Selective Service System	0	0	0	0	0	0.00%	$0.00	$0.00
Small Business Administration	9	173.56	7	1	8	88.89%	$5,000.00	$555.56
Smithsonian Institution	0	0	0	0	0	0.00%	$0.00	$0.00
Social Security Administration	0	0	0	0	0	0.00%	$0.00	$0.00
Tennessee Valley Authority	3	115	3	0	3	100.00%	$13,000.00	$4,333.33

Table B-9a FY 2012 Timeliness and Cost of Complaint Investigations Completed by Agency Investigators								
Agency or Department	Total Number Completed Investigations By Agency	Average Processing Days Completed Investigations By Agency	Number Timely Completed within 180 Days	Number Timely Completed within 181-360 Days	Total Number Timely Completed Investigations By Agency	% Investigations Timely Completed By Agency	Total Cost Completed Investigations By Agency	Average Cost Completed Investigations By Agency
Trade and Development Agency	0	0	0	0	0	0.00%	$0.00	$0.00
U.S. Postal Service	0	0	0	0	0	0.00%	$0.00	$0.00
Utah Reclamation Mitigation and Conservation Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Valles Caldera Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Cabinet Level Subtotal	3,411	218.16	1,451	636	2,087	61.18%	$24,500,474.99	$7,182.78
Midsize Agencies Subtotal	75	252.93	34	7	41	54.67%	$324,959.30	$4,332.79
Small Agencies Subtotal	31	279.29	7	9	16	51.61%	$344,760.20	$11,121.30
Micro Agencies Subtotal	0	0	0	0	0	0.00%	$0.00	$0.00
Government-wide	3,517	219.44	1,492	652	2,144	60.96%	$25,170,194.49	$7,156.72

NRF = No Report Filed

Table B-9b FY 2012 Timeliness and Cost of Complaint Investigations Completed by Contract Investigators								
Agency or Department	**Total Number Completed Investigations By Contractor**	**Average Processing Days Completed Investigations By Contractor**	**Number Timely Completed within 180 Days**	**Number Timely Completed within 181-360 Days**	**Total Number Timely Completed Investigations By Contractor**	**% Investigations Timely Completed By Contractor**	**Total Cost Completed Investigations By Contractor**	**Average Cost Completed Investigations By Contractor**
Advisory Council on Historic Preservation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
African Development Foundation	0	0	0	0	0	0.00%	$0.00	$0.00
Agency for International Development	11	270.09	1	0	1	9.09%	$28,479.00	$2,589.00
American Battle Monuments Commission	0	0	0	0	0	0.00%	$0.00	$0.00
Appalachian Regional Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Architectural and Transportation Barriers Compliance Board	0	0	0	0	0	0.00%	$0.00	$0.00
Arctic Research Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Armed Forces Retirement Home	0	0	0	0	0	0.00%	$0.00	$0.00
Barry Goldwater Scholarship and Excellence in Education Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Broadcasting Board of Governors	5	161.2	4	1	5	100.00%	$13,500.00	$2,700.00
Central Intelligence Agency	3	322.33	0	0	0	0.00%	$72,159.48	$24,053.16
Chemical Safety and Hazard Investigation Board	0	0	0	0	0	0.00%	$0.00	$0.00
Christopher Columbus Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission of Fine Arts	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission on Civil Rights	0	0	0	0	0	0.00%	$0.00	$0.00
Committee for Purchase from People Who Are Blind or Severely Disabled	0	0	0	0	0	0.00%	$0.00	$0.00
Commodity Futures Trading Commission	1	110	1	0	1	100.00%	$6,750.00	$6,750.00
Consumer Financial Protection Bureau	0	0	0	0	0	0.00%	$0.00	$0.00
Consumer Product Safety Commission	4	142.25	4	0	4	100.00%	$9,808.00	$2,452.00
Corporation for National and Community Service	6	108.67	5	1	6	100.00%	$27,107.00	$4,517.83
Court Services and Offender Supervision Agency for the District of Columbia	4	130.25	4	0	4	100.00%	$18,060.00	$4,515.00
Defense Army and Air Force Exchange	0	0	0	0	0	0.00%	$0.00	$0.00
Defense Commissary Agency	0	0	0	0	0	0.00%	$0.00	$0.00
Defense Contract Audit Agency	0	0	0	0	0	0.00%	$0.00	$0.00
Defense Contract Management Agency	0	0	0	0	0	0.00%	$0.00	$0.00
Defense Finance and Accounting Service	0	0	0	0	0	0.00%	$0.00	$0.00
Defense Human Resources Activity	0	0	0	0	0	0.00%	$0.00	$0.00
Defense Information Systems Agency	0	0	0	0	0	0.00%	$0.00	$0.00
Defense Intelligence Agency	1	231	0	0	0	0.00%	$3,200.00	$3,200.00
Defense Joint Task Force National Capital Region Medical	1	315	0	0	0	0.00%	$3,025.00	$3,025.00

Table B-9b FY 2012 Timeliness and Cost of Complaint Investigations Completed by Contract Investigators								
Agency or Department	**Total Number Completed Investigations By Contractor**	**Average Processing Days Completed Investigations By Contractor**	**Number Timely Completed within 180 Days**	**Number Timely Completed within 181-360 Days**	**Total Number Timely Completed Investigations By Contractor**	**% Investigations Timely Completed By Contractor**	**Total Cost Completed Investigations By Contractor**	**Average Cost Completed Investigations By Contractor**
Defense Logistics Agency	0	0	0	0	0	0.00%	$0.00	$0.00
Defense Media Activity	0	0	0	0	0	0.00%	$0.00	$0.00
Defense Missile Defense Agency	0	0	0	0	0	0.00%	$0.00	$0.00
Defense National Geospatial-Intelligence Agency	0	0	0	0	0	0.00%	$0.00	$0.00
Defense National Guard Bureau	0	0	0	0	0	0.00%	$0.00	$0.00
Defense National Security Agency	0	0	0	0	0	0.00%	$0.00	$0.00
Defense Nuclear Facilities Safety Board	0	0	0	0	0	0.00%	$0.00	$0.00
Defense Office of the Inspector General	0	0	0	0	0	0.00%	$0.00	$0.00
Defense Office of the Secretary - Wash. Hqtrs. Services	0	0	0	0	0	0.00%	$0.00	$0.00
Defense Security Service	5	193	0	0	0	0.00%	$22,185.00	$4,437.00
Defense Technical Information Center	0	0	0	0	0	0.00%	$0.00	$0.00
Defense Threat Reduction Agency	0	0	0	0	0	0.00%	$0.00	$0.00
Defense TRICARE Management Activity	2	368.5	0	1	1	50.00%	$6,094.00	$3,047.00
Defense Uniformed Services University	0	0	0	0	0	0.00%	$0.00	$0.00
Department of Agriculture	437	241.59	187	30	217	49.66%	$1,535,339.78	$3,513.36
Department of Commerce	177	189.83	91	70	161	90.96%	$1,024,027.50	$5,785.47
Department of Defense Education Activity	43	153.19	36	6	42	97.67%	$137,500.30	$3,197.68
Department of Education	26	179	17	9	26	100.00%	$90,427.61	$3,477.99
Department of Energy	51	178.84	23	19	42	82.35%	$133,184.06	$2,611.45
Department of Health and Human Services	281	153.7	225	37	262	93.24%	$1,218,862.06	$4,337.59
Department of Homeland Security	725	243.78	225	112	337	46.48%	$2,219,548.91	$3,061.45
Department of Housing and Urban Development	77	285.31	20	6	26	33.77%	$148,322.00	$1,926.26
Department of Justice	459	191.59	260	100	360	78.43%	$1,616,204.04	$3,521.14
Department of Labor	85	204.12	51	32	83	97.65%	$262,000.00	$3,082.35
Department of State	90	247.5	25	21	46	51.11%	$276,255.00	$3,069.50
Department of the Air Force	0	0	0	0	0	0.00%	$0.00	$0.00
Department of the Army	0	0	0	0	0	0.00%	$0.00	$0.00
Department of the Interior	238	270.06	87	36	123	51.68%	$781,905.60	$3,285.32
Department of the Navy	0	0	0	0	0	0.00%	$0.00	$0.00
Department of the Treasury	0	0	0	0	0	0.00%	$0.00	$0.00
Department of Transportation	105	129.56	94	10	104	99.05%	$471,660.00	$4,492.00
Department of Veterans Affairs	541	155.29	479	24	503	92.98%	$1,679,652.70	$3,104.72
Election Assistance Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Environmental Protection Agency	24	315.13	0	5	5	20.83%	$40,969.00	$1,707.04

Table B-9b FY 2012 Timeliness and Cost of Complaint Investigations Completed by Contract Investigators								
Agency or Department	**Total Number Completed Investigations By Contractor**	**Average Processing Days Completed Investigations By Contractor**	**Number Timely Completed within 180 Days**	**Number Timely Completed within 181-360 Days**	**Total Number Timely Completed Investigations By Contractor**	**% Investigations Timely Completed By Contractor**	**Total Cost Completed Investigations By Contractor**	**Average Cost Completed Investigations By Contractor**
Equal Employment Opportunity Commission	0	0	0	0	0	0.00%	$0.00	$0.00
Export-Import Bank of the US	1	240	0	1	1	100.00%	$6,238.58	$6,238.58
Farm Credit Administration	0	0	0	0	0	0.00%	$0.00	$0.00
Farm Credit System Insurance Corporation	0	0	0	0	0	0.00%	$0.00	$0.00
Federal Communications Commission	10	39	0	10	10	100.00%	$36,000.00	$3,600.00
Federal Deposit Insurance Corporation	29	224.21	13	16	29	100.00%	$165,049.44	$5,691.36
Federal Election Commission	0	0	0	0	0	0.00%	$0.00	$0.00
Federal Energy Regulatory Commission	6	180	6	0	6	100.00%	$21,000.00	$3,500.00
Federal Financial Institutions Examination Council	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Housing Finance Agency	3	225	1	1	2	66.67%	$14,509.00	$4,836.33
Federal Labor Relations Authority	1	248	0	1	1	100.00%	$7,649.00	$7,649.00
Federal Maritime Commission	0	0	0	0	0	0.00%	$0.00	$0.00
Federal Mediation and Conciliation Service	0	0	0	0	0	0.00%	$0.00	$0.00
Federal Mine Safety & Health Review Commission	0	0	0	0	0	0.00%	$0.00	$0.00
Federal Reserve System--Board of Governors	5	151	4	1	5	100.00%	$41,956.10	$8,391.22
Federal Retirement Thrift Investment Board	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Trade Commission	0	0	0	0	0	0.00%	$0.00	$0.00
General Services Administration	77	265.82	23	21	44	57.14%	$230,204.61	$2,989.67
Government Printing Office	26	274.27	1	11	12	46.15%	$79,107.00	$3,042.58
Harry S. Truman Scholarship Foundation	0	0	0	0	0	0.00%	$0.00	$0.00
Holocaust Memorial Museum U.S.	0	0	0	0	0	0.00%	$0.00	$0.00
Institute of Museum and Library Services	0	0	0	0	0	0.00%	$0.00	$0.00
Inter-American Foundation	0	0	0	0	0	0.00%	$0.00	$0.00
International Boundary and Water Commission	0	0	0	0	0	0.00%	$0.00	$0.00
International Joint Commission: US and Canada	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
International Trade Commission	2	161.5	1	0	1	50.00%	$10,344.00	$5,172.00
James Madison Memorial Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Japan-United States Friendship Commission	0	0	0	0	0	0.00%	$0.00	$0.00
John F. Kennedy Center for the Performing Arts	1	61	1	0	1	100.00%	$3,974.00	$3,974.00
Marine Mammal Commission	0	0	0	0	0	0.00%	$0.00	$0.00
Merit Systems Protection Board	1	148	1	0	1	100.00%	$5,619.00	$5,619.00
Millennium Challenge Corporation	0	0	0	0	0	0.00%	$0.00	$0.00
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Aeronautics and Space Administration	21	193.57	10	7	17	80.95%	$91,245.88	$4,345.04

Table B-9b FY 2012 Timeliness and Cost of Complaint Investigations Completed by Contract Investigators								
Agency or Department	**Total Number Completed Investigations By Contractor**	**Average Processing Days Completed Investigations By Contractor**	**Number Timely Completed within 180 Days**	**Number Timely Completed within 181-360 Days**	**Total Number Timely Completed Investigations By Contractor**	**% Investigations Timely Completed By Contractor**	**Total Cost Completed Investigations By Contractor**	**Average Cost Completed Investigations By Contractor**
National Archives and Records Administration	3	170	2	1	3	100.00%	$11,477.43	$3,825.81
National Capital Planning Commission	0	0	0	0	0	0.00%	$0.00	$0.00
National Council on Disability	0	0	0	0	0	0.00%	$0.00	$0.00
National Credit Union Administration	3	217	1	1	2	66.67%	$15,830.00	$5,276.67
National Endowment for the Arts	0	0	0	0	0	0.00%	$0.00	$0.00
National Endowment for the Humanities	0	0	0	0	0	0.00%	$0.00	$0.00
National Foundation on the Arts & the Humanities	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Gallery of Art	0	0	0	0	0	0.00%	$0.00	$0.00
National Indian Gaming Commission	2	266	0	1	1	50.00%	$9,903.00	$4,951.50
National Labor Relations Board	0	0	0	0	0	0.00%	$0.00	$0.00
National Mediation Board	0	0	0	0	0	0.00%	$0.00	$0.00
National Reconnaissance Office	0	0	0	0	0	0.00%	$0.00	$0.00
National Science Foundation	4	371.75	0	0	0	0.00%	$11,940.00	$2,985.00
National Transportation Safety Board	2	111	2	0	2	100.00%	$5,465.00	$2,732.50
Navajo and Hopi Indian Relocation Commission	0	0	0	0	0	0.00%	$0.00	$0.00
Nuclear Regulatory Commission	9	209.44	6	1	7	77.78%	$45,000.00	$5,000.00
Nuclear Waste Technical Review Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Occupational Safety &Health Review Commission	0	0	0	0	0	0.00%	$0.00	$0.00
Office of Government Ethics	0	0	0	0	0	0.00%	$0.00	$0.00
Office of Personnel Management	2	120	2	0	2	100.00%	$5,500.00	$2,750.00
Office of Special Counsel	0	0	0	0	0	0.00%	$0.00	$0.00
Office of the Director of National Intelligence	0	0	0	0	0	0.00%	$0.00	$0.00
Overseas Private Investment Corporation	0	0	0	0	0	0.00%	$0.00	$0.00
Peace Corps	4	156.75	3	1	4	100.00%	$16,786.00	$4,196.50
Pension Benefit Guaranty Corporation	7	194.14	3	3	6	85.71%	$18,000.00	$2,571.43
Postal Regulatory Commission	0	0	0	0	0	0.00%	$0.00	$0.00
Presidio Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Railroad Retirement Board	4	178	4	0	4	100.00%	$8,090.00	$2,022.50
Securities and Exchange Commission	10	259.7	4	4	8	80.00%	$36,258.26	$3,625.83
Selective Service System	2	288	0	2	2	100.00%	$3,864.00	$1,932.00
Small Business Administration	24	215.54	5	17	22	91.67%	$106,641.00	$4,443.38
Smithsonian Institution	8	173.5	7	1	8	100.00%	$19,250.00	$2,406.25
Social Security Administration	339	194.84	222	57	279	82.30%	$1,520,762.08	$4,486.02
Tennessee Valley Authority	41	139.9	41	0	41	100.00%	$70,258.59	$1,713.62
Trade and Development Agency	0	0	0	0	0	0.00%	$0.00	$0.00

Table B-9b FY 2012 Timeliness and Cost of Complaint Investigations Completed by Contract Investigators								
Agency or Department	**Total Number Completed Investigations By Contractor**	**Average Processing Days Completed Investigations By Contractor**	**Number Timely Completed within 180 Days**	**Number Timely Completed within 181-360 Days**	**Total Number Timely Completed Investigations By Contractor**	**% Investigations Timely Completed By Contractor**	**Total Cost Completed Investigations By Contractor**	**Average Cost Completed Investigations By Contractor**
U.S. Postal Service	2,660	112.86	2,562	74	2,636	99.10%	$4,395,336.75	$1,652.38
Utah Reclamation Mitigation and Conservation Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Valles Caldera Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Cabinet Level Subtotal	6,004	165.45	4,382	587	4,969	82.76%	$16,024,730.31	$2,669.01
Midsize Agencies Subtotal	565	207.41	323	124	447	79.12%	$2,249,880.60	$3,982.09
Small Agencies Subtotal	140	205.75	59	41	100	71.43%	$584,873.85	$4,177.67
Micro Agencies Subtotal	0	0	0	0	0	0.00%	$0.00	$0.00
Government-wide	6,709	169.82	4,764	752	5,516	82.22%	$18,859,484.76	$2,811.07

NRF = No Report Filed

Table B-9c FY 2012 Timeliness and Cost of All Completed Complaint Investigations

Agency or Department	Total Number Completed Investigations	Average Processing Days Completed Investigations	Number Timely Completed within 180 Days	Number Timely Completed within 181-360 Days	Total Number Timely Completed Investigations	% Investigations Timely Completed	Total Cost All Completed Investigations	Average Cost All Completed Investigations
Defense Logistics Agency Wide	**52**	**272.19**	**4**	**8**	**12**	**23.08%**	**$464,213.36**	**$8,927.18**
DLA Aviation	10	238.8	0	2	2	20.00%	$89,271.80	$8,927.18
DLA Disposition Services	5	328.8	0	0	0	0.00%	$44,635.90	$8,927.18
DLA Distribution	19	276.42	2	4	6	31.58%	$169,616.42	$8,927.18
DLA Headquarters Operations Division	7	264.14	1	1	2	28.57%	$62,490.26	$8,927.18
DLA Land and Maritime	6	321	0	0	0	0.00%	$53,563.08	$8,927.18
DLA Logistics Information Service	2	288.5	0	0	0	0.00%	$17,854.36	$8,927.18
DLA Troop Support	3	172.67	1	1	2	66.67%	$26,781.54	$8,927.18
Defense National Guard Bureau Wide	**0**	**0**	**0**	**0**	**0**	**0.00%**	**$0.00**	**$0.00**
Alabama National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Alaska National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Arizona National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Arkansas National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
California National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Colorado National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Connecticut National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
DC National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Delaware National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Florida National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Georgia National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Guam National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Hawaii National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Idaho National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Illinois National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Indiana National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Iowa National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Kansas National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Kentucky National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Louisiana National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Maine National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Maryland National Guard	0	0	0	0	0	0.00%	$0.00	$0.00

Table B-9c FY 2012 Timeliness and Cost of All Completed Complaint Investigations

Agency or Department	Total Number Completed Investigations	Average Processing Days Completed Investigations	Number Timely Completed within 180 Days	Number Timely Completed within 181-360 Days	Total Number Timely Completed Investigations	% Investigations Timely Completed	Total Cost All Completed Investigations	Average Cost All Completed Investigations
Massachusetts National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Michigan National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Minnesota National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Mississippi National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Missouri National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Montana National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Nebraska National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Nevada National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
New Hampshire National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
New Jersey National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
New Mexico National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
New York National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
North Carolina National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
North Dakota National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Ohio National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Oklahoma National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Oregon National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Pennsylvania National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Puerto Rico National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Rhode Island National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
South Carolina National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
South Dakota National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Tennessee National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Texas National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Utah National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Vermont National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Virgin Islands National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Virginia National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Washington State National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
West Virginia National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Wisconsin National Guard	0	0	0	0	0	0.00%	$0.00	$0.00
Wyoming National Guard	0	0	0	0	0	0.00%	$0.00	$0.00

Table B-9c FY 2012 Timeliness and Cost of All Completed Complaint Investigations

Agency or Department	Total Number Completed Investigations	Average Processing Days Completed Investigations	Number Timely Completed within 180 Days	Number Timely Completed within 181-360 Days	Total Number Timely Completed Investigations	% Investigations Timely Completed	Total Cost All Completed Investigations	Average Cost All Completed Investigations
Department of Agriculture Wide	**437**	**241.59**	**187**	**30**	**217**	**49.66%**	**$1,535,339.78**	**$3,513.36**
USDA - Office Of Inspector General	6	154.17	4	2	6	100.00%	$18,276.00	$3,046.00
USDA Agricultural Marketing Service	15	146.8	13	0	13	86.67%	$54,117.00	$3,607.80
USDA Agricultural Research Service	21	286.29	10	1	11	52.38%	$54,586.00	$2,599.33
USDA Agriculture Headquarters	14	259.79	4	0	4	28.57%	$18,515.00	$1,322.50
USDA Animal and Plant Health Inspection Service	39	195.41	17	4	21	53.85%	$147,776.00	$3,789.13
USDA Economic Research Service	3	534	1	0	1	33.33%	$9,561.00	$3,187.00
USDA Farm Service Agency	23	95.87	22	1	23	100.00%	$107,697.43	$4,682.50
USDA Food and Nutrition Service	3	190.33	2	0	2	66.67%	$11,296.00	$3,765.33
USDA Food Safety And Inspection Service	70	247.21	25	8	33	47.14%	$265,345.44	$3,790.65
USDA Foreign Agricultural Service	3	182.33	2	0	2	66.67%	$8,450.00	$2,816.67
USDA Forest Service	137	210.57	63	9	72	52.55%	$539,654.00	$3,939.08
USDA Grain Inspection, Packers& Stockyards Admin	6	149.5	5	0	5	83.33%	$24,840.00	$4,140.00
USDA National Agricultural Statistics Service	2	215.5	1	0	1	50.00%	$7,118.00	$3,559.00
USDA National Appeals Division	0	0	0	0	0	0.00%	$0.00	$0.00
USDA National Institute of Food and Agriculture	0	0	0	0	0	0.00%	$0.00	$0.00
USDA Natural Resources Conservation Service	22	188.73	14	2	16	72.73%	$56,145.00	$2,552.05
USDA Office Of The Chief Financial Officer	22	384.95	2	1	3	13.64%	$63,089.91	$2,867.72
USDA Risk Management Agency	7	396.14	1	0	1	14.29%	$17,085.00	$2,440.71
USDA Rural Development	44	394.91	1	2	3	6.82%	$131,788.00	$2,995.18
Department of Commerce Wide	**183**	**188.25**	**95**	**71**	**166**	**90.71%**	**$1,045,662.42**	**$5,714.00**
DOC All Other Commerce Bureaus	21	185.57	10	11	21	100.00%	$123,539.00	$5,882.81
DOC Bureau of the Census	66	181.77	28	32	60	90.91%	$379,898.32	$5,756.04
DOC Decennial Census	3	192	2	1	3	100.00%	$12,328.60	$4,109.53
DOC International Trade Administration	7	206.71	4	2	6	85.71%	$44,531.00	$6,361.57
DOC National Institute of Standards & Technology	8	197.63	6	1	7	87.50%	$43,411.00	$5,426.38
DOC National Oceanic & Atmospheric Administration	61	191.23	35	17	52	85.25%	$371,436.50	$6,089.12
DOC U. S. Patent and Trademark Office	17	193.29	10	7	17	100.00%	$70,518.00	$4,148.12

Table B-9c FY 2012 Timeliness and Cost of All Completed Complaint Investigations

Agency or Department	Total Number Completed Investigations	Average Processing Days Completed Investigations	Number Timely Completed within 180 Days	Number Timely Completed within 181-360 Days	Total Number Timely Completed Investigations	% Investigations Timely Completed	Total Cost All Completed Investigations	Average Cost All Completed Investigations
Department of Energy Wide	**51**	**178.84**	**23**	**19**	**42**	**82.35%**	**$133,184.06**	**$2,611.45**
DOE Bonneville Power Administration	6	228.17	1	0	1	16.67%	$20,748.31	$3,458.05
DOE Chicago Operations Office	0	0	0	0	0	0.00%	$0.00	$0.00
DOE EM Consolidated Business Center	1	398	0	0	0	0.00%	$2,500.00	$2,500.00
DOE Golden Field Office	1	330	0	0	0	0.00%	$3,800.00	$3,800.00
DOE Headquarters	12	219.42	5	7	12	100.00%	$53,017.75	$4,418.15
DOE Idaho Operations Office	1	91	1	0	1	100.00%	$3,450.00	$3,450.00
DOE National Energy Technology Lab	1	207	0	0	0	0.00%	$5,362.00	$5,362.00
DOE NNSA Service Center	19	122.63	9	9	18	94.74%	$11,463.00	$603.32
DOE Oak Ridge Operations	0	0	0	0	0	0.00%	$0.00	$0.00
DOE OSTI	0	0	0	0	0	0.00%	$0.00	$0.00
DOE Richland Operations Office	0	0	0	0	0	0.00%	$0.00	$0.00
DOE Savannah River Operations	0	0	0	0	0	0.00%	$0.00	$0.00
DOE Southeastern Power Administration	0	0	0	0	0	0.00%	$0.00	$0.00
DOE Southwestern Power Administration	0	0	0	0	0	0.00%	$0.00	$0.00
DOE Strategic Petroleum Reserve	0	0	0	0	0	0.00%	$0.00	$0.00
DOE Western Area Power Administration	10	176.3	7	3	10	100.00%	$32,843.00	$3,284.30
Department of Health and Human Services Wide	**288**	**153.41**	**232**	**37**	**269**	**93.40%**	**$1,233,362.06**	**$4,282.51**
HHS Administration for Children and Families	4	197.25	2	0	2	50.00%	$10,686.00	$2,671.50
HHS Agency for Healthcare Research and Quality	3	141	3	0	3	100.00%	$11,811.00	$3,937.00
HHS Centers for Disease Control and Prevention	47	157.83	36	6	42	89.36%	$164,891.00	$3,508.32
HHS Centers for Medicare & Medicaid Services	24	136.17	24	0	24	100.00%	$82,417.41	$3,434.06
HHS Food and Drug Administration	58	176.79	38	18	56	96.55%	$314,141.20	$5,416.23
HHS Health Resources and Services Administration	7	127.43	7	0	7	100.00%	$49,098.00	$7,014.00
HHS Indian Health Service	57	116.07	49	7	56	98.25%	$225,568.25	$3,957.34
HHS National Institutes of Health	51	162.88	44	2	46	90.20%	$235,854.20	$4,624.59
HHS Office of the Secretary of Health&Human Srvcs	30	174.23	24	3	27	90.00%	$107,894.00	$3,596.47
HHS Program Support Center	3	120.33	3	0	3	100.00%	$13,570.00	$4,523.33
HHS Substance Abuse & Mental Health Srvcs Admin	4	157	2	1	3	75.00%	$17,431.00	$4,357.75

Table B-9c FY 2012 Timeliness and Cost of All Completed Complaint Investigations

Agency or Department	Total Number Completed Investigations	Average Processing Days Completed Investigations	Number Timely Completed within 180 Days	Number Timely Completed within 181-360 Days	Total Number Timely Completed Investigations	% Investigations Timely Completed	Total Cost All Completed Investigations	Average Cost All Completed Investigations
Department of Homeland Security Wide	**1,046**	**229.94**	**427**	**169**	**596**	**56.98%**	**$4,963,672.94**	**$4,745.39**
DHS Federal Emergency Management Agency	110	360.8	3	10	13	11.82%	$371,594.90	$3,378.14
DHS Federal Law Enforcement Training Center	9	222.33	2	6	8	88.89%	$18,216.92	$2,024.10
DHS Headquarters	24	226.13	9	12	21	87.50%	$51,313.32	$2,138.06
DHS Transportation Security Administration	429	224.57	130	60	190	44.29%	$1,290,135.00	$3,007.31
DHS U.S. Citizenship and Immigration Services	74	141.64	63	10	73	98.65%	$347,884.96	$4,701.15
DHS U.S. Coast Guard	39	205.79	21	18	39	100.00%	$139,461.00	$3,575.92
DHS U.S. Customs and Border Protection	252	175.54	192	49	241	95.63%	$2,499,109.03	$9,917.10
DHS U.S. Immigration and Customs Enforcement	81	301.32	4	2	6	7.41%	$148,065.72	$1,827.97
DHS U.S. Secret Service	28	354.07	3	2	5	17.86%	$97,892.09	$3,496.15
Department of Justice Wide	**614**	**202.46**	**302**	**181**	**483**	**78.66%**	**$2,575,296.36**	**$4,194.29**
DOJ Alcohol, Tobacco, Firearms and Explosives	34	314.74	4	5	9	26.47%	$176,414.33	$5,188.66
DOJ Bureau of Prisons	350	160.57	231	78	309	88.29%	$1,162,700.00	$3,322.00
DOJ Drug Enforcement Administration	23	313.35	6	2	8	34.78%	$81,454.65	$3,541.51
DOJ Executive Office for Immigration Review	10	215.8	6	3	9	90.00%	$44,058.60	$4,405.86
DOJ Executive Office for U.S. Attorneys	22	208.91	15	6	21	95.45%	$38,742.00	$1,761.00
DOJ Federal Bureau of Investigation	128	239.77	24	74	98	76.56%	$913,460.76	$7,136.41
DOJ Office of Justice Programs	9	227.22	3	6	9	100.00%	$17,415.00	$1,935.00
DOJ Offices, Boards, and Divisions	14	280.57	4	2	6	42.86%	$66,956.49	$4,782.61
DOJ U.S. Marshals Service	24	282.67	9	5	14	58.33%	$74,094.53	$3,087.27
Department of Labor Wide	**85**	**204.12**	**51**	**32**	**83**	**97.65%**	**$262,000.00**	**$3,082.35**
DOL (DM and others)	28	196	18	9	27	96.43%	$83,200.00	$2,971.43
DOL Bureau of Labor Statistics	1	176	1	0	1	100.00%	$2,500.00	$2,500.00
DOL Employment and Training Administration	10	180.2	8	2	10	100.00%	$28,900.00	$2,890.00
DOL Mine Safety and Health Administration	9	196.44	7	2	9	100.00%	$27,500.00	$3,055.56
DOL Occupational Safety and Health Administration	14	188.86	9	5	14	100.00%	$43,200.00	$3,085.71
DOL Office of Workers Compensation Programs	9	228.22	4	5	9	100.00%	$28,800.00	$3,200.00
DOL Wage and Hour Division	14	244.14	4	9	13	92.86%	$47,900.00	$3,421.43

Table B-9c FY 2012 Timeliness and Cost of All Completed Complaint Investigations

Agency or Department	Total Number Completed Investigations	Average Processing Days Completed Investigations	Number Timely Completed within 180 Days	Number Timely Completed within 181-360 Days	Total Number Timely Completed Investigations	% Investigations Timely Completed	Total Cost All Completed Investigations	Average Cost All Completed Investigations
Department of the Army Wide	**484**	**258.31**	**66**	**48**	**114**	**23.55%**	**$3,014,704.36**	**$6,228.73**
Eighth U.S. Army (KOREA)	2	324.5	0	0	0	0.00%	$12,718.38	$6,359.19
Headquarters, Department of Army	41	292.93	1	2	3	7.32%	$259,215.57	$6,322.33
U.S. Army Corps of Engineers	57	262.04	6	8	14	24.56%	$383,721.79	$6,731.96
U.S. Army Europe	1	197	0	1	1	100.00%	$10,983.90	$10,983.90
U.S. Army Forces Command	24	233.13	3	5	8	33.33%	$145,504.35	$6,062.68
U.S. Army Installation Management Command	112	240.04	19	10	29	25.89%	$711,643.16	$6,353.96
U.S. Army Intelligence and Security Command	9	241.56	1	1	2	22.22%	$57,042.35	$6,338.04
U.S. Army Material Command	103	256.47	14	12	26	25.24%	$607,548.39	$5,898.53
U.S. Army Medical Command	86	268	13	5	18	20.93%	$519,431.71	$6,039.90
U.S. Army Network Enterprise Technology Command	11	270.73	4	1	5	45.45%	$73,072.49	$6,642.95
U.S. Army Pacific (USARPAC)	0	0	0	0	0	0.00%	$0.00	$0.00
U.S. Army Space and Missile Defense Command	4	269.75	0	1	1	25.00%	$23,468.60	$5,867.15
U.S. Army Special Operations Command (USASOC)	0	0	0	0	0	0.00%	$0.00	$0.00
U.S. Army Test and Evaluation Command	10	262.7	3	0	3	30.00%	$62,395.51	$6,239.55
U.S. Army Training and Doctrine Command	24	267.83	2	2	4	16.67%	$147,958.16	$6,164.92
Department of the Interior Wide	**238**	**270.06**	**87**	**36**	**123**	**51.68%**	**$781,905.60**	**$3,285.32**
Bureau of Ocean Energy Management	2	245.5	1	1	2	100.00%	$13,072.90	$6,536.45
Bureau of Safety and Environmental Enforcement	3	193	2	0	2	66.67%	$7,290.00	$2,430.00
DOI Bureau Of Indian Affairs	52	369.54	10	3	13	25.00%	$209,755.00	$4,033.75
DOI Bureau Of Land Management	33	158.15	21	9	30	90.91%	$98,439.50	$2,983.02
DOI Bureau Of Reclamation	28	150.96	25	0	25	89.29%	$74,595.00	$2,664.11
DOI Fish And Wildlife Service	22	178.18	19	3	22	100.00%	$77,063.00	$3,502.86
DOI Geological Survey	6	279.83	1	3	4	66.67%	$19,589.70	$3,264.95
DOI National Park Service	65	345.51	1	6	7	10.77%	$191,014.50	$2,938.68
DOI Office Of Surface Mining, Reclamation & Enforcement	4	149	4	0	4	100.00%	$15,953.00	$3,988.25
DOI-Office Of The Secretary	23	256.04	3	11	14	60.87%	$75,133.00	$3,266.65

Table B-9c FY 2012 Timeliness and Cost of All Completed Complaint Investigations

Agency or Department	Total Number Completed Investigations	Average Processing Days Completed Investigations	Number Timely Completed within 180 Days	Number Timely Completed within 181-360 Days	Total Number Timely Completed Investigations	% Investigations Timely Completed	Total Cost All Completed Investigations	Average Cost All Completed Investigations
Department of the Navy Wide	**409**	**276.71**	**41**	**121**	**162**	**39.61%**	**$3,715,910.00**	**$9,085.35**
Chief Of Naval Operations	9	252	1	3	4	44.44%	$82,170.00	$9,130.00
Commander Naval Installations Command	40	256.75	7	9	16	40.00%	$365,200.00	$9,130.00
Commander Naval Reserve	0	0	0	0	0	0.00%	$0.00	$0.00
Commander Pacific Fleet	28	262.71	4	14	18	64.29%	$255,640.00	$9,130.00
DON Assistant for Administration	16	308.44	0	6	6	37.50%	$146,080.00	$9,130.00
DON Bureau of Medicine & Surgery	32	304.59	0	12	12	37.50%	$292,160.00	$9,130.00
DON SPAWAR	5	264.2	1	1	2	40.00%	$45,650.00	$9,130.00
DON Strategic Systems Project Office	3	359	0	1	1	33.33%	$27,390.00	$9,130.00
Fleet Cyber Command	1	160	1	0	1	100.00%	$9,130.00	$9,130.00
Fleet Forces Command	22	282.23	1	5	6	27.27%	$200,860.00	$9,130.00
Marine Corps HQ	64	287	5	13	18	28.13%	$584,320.00	$9,130.00
Military Sealift Command	18	296.5	1	5	6	33.33%	$164,340.00	$9,130.00
Naval Air Systems Command	42	265.95	3	16	19	45.24%	$365,200.00	$8,695.24
Naval Education & Training Command	11	446.82	0	1	1	9.09%	$100,430.00	$9,130.00
Naval Sea Systems Command	30	249.73	4	8	12	40.00%	$273,900.00	$9,130.00
Naval Special Warfare Command	1	312	0	0	0	0.00%	$9,130.00	$9,130.00
Naval Supply Systems Command	29	260	4	11	15	51.72%	$264,770.00	$9,130.00
Naval Systems Management Activity	0	0	0	0	0	0.00%	$0.00	$0.00
Navy Facilities & Engineering Command	47	250.98	7	12	19	40.43%	$429,110.00	$9,130.00
Navy Military Personnel Command	5	277.6	2	0	2	40.00%	$45,650.00	$9,130.00
Office Of Naval Intelligence	5	252.2	0	3	3	60.00%	$45,650.00	$9,130.00
Office Of Naval Research	1	252	0	1	1	100.00%	$9,130.00	$9,130.00
Department of the Treasury Wide	**285**	**197.5**	**135**	**113**	**248**	**87.02%**	**$2,229,613.00**	**$7,823.20**
Treas - Alcohol and Tobacco Tax and Trade Bureau	0	0	0	0	0	0.00%	$0.00	$0.00
Treas - Bureau of Engraving and Printing	13	160.85	10	2	12	92.31%	$0.00	$0.00
Treas - Bureau of the Public Debt	3	251	1	1	2	66.67%	$0.00	$0.00
Treas - Departmental Offices	8	156.75	6	2	8	100.00%	$0.00	$0.00
Treas - Financial Crimes Enforcement Network	1	173	1	0	1	100.00%	$0.00	$0.00
Treas - Financial Management Service	6	149.17	4	1	5	83.33%	$0.00	$0.00
Treas - Inspector General For Tax Administration	1	185	0	1	1	100.00%	$0.00	$0.00

Table B-9c FY 2012 Timeliness and Cost of All Completed Complaint Investigations

Agency or Department	Total Number Completed Investigations	Average Processing Days Completed Investigations	Number Timely Completed within 180 Days	Number Timely Completed within 181-360 Days	Total Number Timely Completed Investigations	% Investigations Timely Completed	Total Cost All Completed Investigations	Average Cost All Completed Investigations
Treas - Internal Revenue Service	225	204.01	96	97	193	85.78%	$2,229,613.00	$9,909.39
Treas - Office of the Comptroller of the Currency	5	100.8	5	0	5	100.00%	$0.00	$0.00
Treas -Special Inspector General for the Trouble Assets Relief Program	0	0	0	0	0	0.00%	$0.00	$0.00
Treas - U. S. Mint	17	205.47	7	9	16	94.12%	$0.00	$0.00
Treas -Internal Revenue Service Office of the Chief Counsel	4	164.25	4	0	4	100.00%	$0.00	$0.00
Treas- Office of the Inspector General	2	189.5	1	0	1	50.00%	$0.00	$0.00
Department of Transportation Wide	**216**	**136.06**	**196**	**18**	**214**	**99.07%**	**$1,376,310.00**	**$6,371.81**
DOT Federal Aviation Administration	178	136.69	160	16	176	98.88%	$1,158,060.00	$6,505.96
DOT Federal Highway Administration	7	117	7	0	7	100.00%	$38,760.00	$5,537.14
DOT Federal Motor Carrier Safety Administration	2	143.5	2	0	2	100.00%	$8,984.00	$4,492.00
DOT Federal Railroad Administration	2	133	2	0	2	100.00%	$12,642.00	$6,321.00
DOT Federal Transit Administration	4	125.75	4	0	4	100.00%	$21,626.00	$5,406.50
DOT Maritime Administration	7	134.43	7	0	7	100.00%	$35,102.00	$5,014.57
DOT National Highway Traffic Safety Administration	7	106.29	7	0	7	100.00%	$42,418.00	$6,059.71
DOT Office of Inspector General	1	175	1	0	1	100.00%	$8,150.00	$8,150.00
DOT Office of the Secretary	1	128	1	0	1	100.00%	$4,492.00	$4,492.00
DOT Pipeline & Hazardous Materials Safety Admin	1	177	1	0	1	100.00%	$8,150.00	$8,150.00
DOT Research& Innovative Technology Administration	6	170	4	2	6	100.00%	$37,926.00	$6,321.00
DOT St. Lawrence Development Corporation	0	0	0	0	0	0.00%	$0.00	$0.00
Department of Veterans Affairs Wide	**1,583**	**164.52**	**1,258**	**133**	**1,391**	**87.87%**	**$9,137,264.70**	**$5,772.12**
VA-HQ and Others	71	168.08	52	6	58	81.69%	$0.00	$0.00
VA-NCA	18	162.17	17	0	17	94.44%	$0.00	$0.00
VA-Veterans Benefits Administration	108	162.39	87	14	101	93.52%	$0.00	$0.00
VA-Veterans Health Administration	1,386	164.54	1,102	113	1,215	87.66%	$0.00	$0.00
Federal Housing Finance Agency Wide	**3**	**225**	**1**	**1**	**2**	**66.67%**	**$14,509.00**	**$4,836.33**
Federal Housing Finance Agency Hqtrs	2	249	0	1	1	50.00%	$10,671.00	$5,335.50
Federal Housing Finance Agency OIG	1	177	1	0	1	100.00%	$3,838.00	$3,838.00

Table B-9c FY 2012 Timeliness and Cost of All Completed Complaint Investigations

Agency or Department	Total Number Completed Investigations	Average Processing Days Completed Investigations	Number Timely Completed within 180 Days	Number Timely Completed within 181-360 Days	Total Number Timely Completed Investigations	% Investigations Timely Completed	Total Cost All Completed Investigations	Average Cost All Completed Investigations
General Services Administration Wide	**77**	**265.82**	**23**	**21**	**44**	**57.14%**	**$230,204.61**	**$2,989.67**
GSA Central Office	17	343.82	1	5	6	35.29%	$57,549.03	$3,385.24
GSA National Capital Region	11	260.36	3	3	6	54.55%	$30,800.05	$2,800.00
GSA Region 1	1	148	1	0	1	100.00%	$2,850.00	$2,850.00
GSA Region 10	2	134	1	1	2	100.00%	$5,200.00	$2,600.00
GSA Region 2	9	249.44	2	1	3	33.33%	$28,741.00	$3,193.44
GSA Region 3	5	396	0	1	1	20.00%	$15,783.56	$3,156.71
GSA Region 4	6	313.67	0	3	3	50.00%	$21,300.00	$3,550.00
GSA Region 5	4	152	4	0	4	100.00%	$14,345.97	$3,586.49
GSA Region 6	6	230.33	2	3	5	83.33%	$23,349.00	$3,891.50
GSA Region 7	0	0	0	0	0	0.00%	$0.00	$0.00
GSA Region 8	0	0	0	0	0	0.00%	$0.00	$0.00
GSA Region 9	16	202.88	9	4	13	81.25%	$30,286.00	$1,892.88
U.S. Postal Service Wide	**2,660**	**112.86**	**2,562**	**74**	**2,636**	**99.10%**	**$4,395,336.75**	**$1,652.38**
USPS Capital Metro Area Operations	319	119.84	303	11	314	98.43%	$534,994.59	$1,677.10
USPS Eastern Area	406	108.4	399	5	404	99.51%	$662,747.66	$1,632.38
USPS Great Lakes Area	302	114.29	289	9	298	98.68%	$495,514.22	$1,640.78
USPS Headquarters	55	112.6	55	0	55	100.00%	$88,483.55	$1,608.79
USPS Northeast Area	271	116.3	259	11	270	99.63%	$443,089.46	$1,635.02
USPS Office of Inspector General	7	105.57	7	0	7	100.00%	$11,354.27	$1,622.04
USPS Pacific Area	331	110.13	322	7	329	99.40%	$549,711.91	$1,660.76
USPS Southern Area	641	112.13	617	20	637	99.38%	$1,062,371.01	$1,657.37
USPS Western Area	328	111.83	311	11	322	98.17%	$547,070.08	$1,667.90

NRF= No Report Filed

Table B-10 FY 2012 Total Number and Average Processing Days for All Complaint Closures

Agency or Department	Total Number Complaint Closures	APD Complaint Closures from Date Complaint Filed/ Remanded	Total Number Dismissals	APD Dismissals by FAD or FO from Date Complaint Filed/ Remanded	Total Number Merit Final Agency Decisions (FADs) (No AJ Decision)	APD Merit FADS from Date Complaint Filed/ Remanded	*Number Final Orders (FOs) of Merit AJ Decisions	APD FOs of Merit AJ Decisions from Date Complaint Filed/ Remanded	*Total Number Complaint Closures Finding Discrimi-nation	APD Complaint Closures Finding Discrimi-nation from Date Complaint Filed/ Remanded	*Total Number Complaint Closures Finding No Discrimi-nation	APD Complaint Closures FInding No Discrimination from Date Complaint Filed/ Remanded
Advisory Council on Historic Preservation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
African Development Foundation	3	845	1	934	0	0	0	0	0	0	0	0
Agency for International Development	16	398.81	7	92.14	1	830	1	1,525.00	0	0	2	1,177.50
American Battle Monuments Commission	0	0	0	0	0	0	0	0	0	0	0	0
Appalachian Regional Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Architectural and Transportation Barriers Compliance Board	0	0	0	0	0	0	0	0	0	0	0	0
Arctic Research Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Armed Forces Retirement Home	4	243.5	0	0	4	243.5	0	0	0	0	4	243.5
Barry Goldwater Scholarship and Excellence in Education Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Broadcasting Board of Governors	14	356.29	5	235.8	2	326	1	939	0	0	3	530.33
Central Intelligence Agency	39	585.38	10	151.3	6	590.33	11	1,186.82	0	0	17	976.29
Chemical Safety and Hazard Investigation Board	0	0	0	0	0	0	0	0	0	0	0	0
Christopher Columbus Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission of Fine Arts	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission on Civil Rights	0	0	0	0	0	0	0	0	0	0	0	0
Committee for Purchase from People Who Are Blind or Severely Disabled	0	0	0	0	0	0	0	0	0	0	0	0
Commodity Futures Trading Commission	2	314	0	0	2	314	0	0	0	0	2	314
Consumer Financial Protection Bureau	7	181.29	0	0	3	301	0	0	0	0	3	301
Consumer Product Safety Commission	2	380	0	0	1	416	0	0	0	0	1	416
Corporation for National and Community Service	3	431.67	0	0	3	431.67	0	0	0	0	3	431.67
Court Services and Offender Supervision Agency for the District of Columbia	15	756.93	2	85	2	393	5	901.8	1	1,745.00	6	591.67
Defense Army and Air Force Exchange	89	318.17	20	75.3	14	346.29	13	886.31	1	324	26	617.15
Defense Commissary Agency	120	318.85	22	12.91	27	349.44	18	728.11	1	913	44	491.55
Defense Contract Audit Agency	32	252.25	4	40.75	7	357.57	3	503.33	0	0	10	401.3
Defense Contract Management Agency	38	345.03	16	119.69	8	496.63	0	0	0	0	8	496.63
Defense Finance and Accounting Service	39	352.74	9	12.11	8	309.25	6	697.83	1	375	13	483.54
Defense Human Resources Activity	5	149	1	32	0	0	0	0	0	0	0	0
Defense Information Systems Agency	8	686.75	5	996.4	0	0	0	0	0	0	0	0

Table B-10 FY 2012 Total Number and Average Processing Days for All Complaint Closures

Agency or Department	Total Number Complaint Closures	APD Complaint Closures from Date Complaint Filed/ Remanded	Total Number Dismissals	APD Dismissals by FAD or FO from Date Complaint Filed/ Remanded	Total Number Merit Final Agency Decisions (FADs) (No AJ Decision)	APD Merit FADS from Date Complaint Filed/ Remanded	*Number Final Orders (FOs) of Merit AJ Decisions	APD FOs of Merit AJ Decisions from Date Complaint Filed/ Remanded	*Total Number Complaint Closures Finding Discrimi-nation	APD Complaint Closures Finding Discrimi-nation from Date Complaint Filed/ Remanded	*Total Number Complaint Closures Finding No Discrimi-nation	APD Complaint Closures FInding No Discrimination from Date Complaint Filed/ Remanded
Defense Intelligence Agency	34	518.88	11	54.09	7	681.29	7	1,004.00	2	1,487.00	12	735.25
Defense Joint Task Force National Capital Region Medical	7	92	5	53	0	0	0	0	0	0	0	0
Defense Logistics Agency	136	463.1	14	82.14	38	493.92	23	682.26	2	384	59	571.07
Defense Media Activity	3	453	0	0	0	0	0	0	0	0	0	0
Defense Missile Defense Agency	0	0	0	0	0	0	0	0	0	0	0	0
Defense National Geospatial-Intelligence Agency	20	427.3	5	113	4	666.75	3	684.67	0	0	7	674.43
Defense National Guard Bureau	33	327.39	23	354.74	3	361.67	0	0	0	0	3	361.67
Defense National Security Agency	17	636.29	4	320	5	376.4	4	1,378.00	2	1,776.00	7	548.86
Defense Nuclear Facilities Safety Board	0	0	0	0	0	0	0	0	0	0	0	0
Defense Office of the Inspector General	3	468.67	1	8	0	0	0	0	0	0	0	0
Defense Office of the Secretary - Wash. Hqtrs. Services	45	569.62	13	245.15	6	663.5	7	1,174.14	0	0	13	938.46
Defense Security Service	6	166.67	2	100	3	200	0	0	0	0	3	200
Defense Technical Information Center	1	599	0	0	0	0	0	0	0	0	0	0
Defense Threat Reduction Agency	8	742.75	4	868.75	0	0	0	0	0	0	0	0
Defense TRICARE Management Activity	7	217.29	5	107.8	0	0	0	0	0	0	0	0
Defense Uniformed Services University	0	0	0	0	0	0	0	0	0	0	0	0
Department of Agriculture	453	633.2	48	111.85	151	638.32	55	849.15	11	946	195	680.43
Department of Commerce	432	465.11	57	151.47	189	569.24	100	642.38	8	535.63	281	596.22
Department of Defense Education Activity	55	405.89	10	53.7	12	385.67	6	843.17	0	0	18	538.17
Department of Education	46	565.93	2	92	17	358.24	12	1,057.08	0	0	29	647.41
Department of Energy	63	344.75	6	242	18	371.67	3	638.67	2	354.5	19	415.63
Department of Health and Human Services	409	340.52	95	69.84	96	404.14	34	706.97	4	1,068.00	126	464.78
Department of Homeland Security	1,097	461.88	180	177.51	337	493.66	218	747.68	13	831.46	542	587.73
Department of Housing and Urban Development	73	594.14	3	393.67	25	624.24	15	747.73	0	0	40	670.55
Department of Justice	857	591.89	110	135.89	362	775.83	144	759.65	17	773.47	489	771.14
Department of Labor	134	505.19	19	407.32	44	357.14	12	752.08	0	0	56	441.77
Department of State	110	413.4	16	24.13	40	460.58	14	700.64	3	816.33	51	505.55
Department of the Air Force	500	482.59	76	146.8	96	839.44	97	729.6	7	953.71	186	777.85
Department of the Army	1,116	324.63	237	52.69	181	528.11	122	743.84	10	981.5	293	602.46
Department of the Interior	307	487.03	31	197.16	104	574.44	42	822.02	3	789	143	642.66

Table B-10 FY 2012 Total Number and Average Processing Days for All Complaint Closures

Agency or Department	Total Number Complaint Closures	APD Complaint Closures from Date Complaint Filed/ Remanded	Total Number Dismissals	APD Dismissals by FAD or FO from Date Complaint Filed/ Remanded	Total Number Merit Final Agency Decisions (FADs) (No AJ Decision)	APD Merit FADS from Date Complaint Filed/ Remanded	*Number Final Orders (FOs) of Merit AJ Decisions	APD FOs of Merit AJ Decisions from Date Complaint Filed/ Remanded	*Total Number Complaint Closures Finding Discrimi-nation	APD Complaint Closures Finding Discrimi-nation from Date Complaint Filed/ Remanded	*Total Number Complaint Closures Finding No Discrimi-nation	APD Complaint Closures FInding No Discrimination from Date Complaint Filed/ Remanded
Department of the Navy	904	332.14	147	56.65	117	477.23	76	928.68	8	1,385.38	185	623.42
Department of the Treasury	407	468.29	51	260.61	123	355.41	103	782.28	6	543.67	220	550.13
Department of Transportation	335	411.26	87	135.53	89	413.53	53	672.89	3	1,037.33	139	498.96
Department of Veterans Affairs	2,123	393.83	406	107.48	597	464.04	376	679.39	42	790.57	931	536.28
Election Assistance Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Environmental Protection Agency	49	712.04	3	434.33	13	899.31	10	868.4	1	1,373.00	22	863.73
Equal Employment Opportunity Commission	20	329.05	5	161.2	5	529.8	3	601	0	0	8	556.5
Export-Import Bank of the US	1	330	1	330	0	0	0	0	0	0	0	0
Farm Credit Administration	0	0	0	0	0	0	0	0	0	0	0	0
Farm Credit System Insurance Corporation	0	0	0	0	0	0	0	0	0	0	0	0
Federal Communications Commission	2	90	2	90	0	0	0	0	0	0	0	0
Federal Deposit Insurance Corporation	42	291.31	12	158.5	12	407.42	2	660.5	0	0	14	443.57
Federal Election Commission	0	0	0	0	0	0	0	0	0	0	0	0
Federal Energy Regulatory Commission	10	152.3	2	60	6	200	0	0	0	0	6	200
Federal Financial Institutions Examination Council	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Housing Finance Agency	6	199.83	1	170	0	0	0	0	0	0	0	0
Federal Labor Relations Authority	0	0	0	0	0	0	0	0	0	0	0	0
Federal Maritime Commission	0	0	0	0	0	0	0	0	0	0	0	0
Federal Mediation and Conciliation Service	2	15	0	0	0	0	0	0	0	0	0	0
Federal Mine Safety & Health Review Commission	0	0	0	0	0	0	0	0	0	0	0	0
Federal Reserve System--Board of Governors	6	310.17	0	0	0	0	1	792	0	0	1	792
Federal Retirement Thrift Investment Board	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Trade Commission	1	1,115.00	0	0	0	0	1	1,115.00	0	0	1	1,115.00
General Services Administration	85	425.05	11	42.82	21	397.57	23	740.43	0	0	44	576.8
Government Printing Office	29	329.86	5	33.8	11	358.45	2	1,000.00	0	0	13	457.15
Harry S. Truman Scholarship Foundation	0	0	0	0	0	0	0	0	0	0	0	0
Holocaust Memorial Museum U.S.	0	0	0	0	0	0	0	0	0	0	0	0
Institute of Museum and Library Services	0	0	0	0	0	0	0	0	0	0	0	0
Inter-American Foundation	0	0	0	0	0	0	0	0	0	0	0	0
International Boundary and Water Commission	0	0	0	0	0	0	0	0	0	0	0	0
International Joint Commission: US and Canada	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
International Trade Commission	1	195	0	0	0	0	0	0	0	0	0	0

Table B-10 FY 2012 Total Number and Average Processing Days for All Complaint Closures

Agency or Department	Total Number Complaint Closures	APD Complaint Closures from Date Complaint Filed/ Remanded	Total Number Dismissals	APD Dismissals by FAD or FO from Date Complaint Filed/ Remanded	Total Number Merit Final Agency Decisions (FADs) (No AJ Decision)	APD Merit FADS from Date Complaint Filed/ Remanded	*Number Final Orders (FOs) of Merit AJ Decisions	APD FOs of Merit AJ Decisions from Date Complaint Filed/ Remanded	*Total Number Complaint Closures Finding Discrimi-nation	APD Complaint Closures Finding Discrimi-nation from Date Complaint Filed/ Remanded	*Total Number Complaint Closures Finding No Discrimi-nation	APD Complaint Closures FInding No Discrimination from Date Complaint Filed/ Remanded
James Madison Memorial Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Japan-United States Friendship Commission	0	0	0	0	0	0	0	0	0	0	0	0
John F. Kennedy Center for the Performing Arts	0	0	0	0	0	0	0	0	0	0	0	0
Marine Mammal Commission	0	0	0	0	0	0	0	0	0	0	0	0
Merit Systems Protection Board	1	231	0	0	0	0	0	0	0	0	0	0
Millennium Challenge Corporation	0	0	0	0	0	0	0	0	0	0	0	0
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Aeronautics and Space Administration	38	565.26	9	98.89	11	516.36	10	1,214.40	0	0	21	848.76
National Archives and Records Administration	11	685.27	2	64	3	636	3	1,161.33	0	0	6	898.67
National Capital Planning Commission	0	0	0	0	0	0	0	0	0	0	0	0
National Council on Disability	0	0	0	0	0	0	0	0	0	0	0	0
National Credit Union Administration	7	424.57	0	0	1	541	0	0	0	0	1	541
National Endowment for the Arts	3	324.33	1	77	0	0	0	0	0	0	0	0
National Endowment for the Humanities	0	0	0	0	0	0	0	0	0	0	0	0
National Foundation on the Arts & the Humanities	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Gallery of Art	6	817.33	1	21	3	760.67	0	0	0	0	3	760.67
National Indian Gaming Commission	1	304	0	0	0	0	0	0	0	0	0	0
National Labor Relations Board	8	288.88	1	22	2	234.5	1	554	1	242	2	390.5
National Mediation Board	0	0	0	0	0	0	0	0	0	0	0	0
National Reconnaissance Office	7	542.14	2	75	2	333.5	2	1,094.00	0	0	4	713.75
National Science Foundation	6	364	0	0	0	0	0	0	0	0	0	0
National Transportation Safety Board	2	176	0	0	1	276	0	0	0	0	1	276
Navajo and Hopi Indian Relocation Commission	0	0	0	0	0	0	0	0	0	0	0	0
Nuclear Regulatory Commission	16	298.19	0	0	0	0	1	632	0	0	1	632
Nuclear Waste Technical Review Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Occupational Safety & Health Review Commission	0	0	0	0	0	0	0	0	0	0	0	0
Office of Government Ethics	2	15	2	15	0	0	0	0	0	0	0	0

Table B-10 FY 2012 Total Number and Average Processing Days for All Complaint Closures

Agency or Department	Total Number Complaint Closures	APD Complaint Closures from Date Complaint Filed/ Remanded	Total Number Dismissals	APD Dismissals by FAD or FO from Date Complaint Filed/ Remanded	Total Number Merit Final Agency Decisions (FADs) (No AJ Decision)	APD Merit FADS from Date Complaint Filed/ Remanded	*Number Final Orders (FOs) of Merit AJ Decisions	APD FOs of Merit AJ Decisions from Date Complaint Filed/ Remanded	*Total Number Complaint Closures Finding Discrimi-nation	APD Complaint Closures Finding Discrimi-nation from Date Complaint Filed/ Remanded	*Total Number Complaint Closures Finding No Discrimi-nation	APD Complaint Closures FInding No Discrimination from Date Complaint Filed/ Remanded
Office of Personnel Management	28	504.64	6	131.17	8	1,128.25	5	134.8	0	0	13	746.15
Office of Special Counsel	0	0	0	0	0	0	0	0	0	0	0	0
Office of the Director of National Intelligence	4	474	1	157	1	269	0	0	0	0	1	269
Overseas Private Investment Corporation	0	0	0	0	0	0	0	0	0	0	0	0
Peace Corps	4	508.75	1	934	3	367	0	0	0	0	3	367
Pension Benefit Guaranty Corporation	20	437.2	6	34.33	5	361.8	6	927.17	2	494.5	9	709.22
Postal Regulatory Commission	0	0	0	0	0	0	0	0	0	0	0	0
Presidio Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Railroad Retirement Board	1	660	0	0	0	0	0	0	0	0	0	0
Securities and Exchange Commission	4	308.25	2	282	2	334.5	0	0	0	0	2	334.5
Selective Service System	2	288	0	0	0	0	0	0	0	0	0	0
Small Business Administration	38	313.29	14	21	7	329	5	581	0	0	12	434
Smithsonian Institution	15	500.27	4	38.5	5	213.2	3	662.33	0	0	8	381.63
Social Security Administration	414	506.13	58	144.29	136	459.63	116	798.17	12	1,062.08	240	593.14
Tennessee Valley Authority	58	330.36	5	16.6	20	236.25	14	546.36	1	302	33	365.82
Trade and Development Agency	0	0	0	0	0	0	0	0	0	0	0	0
U.S. Postal Service	4,579	275.45	1,588	55.39	1,088	277.48	848	630.97	50	974.72	1,886	417.94
Utah Reclamation Mitigation and Conservation Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Valles Caldera Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Cabinet Level Subtotal	14,651	382.46	3,333	90.67	3,816	462.61	2,414	703.93	196	883.88	6,034	545.47
Midsize Agencies Subtotal	774	475.76	122	116.83	236	470.94	188	771.18	14	1,030.00	410	589.52
Small Agencies Subtotal	276	424.89	57	132.3	66	407.67	38	1,004.18	4	744	100	620.89
Micro Agencies Subtotal	5	513	3	321.33	0	0	0	0	0	0	0	0
Government-wide	15,706	387.84	3,515	92.45	4,118	462.21	2,640	713.04	214	890.82	6,544	549.38

NRF = No Report Filed

*This column also includes Merit Decisions (with AJ Decision) that are not fully implemented (i.e. appealed) by the agency.

Table B-11 FY 2012 Types of Complaints Closures

Agency or Department	Total Complaint Closures	Number Closures by Settlement	% Settlements	Number Closures by Withdrawal	% Withdrawals	Number Dismissal Closures	% Dismissals	Number Merit Complaint Closures	% Merit Complaint Closures
Advisory Council on Historic Preservation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
African Development Foundation	3	2	66.67%	0	0.00%	1	33.33%	0	0.00%
Agency for International Development	16	4	25.00%	3	18.75%	7	43.75%	2	12.50%
American Battle Monuments Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Appalachian Regional Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Architectural and Transportation Barriers Compliance Board	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Arctic Research Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Armed Forces Retirement Home	4	0	0.00%	0	0.00%	0	0.00%	4	100.00%
Barry Goldwater Scholarship and Excellence in Education Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Broadcasting Board of Governors	14	6	42.86%	0	0.00%	5	35.71%	3	21.43%
Central Intelligence Agency	39	10	25.64%	2	5.13%	10	25.64%	17	43.59%
Chemical Safety and Hazard Investigation Board	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Christopher Columbus Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission of Fine Arts	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission on Civil Rights	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Committee for Purchase from People Who Are Blind or Severely Disabled	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Commodity Futures Trading Commission	2	0	0.00%	0	0.00%	0	0.00%	2	100.00%
Consumer Financial Protection Bureau	7	3	42.86%	1	14.29%	0	0.00%	3	42.86%
Consumer Product Safety Commission	2	1	50.00%	0	0.00%	0	0.00%	1	50.00%
Corporation for National and Community Service	3	0	0.00%	0	0.00%	0	0.00%	3	100.00%
Court Services and Offender Supervision Agency for the District of Columbia	15	5	33.33%	1	6.67%	2	13.33%	7	46.67%
Defense Army and Air Force Exchange	89	26	29.21%	16	17.98%	20	22.47%	27	30.34%
Defense Commissary Agency	120	36	30.00%	17	14.17%	22	18.33%	45	37.50%
Defense Contract Audit Agency	32	12	37.50%	6	18.75%	4	12.50%	10	31.25%
Defense Contract Management Agency	38	9	23.68%	5	13.16%	16	42.11%	8	21.05%
Defense Finance and Accounting Service	39	13	33.33%	3	7.69%	9	23.08%	14	35.90%
Defense Human Resources Activity	5	1	20.00%	3	60.00%	1	20.00%	0	0.00%
Defense Information Systems Agency	8	2	25.00%	1	12.50%	5	62.50%	0	0.00%

Table B-11 FY 2012 Types of Complaints Closures

Agency or Department	Total Complaint Closures	Number Closures by Settlement	% Settlements	Number Closures by Withdrawal	% Withdrawals	Number Dismissal Closures	% Dismissals	Number Merit Complaint Closures	% Merit Complaint Closures
Defense Intelligence Agency	34	6	17.65%	3	8.82%	11	32.35%	14	41.18%
Defense Joint Task Force National Capital Region Medical	7	0	0.00%	2	28.57%	5	71.43%	0	0.00%
Defense Logistics Agency	136	49	36.03%	12	8.82%	14	10.29%	61	44.85%
Defense Media Activity	3	2	66.67%	1	33.33%	0	0.00%	0	0.00%
Defense Missile Defense Agency	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Defense National Geospatial-Intelligence Agency	20	7	35.00%	1	5.00%	5	25.00%	7	35.00%
Defense National Guard Bureau	33	6	18.18%	1	3.03%	23	69.70%	3	9.09%
Defense National Security Agency	17	4	23.53%	0	0.00%	4	23.53%	9	52.94%
Defense Nuclear Facilities Safety Board	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Defense Office of the Inspector General	3	2	66.67%	0	0.00%	1	33.33%	0	0.00%
Defense Office of the Secretary - Wash. Hqtrs. Services	45	12	26.67%	7	15.56%	13	28.89%	13	28.89%
Defense Security Service	6	1	16.67%	0	0.00%	2	33.33%	3	50.00%
Defense Technical Information Center	1	1	100.00%	0	0.00%	0	0.00%	0	0.00%
Defense Threat Reduction Agency	8	4	50.00%	0	0.00%	4	50.00%	0	0.00%
Defense TRICARE Management Activity	7	1	14.29%	1	14.29%	5	71.43%	0	0.00%
Defense Uniformed Services University	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Department of Agriculture	453	170	37.53%	29	6.40%	48	10.60%	206	45.47%
Department of Commerce	432	74	17.13%	12	2.78%	57	13.19%	289	66.90%
Department of Defense Education Activity	55	23	41.82%	4	7.27%	10	18.18%	18	32.73%
Department of Education	46	10	21.74%	5	10.87%	2	4.35%	29	63.04%
Department of Energy	63	27	42.86%	9	14.29%	6	9.52%	21	33.33%
Department of Health and Human Services	409	156	38.14%	28	6.85%	95	23.23%	130	31.78%
Department of Homeland Security	1,097	244	22.24%	118	10.76%	180	16.41%	555	50.59%
Department of Housing and Urban Development	73	23	31.51%	7	9.59%	3	4.11%	40	54.79%
Department of Justice	857	148	17.27%	93	10.85%	110	12.84%	506	59.04%
Department of Labor	134	49	36.57%	10	7.46%	19	14.18%	56	41.79%
Department of State	110	27	24.55%	13	11.82%	16	14.55%	54	49.09%
Department of the Air Force	500	174	34.80%	57	11.40%	76	15.20%	193	38.60%
Department of the Army	1,116	476	42.65%	100	8.96%	237	21.24%	303	27.15%
Department of the Interior	307	107	34.85%	23	7.49%	31	10.10%	146	47.56%

Table B-11 FY 2012 Types of Complaints Closures									
Agency or Department	**Total Complaint Closures**	**Number Closures by Settlement**	**% Settlements**	**Number Closures by Withdrawal**	**% Withdrawals**	**Number Dismissal Closures**	**% Dismissals**	**Number Merit Complaint Closures**	**% Merit Complaint Closures**
Department of the Navy	904	423	46.79%	141	15.60%	147	16.26%	193	21.35%
Department of the Treasury	407	96	23.59%	34	8.35%	51	12.53%	226	55.53%
Department of Transportation	335	93	27.76%	13	3.88%	87	25.97%	142	42.39%
Department of Veterans Affairs	2,123	520	24.49%	224	10.55%	406	19.12%	973	45.83%
Election Assistance Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Environmental Protection Agency	49	12	24.49%	11	22.45%	3	6.12%	23	46.94%
Equal Employment Opportunity Commission	20	6	30.00%	1	5.00%	5	25.00%	8	40.00%
Export-Import Bank of the US	1	0	0.00%	0	0.00%	1	100.00%	0	0.00%
Farm Credit Administration	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Farm Credit System Insurance Corporation	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Federal Communications Commission	2	0	0.00%	0	0.00%	2	100.00%	0	0.00%
Federal Deposit Insurance Corporation	42	14	33.33%	2	4.76%	12	28.57%	14	33.33%
Federal Election Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Federal Energy Regulatory Commission	10	1	10.00%	1	10.00%	2	20.00%	6	60.00%
Federal Financial Institutions Examination Council	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Housing Finance Agency	6	5	83.33%	0	0.00%	1	16.67%	0	0.00%
Federal Labor Relations Authority	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Federal Maritime Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Federal Mediation and Conciliation Service	2	0	0.00%	2	100.00%	0	0.00%	0	0.00%
Federal Mine Safety &Health Review Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Federal Reserve System--Board of Governors	6	2	33.33%	3	50.00%	0	0.00%	1	16.67%
Federal Retirement Thrift Investment Board	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Trade Commission	1	0	0.00%	0	0.00%	0	0.00%	1	100.00%
General Services Administration	85	18	21.18%	12	14.12%	11	12.94%	44	51.76%
Government Printing Office	29	10	34.48%	1	3.45%	5	17.24%	13	44.83%
Harry S. Truman Scholarship Foundation	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Holocaust Memorial Museum U.S.	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Institute of Museum and Library Services	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Inter-American Foundation	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
International Boundary and Water Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
International Joint Commission: US and Canada	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
International Trade Commission	1	1	100.00%	0	0.00%	0	0.00%	0	0.00%

Table B-11 FY 2012 Types of Complaints Closures

Agency or Department	Total Complaint Closures	Number Closures by Settlement	% Settlements	Number Closures by Withdrawal	% Withdrawals	Number Dismissal Closures	% Dismissals	Number Merit Complaint Closures	% Merit Complaint Closures
James Madison Memorial Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Japan-United States Friendship Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
John F. Kennedy Center for the Performing Arts	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Marine Mammal Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Merit Systems Protection Board	1	1	100.00%	0	0.00%	0	0.00%	0	0.00%
Millennium Challenge Corporation	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Aeronautics and Space Administration	38	7	18.42%	1	2.63%	9	23.68%	21	55.26%
National Archives and Records Administration	11	3	27.27%	0	0.00%	2	18.18%	6	54.55%
National Capital Planning Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
National Council on Disability	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
National Credit Union Administration	7	6	85.71%	0	0.00%	0	0.00%	1	14.29%
National Endowment for the Arts	3	2	66.67%	0	0.00%	1	33.33%	0	0.00%
National Endowment for the Humanities	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
National Foundation on the Arts &the Humanities	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Gallery of Art	6	2	33.33%	0	0.00%	1	16.67%	3	50.00%
National Indian Gaming Commission	1	0	0.00%	1	100.00%	0	0.00%	0	0.00%
National Labor Relations Board	8	3	37.50%	1	12.50%	1	12.50%	3	37.50%
National Mediation Board	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
National Reconnaissance Office	7	1	14.29%	0	0.00%	2	28.57%	4	57.14%
National Science Foundation	6	6	100.00%	0	0.00%	0	0.00%	0	0.00%
National Transportation Safety Board	2	0	0.00%	1	50.00%	0	0.00%	1	50.00%
Navajo and Hopi Indian Relocation Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Nuclear Regulatory Commission	16	11	68.75%	4	25.00%	0	0.00%	1	6.25%
Nuclear Waste Technical Review Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Occupational Safety& Health Review Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Office of Government Ethics	2	0	0.00%	0	0.00%	2	100.00%	0	0.00%
Office of Personnel Management	28	3	10.71%	6	21.43%	6	21.43%	13	46.43%
Office of Special Counsel	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Office of the Director of National Intelligence	4	2	50.00%	0	0.00%	1	25.00%	1	25.00%
Overseas Private Investment Corporation	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%

Table B-11 FY 2012 Types of Complaints Closures

Agency or Department	Total Complaint Closures	Number Closures by Settlement	% Settlements	Number Closures by Withdrawal	% Withdrawals	Number Dismissal Closures	% Dismissals	Number Merit Complaint Closures	% Merit Complaint Closures
Peace Corps	4	0	0.00%	0	0.00%	1	25.00%	3	75.00%
Pension Benefit Guaranty Corporation	20	1	5.00%	2	10.00%	6	30.00%	11	55.00%
Postal Regulatory Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Presidio Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Railroad Retirement Board	1	1	100.00%	0	0.00%	0	0.00%	0	0.00%
Securities and Exchange Commission	4	0	0.00%	0	0.00%	2	50.00%	2	50.00%
Selective Service System	2	2	100.00%	0	0.00%	0	0.00%	0	0.00%
Small Business Administration	38	11	28.95%	1	2.63%	14	36.84%	12	31.58%
Smithsonian Institution	15	3	20.00%	0	0.00%	4	26.67%	8	53.33%
Social Security Administration	414	50	12.08%	54	13.04%	58	14.01%	252	60.87%
Tennessee Valley Authority	58	12	20.69%	7	12.07%	5	8.62%	34	58.62%
Trade and Development Agency	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
U.S. Postal Service	4,579	815	17.80%	240	5.24%	1,588	34.68%	1,936	42.28%
Utah Reclamation Mitigation and Conservation Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Valles Caldera Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Cabinet Level Subtotal	14,651	3,849	26.27%	1,239	8.46%	3,333	22.75%	6,230	42.52%
Midsize Agencies Subtotal	774	133	17.18%	95	12.27%	122	15.76%	424	54.78%
Small Agencies Subtotal	276	92	33.33%	23	8.33%	57	20.65%	104	37.68%
Micro Agencies Subtotal	5	2	40.00%	0	0.00%	3	60.00%	0	0.00%
Government-wide	15,706	4,076	25.95%	1,357	8.64%	3,515	22.38%	6,758	43.03%

NRF = No Report Filed

Table B-11a FY 2012 Types of Complaints Closures - Sub-Component Data									
Agency or Department	**Total Complaint Closures**	**Number Closures by Settlement**	**% Settlements**	**Number Closures by Withdrawal**	**% Withdrawals**	**Number Dismissal Closures**	**% Dismissals**	**Number Merit Complaint Closures**	**% Merit Complaint Closures**
Defense Logistics Agency Wide	**136**	**49**	**36.03%**	**12**	**8.82%**	**14**	**10.29%**	**61**	**44.85%**
Defense Logistics Agency Headquarters	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
DLA Aviation	20	6	30.00%	3	15.00%	2	10.00%	9	45.00%
DLA Disposition Services	9	1	11.11%	0	0.00%	0	0.00%	8	88.89%
DLA Distribution	56	19	33.93%	6	10.71%	9	16.07%	22	39.29%
DLA Headquarters Operations Division	22	12	54.55%	2	9.09%	2	9.09%	6	27.27%
DLA Land and Maritime	16	7	43.75%	1	6.25%	1	6.25%	7	43.75%
DLA Logistics Information Service	4	0	0.00%	0	0.00%	0	0.00%	4	100.00%
DLA Troop Support	9	4	44.44%	0	0.00%	0	0.00%	5	55.56%
Defense National Guard Bureau Wide	**33**	**6**	**18.18%**	**1**	**3.03%**	**23**	**69.70%**	**3**	**9.09%**
Defense National Guard Bureau Headquarters	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Alabama National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Alaska National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Arizona National Guard	3	1	33.33%	0	0.00%	2	66.67%	0	0.00%
Arkansas National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
California National Guard	7	1	14.29%	0	0.00%	6	85.71%	0	0.00%
Colorado National Guard	1	0	0.00%	0	0.00%	1	100.00%	0	0.00%
Connecticut National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
DC National Guard	1	0	0.00%	0	0.00%	1	100.00%	0	0.00%
Delaware National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Florida National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Georgia National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Guam National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Hawaii National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Idaho National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Illinois National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Indiana National Guard	1	0	0.00%	1	100.00%	0	0.00%	0	0.00%
Iowa National Guard	1	0	0.00%	0	0.00%	1	100.00%	0	0.00%
Kansas National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Kentucky National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Louisiana National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Maine National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%

Table B-11a FY 2012 Types of Complaints Closures - Sub-Component Data									
Agency or Department	**Total Complaint Closures**	**Number Closures by Settlement**	**% Settlements**	**Number Closures by Withdrawal**	**% Withdrawals**	**Number Dismissal Closures**	**% Dismissals**	**Number Merit Complaint Closures**	**% Merit Complaint Closures**
Maryland National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Massachusetts National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Michigan National Guard	1	1	100.00%	0	0.00%	0	0.00%	0	0.00%
Minnesota National Guard	1	0	0.00%	0	0.00%	1	100.00%	0	0.00%
Mississippi National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Missouri National Guard	2	0	0.00%	0	0.00%	2	100.00%	0	0.00%
Montana National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Nebraska National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Nevada National Guard	1	0	0.00%	0	0.00%	1	100.00%	0	0.00%
New Hampshire National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
New Jersey National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
New Mexico National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
New York National Guard	3	3	100.00%	0	0.00%	0	0.00%	0	0.00%
North Carolina National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
North Dakota National Guard	1	0	0.00%	0	0.00%	1	100.00%	0	0.00%
Ohio National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Oklahoma National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Oregon National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Pennsylvania National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Puerto Rico National Guard	1	0	0.00%	0	0.00%	1	100.00%	0	0.00%
Rhode Island National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
South Carolina National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
South Dakota National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Tennessee National Guard	3	0	0.00%	0	0.00%	0	0.00%	3	100.00%
Texas National Guard	5	0	0.00%	0	0.00%	5	100.00%	0	0.00%
Utah National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Vermont National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Virgin Islands National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Virginia National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Washington State National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
West Virginia National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Wisconsin National Guard	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Wyoming National Guard	1	0	0.00%	0	0.00%	1	100.00%	0	0.00%

Table B-11a FY 2012 Types of Complaints Closures - Sub-Component Data									
Agency or Department	**Total Complaint Closures**	**Number Closures by Settlement**	**% Settlements**	**Number Closures by Withdrawal**	**% Withdrawals**	**Number Dismissal Closures**	**% Dismissals**	**Number Merit Complaint Closures**	**% Merit Complaint Closures**
Department of Agriculture Wide	**453**	**170**	**37.53%**	**29**	**6.40%**	**48**	**10.60%**	**206**	**45.47%**
Department of Agriculture Headquarters	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
USDA Agricultural Marketing Service	21	12	57.14%	2	9.52%	2	9.52%	5	23.81%
USDA Agricultural Research Service	27	7	25.93%	3	11.11%	3	11.11%	14	51.85%
USDA Agriculture Headquarters	23	12	52.17%	2	8.70%	0	0.00%	9	39.13%
USDA Animal and Plant Health Inspection Service	43	15	34.88%	1	2.33%	7	16.28%	20	46.51%
USDA Economic Research Service	1	0	0.00%	1	100.00%	0	0.00%	0	0.00%
USDA Farm Service Agency	28	14	50.00%	0	0.00%	0	0.00%	14	50.00%
USDA Food and Nutrition Service	8	0	0.00%	2	25.00%	0	0.00%	6	75.00%
USDA Food Safety And Inspection Service	77	31	40.26%	5	6.49%	7	9.09%	34	44.16%
USDA Foreign Agricultural Service	4	0	0.00%	0	0.00%	2	50.00%	2	50.00%
USDA Forest Service	128	48	37.50%	7	5.47%	18	14.06%	55	42.97%
USDA Grain Inspection, Packers & Stockyards Admin	7	2	28.57%	0	0.00%	0	0.00%	5	71.43%
USDA National Agricultural Statistics Service	1	1	100.00%	0	0.00%	0	0.00%	0	0.00%
USDA National Appeals Division	1	1	100.00%	0	0.00%	0	0.00%	0	0.00%
USDA National Institute of Food and Agriculture	2	1	50.00%	0	0.00%	1	50.00%	0	0.00%
USDA Natural Resources Conservation Service	22	8	36.36%	0	0.00%	3	13.64%	11	50.00%
USDA Office Of The Chief Financial Officer	14	5	35.71%	2	14.29%	0	0.00%	7	50.00%
USDA - Office Of Inspector General	2	0	0.00%	0	0.00%	0	0.00%	2	100.00%
USDA Risk Management Agency	6	2	33.33%	1	16.67%	0	0.00%	3	50.00%
USDA Rural Development	38	11	28.95%	3	7.89%	5	13.16%	19	50.00%
Department of Commerce Wide	**432**	**74**	**17.13%**	**12**	**2.78%**	**57**	**13.19%**	**289**	**66.90%**
Department of Commerce Headquarters	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
DOC All Other Commerce Bureaus	26	7	26.92%	2	7.69%	5	19.23%	12	46.15%
DOC Bureau of the Census	52	10	19.23%	4	7.69%	10	19.23%	28	53.85%
DOC Decennial Census	249	27	10.84%	3	1.20%	14	5.62%	205	82.33%
DOC International Trade Administration	6	2	33.33%	0	0.00%	2	33.33%	2	33.33%
DOC National Institute of Standards & Technology	14	3	21.43%	1	7.14%	4	28.57%	6	42.86%
DOC National Oceanic & Atmospheric Administration	53	18	33.96%	1	1.89%	7	13.21%	27	50.94%
DOC U. S. Patent and Trademark Office	32	7	21.88%	1	3.13%	15	46.88%	9	28.13%

Table B-11a FY 2012 Types of Complaints Closures - Sub-Component Data

Agency or Department	Total Complaint Closures	Number Closures by Settlement	% Settlements	Number Closures by Withdrawal	% Withdrawals	Number Dismissal Closures	% Dismissals	Number Merit Complaint Closures	% Merit Complaint Closures
Department of Energy Wide	**63**	**27**	**42.86%**	**9**	**14.29%**	**6**	**9.52%**	**21**	**33.33%**
Department of Energy Headquarters	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
DOE Bonneville Power Administration	13	5	38.46%	3	23.08%	2	15.38%	3	23.08%
DOE Chicago Operations Office	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
DOE EM Consolidated Business Center	1	0	0.00%	0	0.00%	1	100.00%	0	0.00%
DOE Golden Field Office	1	1	100.00%	0	0.00%	0	0.00%	0	0.00%
DOE Headquarters	18	7	38.89%	4	22.22%	2	11.11%	5	27.78%
DOE Idaho Operations Office	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
DOE National Energy Technology Lab	1	0	0.00%	0	0.00%	1	100.00%	0	0.00%
DOE NNSA Service Center	9	5	55.56%	0	0.00%	0	0.00%	4	44.44%
DOE Oak Ridge Operations	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
DOE OSTI	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
DOE Richland Operations Office	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
DOE Savannah River Operations	2	0	0.00%	0	0.00%	0	0.00%	2	100.00%
DOE Southeastern Power Administration	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
DOE Southwestern Power Administration	3	0	0.00%	2	66.67%	0	0.00%	1	33.33%
DOE Strategic Petroleum Reserve	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
DOE Western Area Power Administration	15	9	60.00%	0	0.00%	0	0.00%	6	40.00%
Department of Health and Human Services Wide	**409**	**156**	**38.14%**	**28**	**6.85%**	**95**	**23.23%**	**130**	**31.78%**
Department of Health & Human Services Headquarters	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
HHS Administration for Children and Families	5	1	20.00%	0	0.00%	1	20.00%	3	60.00%
HHS Agency for Healthcare Research and Quality	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
HHS Centers for Disease Control and Prevention	69	23	33.33%	5	7.25%	20	28.99%	21	30.43%
HHS Centers for Medicare & Medicaid Services	38	14	36.84%	3	7.89%	7	18.42%	14	36.84%
HHS Food and Drug Administration	60	34	56.67%	6	10.00%	14	23.33%	6	10.00%
HHS Health Resources and Services Administration	13	4	30.77%	2	15.38%	0	0.00%	7	53.85%
HHS Indian Health Service	105	26	24.76%	5	4.76%	38	36.19%	36	34.29%
HHS National Institutes of Health	82	40	48.78%	3	3.66%	12	14.63%	27	32.93%
HHS Office of the Secretary of Health & Human Srvcs	30	10	33.33%	3	10.00%	2	6.67%	15	50.00%
HHS Program Support Center	1	0	0.00%	0	0.00%	1	100.00%	0	0.00%
HHS Substance Abuse & Mental Health Srvcs Admin	6	4	66.67%	1	16.67%	0	0.00%	1	16.67%

Table B-11a FY 2012 Types of Complaints Closures - Sub-Component Data									
Agency or Department	**Total Complaint Closures**	**Number Closures by Settlement**	**% Settlements**	**Number Closures by Withdrawal**	**% Withdrawals**	**Number Dismissal Closures**	**% Dismissals**	**Number Merit Complaint Closures**	**% Merit Complaint Closures**
Department of Homeland Security Wide	**1,097**	**244**	**22.24%**	**118**	**10.76%**	**180**	**16.41%**	**555**	**50.59%**
Department of Homeland Security Headquarters	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
DHS Federal Emergency Management Agency	96	21	21.88%	14	14.58%	7	7.29%	54	56.25%
DHS Federal Law Enforcement Training Center	16	9	56.25%	1	6.25%	2	12.50%	4	25.00%
DHS Headquarters	24	5	20.83%	6	25.00%	2	8.33%	11	45.83%
DHS Transportation Security Administration	373	80	21.45%	27	7.24%	95	25.47%	171	45.84%
DHS U.S. Citizenship and Immigration Services	78	14	17.95%	9	11.54%	13	16.67%	42	53.85%
DHS U.S. Coast Guard	51	12	23.53%	6	11.76%	9	17.65%	24	47.06%
DHS U.S. Customs and Border Protection	294	58	19.73%	45	15.31%	33	11.22%	158	53.74%
DHS U.S. Immigration and Customs Enforcement	133	38	28.57%	9	6.77%	9	6.77%	77	57.89%
DHS U.S. Secret Service	32	7	21.88%	1	3.13%	10	31.25%	14	43.75%
Department of Justice Wide	**857**	**148**	**17.27%**	**93**	**10.85%**	**110**	**12.84%**	**506**	**59.04%**
Department of Justice Headquarters	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
DOJ Alcohol, Tobacco, Firearms and Explosives	52	12	23.08%	4	7.69%	6	11.54%	30	57.69%
DOJ Bureau of Prisons	412	68	16.50%	58	14.08%	58	14.08%	228	55.34%
DOJ Drug Enforcement Administration	32	3	9.38%	1	3.13%	5	15.63%	23	71.88%
DOJ Executive Office for Immigration Review	11	1	9.09%	0	0.00%	1	9.09%	9	81.82%
DOJ Executive Office for U.S. Attorneys	42	8	19.05%	4	9.52%	7	16.67%	23	54.76%
DOJ Federal Bureau of Investigation	203	20	9.85%	18	8.87%	23	11.33%	142	69.95%
DOJ Office of Justice Programs	9	3	33.33%	3	33.33%	2	22.22%	1	11.11%
DOJ Offices, Boards, and Divisions	34	15	44.12%	3	8.82%	1	2.94%	15	44.12%
DOJ U.S. Marshals Service	62	18	29.03%	2	3.23%	7	11.29%	35	56.45%
Department of Labor Wide	**134**	**49**	**36.57%**	**10**	**7.46%**	**19**	**14.18%**	**56**	**41.79%**
Department of Labor Headquarters	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
DOL (DM and others)	51	17	33.33%	5	9.80%	8	15.69%	21	41.18%
DOL Bureau of Labor Statistics	4	0	0.00%	0	0.00%	1	25.00%	3	75.00%
DOL Employment and Training Administration	18	4	22.22%	1	5.56%	2	11.11%	11	61.11%
DOL Mine Safety and Health Administration	15	9	60.00%	1	6.67%	0	0.00%	5	33.33%
DOL Occupational Safety& Health Administration	18	9	50.00%	1	5.56%	4	22.22%	4	22.22%
DOL Office of Workers Compensation Programs	15	4	26.67%	1	6.67%	2	13.33%	8	53.33%
DOL Wage and Hour Division	13	6	46.15%	1	7.69%	2	15.38%	4	30.77%

Table B-11a FY 2012 Types of Complaints Closures - Sub-Component Data									
Agency or Department	**Total Complaint Closures**	**Number Closures by Settlement**	**% Settlements**	**Number Closures by Withdrawal**	**% Withdrawals**	**Number Dismissal Closures**	**% Dismissals**	**Number Merit Complaint Closures**	**% Merit Complaint Closures**
Department of the Army Wide	**1,116**	**476**	**42.65%**	**100**	**8.96%**	**237**	**21.24%**	**303**	**27.15%**
Department of the Army Headquarters	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Eighth U.S. Army (KOREA)	5	2	40.00%	1	20.00%	1	20.00%	1	20.00%
Headquarters, Department of Army	66	21	31.82%	9	13.64%	16	24.24%	20	30.30%
U.S. Army Corps of Engineers	135	51	37.78%	6	4.44%	47	34.81%	31	22.96%
U.S. Army Europe	4	1	25.00%	2	50.00%	1	25.00%	0	0.00%
U.S. Army Forces Command	85	37	43.53%	10	11.76%	21	24.71%	17	20.00%
U.S. Army Installation Management Command	279	135	48.39%	27	9.68%	43	15.41%	74	26.52%
U.S. Army Intelligence and Security Command	12	3	25.00%	1	8.33%	2	16.67%	6	50.00%
U.S. Army Material Command	259	109	42.08%	21	8.11%	61	23.55%	68	26.25%
U.S. Army Medical Command	175	78	44.57%	15	8.57%	33	18.86%	49	28.00%
U.S. Army Network Enterprise Technology Command	10	7	70.00%	0	0.00%	1	10.00%	2	20.00%
U.S. Army Pacific (USARPAC)	1	0	0.00%	0	0.00%	1	100.00%	0	0.00%
U.S. Army Space and Missile Defense Command	5	0	0.00%	0	0.00%	0	0.00%	5	100.00%
U.S. Army Special Operations Command (USASOC)	7	4	57.14%	1	14.29%	1	14.29%	1	14.29%
U.S. Army Test and Evaluation Command	12	7	58.33%	0	0.00%	2	16.67%	3	25.00%
U.S. Army Training and Doctrine Command	61	21	34.43%	7	11.48%	7	11.48%	26	42.62%
Department of the Interior Wide	**307**	**107**	**34.85%**	**23**	**7.49%**	**31**	**10.10%**	**146**	**47.56%**
Department of the Interior Headquarters	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Bureau of Ocean Energy Management	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Bureau of Safety and Environmental Enforcement	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
DOI Bureau Of Indian Affairs	49	15	30.61%	4	8.16%	3	6.12%	27	55.10%
DOI Bureau Of Land Management	36	10	27.78%	3	8.33%	6	16.67%	17	47.22%
DOI Bureau Of Reclamation	49	17	34.69%	5	10.20%	4	8.16%	23	46.94%
DOI Fish And Wildlife Service	27	6	22.22%	1	3.70%	7	25.93%	13	48.15%
DOI Geological Survey	18	11	61.11%	1	5.56%	1	5.56%	5	27.78%
DOI National Park Service	74	27	36.49%	5	6.76%	7	9.46%	35	47.30%
DOI Office Of Surface Mining,Reclamation &	5	2	40.00%	2	40.00%	0	0.00%	1	20.00%
DOI-Office Of The Secretary	49	19	38.78%	2	4.08%	3	6.12%	25	51.02%

Table B-11a FY 2012 Types of Complaints Closures - Sub-Component Data

Agency or Department	Total Complaint Closures	Number Closures by Settlement	% Settlements	Number Closures by Withdrawal	% Withdrawals	Number Dismissal Closures	% Dismissals	Number Merit Complaint Closures	% Merit Complaint Closures
Department of the Navy Wide	**904**	**423**	**46.79%**	**141**	**15.60%**	**147**	**16.26%**	**193**	**21.35%**
Department of the Navy Headquarters	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Chief Of Naval Operations	12	2	16.67%	2	16.67%	2	16.67%	6	50.00%
Commander Naval Installations Command	171	42	24.56%	75	43.86%	21	12.28%	33	19.30%
Commander Naval Reserve	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Commander Pacific Fleet	39	15	38.46%	3	7.69%	8	20.51%	13	33.33%
DON Assistant for Administration	20	11	55.00%	1	5.00%	1	5.00%	7	35.00%
DON Bureau of Medicine & Surgery	58	18	31.03%	7	12.07%	17	29.31%	16	27.59%
DON SPAWAR	6	1	16.67%	2	33.33%	1	16.67%	2	33.33%
DON Strategic Systems Project Office	3	1	33.33%	1	33.33%	0	0.00%	1	33.33%
Fleet Cyber Command	1	1	100.00%	0	0.00%	0	0.00%	0	0.00%
Fleet Forces Command	36	16	44.44%	2	5.56%	8	22.22%	10	27.78%
Marine Corps HQ	321	243	75.70%	18	5.61%	29	9.03%	31	9.66%
Military Sealift Command	23	7	30.43%	7	30.43%	6	26.09%	3	13.04%
Naval Air Systems Command	57	13	22.81%	5	8.77%	25	43.86%	14	24.56%
Naval Education & Training Command	15	5	33.33%	2	13.33%	5	33.33%	3	20.00%
Naval Sea Systems Command	36	12	33.33%	3	8.33%	7	19.44%	14	38.89%
Naval Special Warfare Command	3	2	66.67%	0	0.00%	1	33.33%	0	0.00%
Naval Supply Systems Command	41	15	36.59%	3	7.32%	6	14.63%	17	41.46%
Naval Systems Management Activity	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Navy Facilities & Engineering Command	56	17	30.36%	10	17.86%	9	16.07%	20	35.71%
Navy Military Personnel Command	2	1	50.00%	0	0.00%	0	0.00%	1	50.00%
Office Of Naval Intelligence	2	1	50.00%	0	0.00%	0	0.00%	1	50.00%
Office Of Naval Research	2	0	0.00%	0	0.00%	1	50.00%	1	50.00%
Department of the Treasury Wide	**407**	**96**	**23.59%**	**34**	**8.35%**	**51**	**12.53%**	**226**	**55.53%**
Department of the Treasury Headquarters	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Treas - Alcohol and Tobacco Tax & Trade Bureau	3	2	66.67%	0	0.00%	0	0.00%	1	33.33%
Treas - Bureau of Engraving and Printing	16	4	25.00%	3	18.75%	2	12.50%	7	43.75%
Treas - Bureau of the Public Debt	2	0	0.00%	1	50.00%	0	0.00%	1	50.00%
Treas - Departmental Offices	16	4	25.00%	0	0.00%	3	18.75%	9	56.25%
Treas - Financial Crimes Enforcement Network	2	0	0.00%	0	0.00%	0	0.00%	2	100.00%

Table B-11a FY 2012 Types of Complaints Closures - Sub-Component Data									
Agency or Department	**Total Complaint Closures**	**Number Closures by Settlement**	**% Settlements**	**Number Closures by Withdrawal**	**% Withdrawals**	**Number Dismissal Closures**	**% Dismissals**	**Number Merit Complaint Closures**	**% Merit Complaint Closures**
Treas - Financial Management Service	7	2	28.57%	1	14.29%	0	0.00%	4	57.14%
Treas - Inspector General For Tax Administration	1	0	0.00%	0	0.00%	0	0.00%	1	100.00%
Treas - Internal Revenue Service	283	52	18.37%	23	8.13%	38	13.43%	170	60.07%
Treas - Office of the Comptroller of the Currency	9	4	44.44%	0	0.00%	2	22.22%	3	33.33%
Treas - Special Inspector General for the Trouble	1	1	100.00%	0	0.00%	0	0.00%	0	0.00%
Treas - U. S. Mint	57	23	40.35%	4	7.02%	5	8.77%	25	43.86%
Treas -Internal Revenue Service Office of the Chief	9	3	33.33%	2	22.22%	1	11.11%	3	33.33%
Treas- Office of the Inspector General	1	1	100.00%	0	0.00%	0	0.00%	0	0.00%
Department of Transportation Wide	**335**	**93**	**27.76%**	**13**	**3.88%**	**87**	**25.97%**	**142**	**42.39%**
Department of Transportation Headquarters	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
DOT Federal Aviation Administration	268	70	26.12%	11	4.10%	75	27.99%	112	41.79%
DOT Federal Highway Administration	10	4	40.00%	0	0.00%	0	0.00%	6	60.00%
DOT Federal Motor Carrier Safety Administration	7	0	0.00%	0	0.00%	0	0.00%	7	100.00%
DOT Federal Railroad Administrataion	6	1	16.67%	0	0.00%	3	50.00%	2	33.33%
DOT Federal Transit Administration	3	1	33.33%	0	0.00%	2	66.67%	0	0.00%
DOT Maritime Administration	11	5	45.45%	1	9.09%	1	9.09%	4	36.36%
DOT National Highway Traffic Safety Admin	5	2	40.00%	0	0.00%	2	40.00%	1	20.00%
DOT Office of Inspector General	3	0	0.00%	0	0.00%	0	0.00%	3	100.00%
DOT Office of the Secretary	8	6	75.00%	0	0.00%	0	0.00%	2	25.00%
DOT Pipeline& Hazardous Materials Safety Admin	1	0	0.00%	0	0.00%	1	100.00%	0	0.00%
DOT Research & Innovative Technology Admin	13	4	30.77%	1	7.69%	3	23.08%	5	38.46%
DOT St. Lawrence Development Corporation	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Department of Veterans Affairs Wide	**2,123**	**520**	**24.49%**	**224**	**10.55%**	**406**	**19.12%**	**973**	**45.83%**
Department of Veterans Affairs Headquarters	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
VA-HQ and Others	106	26	24.53%	14	13.21%	42	39.62%	24	22.64%
VA-NCA	20	5	25.00%	1	5.00%	3	15.00%	11	55.00%
VA-Veterans Benefits Administration	149	45	30.20%	17	11.41%	29	19.46%	58	38.93%
VA-Veterans Health Administration	1,848	444	24.03%	192	10.39%	332	17.97%	880	47.62%

Table B-11a FY 2012 Types of Complaints Closures - Sub-Component Data

Agency or Department	Total Complaint Closures	Number Closures by Settlement	% Settlements	Number Closures by Withdrawal	% Withdrawals	Number Dismissal Closures	% Dismissals	Number Merit Complaint Closures	% Merit Complaint Closures
Federal Housing Finance Agency Wide	**6**	**5**	**83.33%**	**0**	**0.00%**	**1**	**16.67%**	**0**	**0.00%**
Federal Housing Finance Agency Headquarters	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Federal Housing Finance Agency Hqtrs	6	5	83.33%	0	0.00%	1	16.67%	0	0.00%
Federal Housing Finance Agency OIG	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
General Services Administration Wide	**85**	**18**	**21.18%**	**12**	**14.12%**	**11**	**12.94%**	**44**	**51.76%**
General Services Administration Headquarters	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
GSA Central Office	15	2	13.33%	4	26.67%	1	6.67%	8	53.33%
GSA National Capital Region	20	5	25.00%	2	10.00%	2	10.00%	11	55.00%
GSA Region 1	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
GSA Region 10	2	1	50.00%	0	0.00%	1	50.00%	0	0.00%
GSA Region 2	7	1	14.29%	1	14.29%	0	0.00%	5	71.43%
GSA Region 3	9	2	22.22%	1	11.11%	0	0.00%	6	66.67%
GSA Region 4	7	1	14.29%	2	28.57%	0	0.00%	4	57.14%
GSA Region 5	6	3	50.00%	1	16.67%	0	0.00%	2	33.33%
GSA Region 6	1	0	0.00%	0	0.00%	0	0.00%	1	100.00%
GSA Region 7	4	3	75.00%	0	0.00%	1	25.00%	0	0.00%
GSA Region 8	1	0	0.00%	0	0.00%	1	100.00%	0	0.00%
GSA Region 9	13	0	0.00%	1	7.69%	5	38.46%	7	53.85%
U.S. Postal Service Wide	**4,579**	**815**	**17.80%**	**240**	**5.24%**	**1,588**	**34.68%**	**1,936**	**42.28%**
U.S. Postal Service Headquarters	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
USPS Capital Metro Area Operations	617	105	17.02%	24	3.89%	205	33.23%	283	45.87%
USPS Eastern Area	677	105	15.51%	49	7.24%	208	30.72%	315	46.53%
USPS Great Lakes Area	550	95	17.27%	32	5.82%	193	35.09%	230	41.82%
USPS Headquarters	86	15	17.44%	8	9.30%	28	32.56%	35	40.70%
USPS Northeast Area	397	91	22.92%	25	6.30%	132	33.25%	149	37.53%
USPS Office of Inspector General	14	1	7.14%	0	0.00%	7	50.00%	6	42.86%
USPS Pacific Area	493	109	22.11%	28	5.68%	162	32.86%	194	39.35%
USPS Southern Area	1,126	171	15.19%	51	4.53%	392	34.81%	512	45.47%
USPS Western Area	619	123	19.87%	23	3.72%	261	42.16%	212	34.25%

Table B-12 FY 2012 Average Processing Days (APD) All Complaint Closures

Agency or Department	APD All Complaint Closures from Date Complaint Filed/ Remanded	APD All Withdrawals from Date Complaint Filed/ Remanded	APD Non-ADR Withdrawals from Date Complaint Filed/ Remanded	APD ADR Withdrawals from Date Complaint Filed/ Remanded	APD All Settlements from Date Complaint Filed/ Remanded	APD Non-ADR Settlements from Date Complaint Filed/ Remanded	APD ADR Settlements from Date Complaint Filed/ Remanded	APD All Final Agency Actions from Date Complaint Filed/ Remanded
Advisory Council on Historic Preservation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
African Development Foundation	845	0	0	0	800.5	800.5	0	934
Agency for International Development	398.81	370	370	0	567.75	567.75	0	333.33
American Battle Monuments Commission	0	0	0	0	0	0	0	0
Appalachian Regional Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Architectural and Transportation Barriers Compliance Board	0	0	0	0	0	0	0	0
Arctic Research Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Armed Forces Retirement Home	243.5	0	0	0	0	0	0	243.5
Barry Goldwater Scholarship and Excellence in Education Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Broadcasting Board of Governors	356.29	0	0	0	369.67	369.67	0	346.25
Central Intelligence Agency	585.38	118	118	0	448.4	448.4	0	670.74
Chemical Safety and Hazard Investigation Board	0	0	0	0	0	0	0	0
Christopher Columbus Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission of Fine Arts	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission on Civil Rights	0	0	0	0	0	0	0	0
Committee for Purchase from People Who Are Blind or Severely Disabled	0	0	0	0	0	0	0	0
Commodity Futures Trading Commission	314	0	0	0	0	0	0	314
Consumer Financial Protection Bureau	181.29	293	293	0	24.33	24.33	0	301
Consumer Product Safety Commission	380	0	0	0	344	344	0	416
Corporation for National and Community Service	431.67	0	0	0	0	0	0	431.67
Court Services and Offender Supervision Agency for the District of Columbia	756.93	441	441	0	1,089.60	1,089.60	0	607.22
Defense Army and Air Force Exchange	318.17	179.38	189.15	137	291.19	438.4	90.45	380.34
Defense Commissary Agency	318.85	191.12	204.6	90	338.56	391.96	178.33	340.67
Defense Contract Audit Agency	252.25	80.33	80.33	0	284.5	41.5	406	298.29
Defense Contract Management Agency	345.03	290.2	290.2	0	641.33	1,358.00	68	245.33
Defense Finance and Accounting Service	352.74	176.33	176.33	0	496.77	496.77	0	294.35

Table B-12 FY 2012 Average Processing Days (APD) All Complaint Closures

Agency or Department	APD All Complaint Closures from Date Complaint Filed/ Remanded	APD All Withdrawals from Date Complaint Filed/ Remanded	APD Non-ADR Withdrawals from Date Complaint Filed/ Remanded	APD ADR Withdrawals from Date Complaint Filed/ Remanded	APD All Settlements from Date Complaint Filed/ Remanded	APD Non-ADR Settlements from Date Complaint Filed/ Remanded	APD ADR Settlements from Date Complaint Filed/ Remanded	APD All Final Agency Actions from Date Complaint Filed/ Remanded
Defense Human Resources Activity	149	48.67	0	48.67	567	0	567	32
Defense Information Systems Agency	686.75	212	212	0	150	150	0	996.4
Defense Intelligence Agency	518.88	440.33	440.33	0	654.83	654.83	0	495.68
Defense Joint Task Force National Capital Region Medical	92	189.5	189.5	0	0	0	0	53
Defense Logistics Agency	463.1	292.92	292.92	0	486.84	616.18	220.06	474.81
Defense Media Activity	453	60	60	0	649.5	0	649.5	0
Defense Missile Defense Agency	0	0	0	0	0	0	0	0
Defense National Geospatial-Intelligence Agency	427.3	819	819	0	348.71	348.71	0	440.5
Defense National Guard Bureau	327.39	400	400	0	193.33	315	169	355.54
Defense National Security Agency	636.29	0	0	0	535.75	535.75	0	667.23
Defense Nuclear Facilities Safety Board	0	0	0	0	0	0	0	0
Defense Office of the Inspector General	468.67	0	0	0	699	699	0	8
Defense Office of the Secretary - Wash. Hqtrs. Services	569.62	606	606	0	500.33	540.09	63	591.81
Defense Security Service	166.67	0	0	0	200	200	0	160
Defense Technical Information Center	599	0	0	0	599	599	0	0
Defense Threat Reduction Agency	742.75	0	0	0	616.75	616.75	0	868.75
Defense TRICARE Management Activity	217.29	173	173	0	809	0	809	107.8
Defense Uniformed Services University	0	0	0	0	0	0	0	0
Department of Agriculture	633.2	373.72	373.72	0	750.25	717.56	916.04	584.48
Department of Commerce	465.11	137.17	137.17	0	254.39	263.74	90.75	521.55
Department of Defense Education Activity	405.89	293.75	293.75	0	475	494.09	55	365.14
Department of Education	565.93	337	337	0	538.9	538.9	0	611.58
Department of Energy	344.75	264.89	264.89	0	343.59	383.62	203.5	372.52
Department of Health and Human Services	340.52	201.11	201.11	0	411.37	439.58	146.2	308.75
Department of Homeland Security	461.88	261.46	265.12	121	469.36	491.43	192.22	491.57
Department of Housing and Urban Development	594.14	392.29	392.29	0	548.83	615.05	107.33	651.23
Department of Justice	591.89	337.88	340.89	61	477.32	568.99	192.11	657.77
Department of Labor	505.19	154.4	154.4	0	687.22	0	687.22	433.04

Table B-12 FY 2012 Average Processing Days (APD) All Complaint Closures

Agency or Department	APD All Complaint Closures from Date Complaint Filed/ Remanded	APD All Withdrawals from Date Complaint Filed/ Remanded	APD Non-ADR Withdrawals from Date Complaint Filed/ Remanded	APD ADR Withdrawals from Date Complaint Filed/ Remanded	APD All Settlements from Date Complaint Filed/ Remanded	APD Non-ADR Settlements from Date Complaint Filed/ Remanded	APD ADR Settlements from Date Complaint Filed/ Remanded	APD All Final Agency Actions from Date Complaint Filed/ Remanded
Department of State	413.4	172.85	172.85	0	541.07	761.53	17.5	408.83
Department of the Air Force	482.59	307.04	307.04	0	352.2	421.78	223.3	604.14
Department of the Army	324.63	192.76	198.91	96.33	302.93	343.92	171.23	368.19
Department of the Interior	487.03	227.13	227.13	0	410.41	434.86	173.3	567.11
Department of the Navy	332.14	130.65	130.65	0	347.73	350.1	99.75	396.31
Department of the Treasury	468.29	210.59	214.27	89	477.61	553.39	98.75	496.69
Department of Transportation	411.26	276.31	276.31	0	536.8	536.28	584	367.94
Department of Veterans Affairs	393.83	187.02	187.61	144	419.4	425.8	359.32	417.78
Election Assistance Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Environmental Protection Agency	712.04	448.64	448.64	0	689.75	689.75	0	833.77
Equal Employment Opportunity Commission	329.05	139	139	0	197.33	280.75	30.5	404.46
Export-Import Bank of the US	330	0	0	0	0	0	0	330
Farm Credit Administration	0	0	0	0	0	0	0	0
Farm Credit System Insurance Corporation	0	0	0	0	0	0	0	0
Federal Communications Commission	90	0	0	0	0	0	0	90
Federal Deposit Insurance Corporation	291.31	125.5	125.5	0	276.57	422.2	195.67	312
Federal Election Commission	0	0	0	0	0	0	0	0
Federal Energy Regulatory Commission	152.3	180	180	0	23	0	23	165
Federal Financial Institutions Examination Council	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Housing Finance Agency	199.83	0	0	0	205.8	250.67	138.5	170
Federal Labor Relations Authority	0	0	0	0	0	0	0	0
Federal Maritime Commission	0	0	0	0	0	0	0	0
Federal Mediation and Conciliation Service	15	15	15	0	0	0	0	0
Federal Mine Safety & Health Review Commission	0	0	0	0	0	0	0	0
Federal Reserve System--Board of Governors	310.17	180	180	0	264.5	264.5	0	792
Federal Retirement Thrift Investment Board	NRF	NRF	NRF	NRF	NRF	NRF	0	0
Federal Trade Commission	1,115.00	0	0	0	0	0	0	1,115.00
General Services Administration	425.05	152.5	152.5	0	469.39	469.39	0	470
Government Printing Office	329.86	330	330	0	312.4	312.4	0	339.56
Harry S. Truman Scholarship Foundation	0	0	0	0	0	0	0	0

Table B-12 FY 2012 Average Processing Days (APD) All Complaint Closures

Agency or Department	APD All Complaint Closures from Date Complaint Filed/ Remanded	APD All Withdrawals from Date Complaint Filed/ Remanded	APD Non-ADR Withdrawals from Date Complaint Filed/ Remanded	APD ADR Withdrawals from Date Complaint Filed/ Remanded	APD All Settlements from Date Complaint Filed/ Remanded	APD Non-ADR Settlements from Date Complaint Filed/ Remanded	APD ADR Settlements from Date Complaint Filed/ Remanded	APD All Final Agency Actions from Date Complaint Filed/ Remanded
Holocaust Memorial Museum U.S.	0	0	0	0	0	0	0	0
Institute of Museum and Library Services	0	0	0	0	0	0	0	0
Inter-American Foundation	0	0	0	0	0	0	0	0
International Boundary and Water Commission	0	0	0	0	0	0	0	0
International Joint Commission: US and Canada	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
International Trade Commission	195	0	0	0	195	195	0	0
James Madison Memorial Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Japan-United States Friendship Commission	0	0	0	0	0	0	0	0
John F. Kennedy Center for the Performing Arts	0	0	0	0	0	0	0	0
Marine Mammal Commission	0	0	0	0	0	0	0	0
Merit Systems Protection Board	231	0	0	0	231	231	0	0
Millennium Challenge Corporation	0	0	0	0	0	0	0	0
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Aeronautics and Space Administration	565.26	197	197	0	367	367	0	623.8
National Archives and Records Administration	685.27	0	0	0	672.67	672.67	0	690
National Capital Planning Commission	0	0	0	0	0	0	0	0
National Council on Disability	0	0	0	0	0	0	0	0
National Credit Union Administration	424.57	0	0	0	405.17	405.17	0	541
National Endowment for the Arts	324.33	0	0	0	448	448	0	77
National Endowment for the Humanities	0	0	0	0	0	0	0	0
National Foundation on the Arts & the Humanities	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Gallery of Art	817.33	0	0	0	1,300.50	1,300.50	0	575.75
National Indian Gaming Commission	304	304	304	0	0	0	0	0
National Labor Relations Board	288.88	35	0	35	410.33	410.33	0	261.25
National Mediation Board	0	0	0	0	0	0	0	0
National Reconnaissance Office	542.14	0	0	0	790	0	790	500.83
National Science Foundation	364	0	0	0	364	373.25	345.5	0
National Transportation Safety Board	176	76	76	0	0	0	0	276
Navajo and Hopi Indian Relocation Commission	0	0	0	0	0	0	0	0

Table B-12 FY 2012 Average Processing Days (APD) All Complaint Closures

Agency or Department	APD All Complaint Closures from Date Complaint Filed/ Remanded	APD All Withdrawals from Date Complaint Filed/ Remanded	APD Non-ADR Withdrawals from Date Complaint Filed/ Remanded	APD ADR Withdrawals from Date Complaint Filed/ Remanded	APD All Settlements from Date Complaint Filed/ Remanded	APD Non-ADR Settlements from Date Complaint Filed/ Remanded	APD ADR Settlements from Date Complaint Filed/ Remanded	APD All Final Agency Actions from Date Complaint Filed/ Remanded
Nuclear Regulatory Commission	298.19	317.25	317.25	0	260.91	275.1	119	632
Nuclear Waste Technical Review Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Occupational Safety & Health Review Commission	0	0	0	0	0	0	0	0
Office of Government Ethics	15	0	0	0	0	0	0	15
Office of Personnel Management	504.64	468.17	468.17	0	278	278	0	551.95
Office of Special Counsel	0	0	0	0	0	0	0	0
Office of the Director of National Intelligence	474	0	0	0	735	735	0	213
Overseas Private Investment Corporation	0	0	0	0	0	0	0	0
Peace Corps	508.75	0	0	0	0	0	0	508.75
Pension Benefit Guaranty Corporation	437.2	205.5	205.5	0	755	755	0	445.76
Postal Regulatory Commission	0	0	0	0	0	0	0	0
Presidio Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Railroad Retirement Board	660	0	0	0	660	660	0	0
Securities and Exchange Commission	308.25	0	0	0	0	0	0	308.25
Selective Service System	288	0	0	0	288	288	0	0
Small Business Administration	313.29	208	208	0	563.18	563.18	0	211.62
Smithsonian Institution	500.27	0	0	0	1,432.33	1,432.33	0	267.25
Social Security Administration	506.13	398.33	398.33	0	491.18	509.48	52	527.31
Tennessee Valley Authority	330.36	126	126	0	485.17	485.17	0	319.41
Trade and Development Agency	0	0	0	0	0	0	0	0
U.S. Postal Service	275.45	215.19	219.77	36.5	349.36	447.23	40.26	262.46

Table B-12 FY 2012 Average Processing Days (APD) All Complaint Closures								
Agency or Department	**APD All Complaint Closures from Date Complaint Filed/ Remanded**	**APD All Withdrawals from Date Complaint Filed/ Remanded**	**APD Non-ADR Withdrawals from Date Complaint Filed/ Remanded**	**APD ADR Withdrawals from Date Complaint Filed/ Remanded**	**APD All Settlements from Date Complaint Filed/ Remanded**	**APD Non-ADR Settlements from Date Complaint Filed/ Remanded**	**APD ADR Settlements from Date Complaint Filed/ Remanded**	**APD All Final Agency Actions from Date Complaint Filed/ Remanded**
Utah Reclamation Mitigation and Conservation Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Valles Caldera Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Cabinet Level Subtotal	382.46	223.35	226.47	88.54	405.26	444.48	221.84	393.89
Midsize Agencies Subtotal	475.76	346.47	346.47	0	488.32	517.07	169.55	495.2
Small Agencies Subtotal	424.89	221.78	230.27	35	430.02	453.02	217.89	450.97
Micro Agencies Subtotal	513	0	0	0	800.5	800.5	0	321.33
Government-wide	387.84	231.94	235.12	86.69	408.72	447.52	220.97	400.15

NRF = No Report Filed

Table B-13 FY 2012 Complaints Closed with Dismissals

Agency or Department	Total Complaint Closures	Number All Dismissals	Number Final Agency Decision (FAD) Dismissals (no AJ)	% FAD Dismissals	Number Final Orders (FOs) of AJ Dismissals	% FOs of AJ Dismissals	Number FOs Fully Implementing (FI) AJ Dismissals	% FOs FI AJ Dismissals	Number FOs Not Fully Implementing (NFI) AJ Dismissals	% FOs NFI AJ Dismissals
Advisory Council on Historic Preservation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
African Development Foundation	3	1	0	0.00%	1	100.00%	1	100.00%	0	0.00%
Agency for International Development	16	7	7	100.00%	0	0.00%	0	0.00%	0	0.00%
American Battle Monuments Commission	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Appalachian Regional Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Architectural and Transportation Barriers Compliance Board	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Arctic Research Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Armed Forces Retirement Home	4	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Barry Goldwater Scholarship and Excellence in Education Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Broadcasting Board of Governors	14	5	5	100.00%	0	0.00%	0	0.00%	0	0.00%
Central Intelligence Agency	39	10	9	90.00%	1	10.00%	1	100.00%	0	0.00%
Chemical Safety and Hazard Investigation Board	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Christopher Columbus Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission of Fine Arts	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission on Civil Rights	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Committee for Purchase from People Who Are Blind or Severely Disabled	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Commodity Futures Trading Commission	2	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Consumer Financial Protection Bureau	7	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Consumer Product Safety Commission	2	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Corporation for National and Community Service	3	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Court Services and Offender Supervision Agency for the District of Columbia	15	2	2	100.00%	0	0.00%	0	0.00%	0	0.00%
Defense Army and Air Force Exchange	89	20	20	100.00%	0	0.00%	0	0.00%	0	0.00%
Defense Commissary Agency	120	22	22	100.00%	0	0.00%	0	0.00%	0	0.00%
Defense Contract Audit Agency	32	4	4	100.00%	0	0.00%	0	0.00%	0	0.00%
Defense Contract Management Agency	38	16	16	100.00%	0	0.00%	0	0.00%	0	0.00%
Defense Finance and Accounting Service	39	9	9	100.00%	0	0.00%	0	0.00%	0	0.00%
Defense Human Resources Activity	5	1	1	100.00%	0	0.00%	0	0.00%	0	0.00%
Defense Information Systems Agency	8	5	5	100.00%	0	0.00%	0	0.00%	0	0.00%
Defense Intelligence Agency	34	11	11	100.00%	0	0.00%	0	0.00%	0	0.00%
Defense Joint Task Force National Capital Region Medical	7	5	5	100.00%	0	0.00%	0	0.00%	0	0.00%
Defense Logistics Agency	136	14	14	100.00%	0	0.00%	0	0.00%	0	0.00%

Table B-13 FY 2012 Complaints Closed with Dismissals

Agency or Department	Total Complaint Closures	Number All Dismissals	Number Final Agency Decision (FAD) Dismissals (no AJ)	% FAD Dismissals	Number Final Orders (FOs) of AJ Dismissals	% FOs of AJ Dismissals	Number FOs Fully Implementing (FI) AJ Dismissals	% FOs FI AJ Dismissals	Number FOs Not Fully Implementing (NFI) AJ Dismissals	% FOs NFI AJ Dismissals
Defense Media Activity	3	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Defense Missile Defense Agency	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Defense National Geospatial-Intelligence Agency	20	5	5	100.00%	0	0.00%	0	0.00%	0	0.00%
Defense National Guard Bureau	33	23	23	100.00%	0	0.00%	0	0.00%	0	0.00%
Defense National Security Agency	17	4	3	75.00%	1	25.00%	1	100.00%	0	0.00%
Defense Nuclear Facilities Safety Board	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Defense Office of the Inspector General	3	1	1	100.00%	0	0.00%	0	0.00%	0	0.00%
Defense Office of the Secretary - Wash. Hqtrs. Services	45	13	13	100.00%	0	0.00%	0	0.00%	0	0.00%
Defense Security Service	6	2	2	100.00%	0	0.00%	0	0.00%	0	0.00%
Defense Technical Information Center	1	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Defense Threat Reduction Agency	8	4	4	100.00%	0	0.00%	0	0.00%	0	0.00%
Defense TRICARE Management Activity	7	5	5	100.00%	0	0.00%	0	0.00%	0	0.00%
Defense Uniformed Services University	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Department of Agriculture	453	48	48	100.00%	0	0.00%	0	0.00%	0	0.00%
Department of Commerce	432	57	49	85.96%	8	14.04%	8	100.00%	0	0.00%
Department of Defense Education Activity	55	10	10	100.00%	0	0.00%	0	0.00%	0	0.00%
Department of Education	46	2	2	100.00%	0	0.00%	0	0.00%	0	0.00%
Department of Energy	63	6	6	100.00%	0	0.00%	0	0.00%	0	0.00%
Department of Health and Human Services	409	95	94	98.95%	1	1.05%	1	100.00%	0	0.00%
Department of Homeland Security	1,097	180	164	91.11%	16	8.89%	16	100.00%	0	0.00%
Department of Housing and Urban Development	73	3	3	100.00%	0	0.00%	0	0.00%	0	0.00%
Department of Justice	857	110	110	100.00%	0	0.00%	0	0.00%	0	0.00%
Department of Labor	134	19	11	57.89%	8	42.11%	8	100.00%	0	0.00%
Department of State	110	16	16	100.00%	0	0.00%	0	0.00%	0	0.00%
Department of the Air Force	500	76	67	88.16%	9	11.84%	9	100.00%	0	0.00%
Department of the Army	1,116	237	234	98.73%	3	1.27%	3	100.00%	0	0.00%
Department of the Interior	307	31	30	96.77%	1	3.23%	1	100.00%	0	0.00%
Department of the Navy	904	147	147	100.00%	0	0.00%	0	0.00%	0	0.00%
Department of the Treasury	407	51	44	86.27%	7	13.73%	7	100.00%	0	0.00%
Department of Transportation	335	87	85	97.70%	2	2.30%	2	100.00%	0	0.00%
Department of Veterans Affairs	2,123	406	392	96.55%	14	3.45%	14	100.00%	0	0.00%
Election Assistance Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Environmental Protection Agency	49	3	2	66.67%	1	33.33%	1	100.00%	0	0.00%
Equal Employment Opportunity Commission	20	5	5	100.00%	0	0.00%	0	0.00%	0	0.00%
Export-Import Bank of the US	1	1	1	100.00%	0	0.00%	0	0.00%	0	0.00%

Table B-13 FY 2012 Complaints Closed with Dismissals

Agency or Department	Total Complaint Closures	Number All Dismissals	Number Final Agency Decision (FAD) Dismissals (no AJ)	% FAD Dismissals	Number Final Orders (FOs) of AJ Dismissals	% FOs of AJ Dismissals	Number FOs Fully Implementing (FI) AJ Dismissals	% FOs FI AJ Dismissals	Number FOs Not Fully Implementing (NFI) AJ Dismissals	% FOs NFI AJ Dismissals
Farm Credit Administration	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Farm Credit System Insurance Corporation	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Federal Communications Commission	2	2	2	100.00%	0	0.00%	0	0.00%	0	0.00%
Federal Deposit Insurance Corporation	42	12	11	91.67%	1	8.33%	1	100.00%	0	0.00%
Federal Election Commission	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Federal Energy Regulatory Commission	10	2	2	100.00%	0	0.00%	0	0.00%	0	0.00%
Federal Financial Institutions Examination Council	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Housing Finance Agency	6	1	1	100.00%	0	0.00%	0	0.00%	0	0.00%
Federal Labor Relations Authority	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Federal Maritime Commission	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Federal Mediation and Conciliation Service	2	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Federal Mine Safety & Health Review Commission	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Federal Reserve System--Board of Governors	6	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Federal Retirement Thrift Investment Board	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Trade Commission	1	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
General Services Administration	85	11	11	100.00%	0	0.00%	0	0.00%	0	0.00%
Government Printing Office	29	5	5	100.00%	0	0.00%	0	0.00%	0	0.00%
Harry S. Truman Scholarship Foundation	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Holocaust Memorial Museum U.S.	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Institute of Museum and Library Services	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Inter-American Foundation	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
International Boundary and Water Commission	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
International Joint Commission: US and Canada	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
International Trade Commission	1	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
James Madison Memorial Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Japan-United States Friendship Commission	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
John F. Kennedy Center for the Performing Arts	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Marine Mammal Commission	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Merit Systems Protection Board	1	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Millennium Challenge Corporation	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Aeronautics and Space Administration	38	9	9	100.00%	0	0.00%	0	0.00%	0	0.00%
National Archives and Records Administration	11	2	2	100.00%	0	0.00%	0	0.00%	0	0.00%
National Capital Planning Commission	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
National Council on Disability	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%

Table B-13 FY 2012 Complaints Closed with Dismissals

Agency or Department	Total Complaint Closures	Number All Dismissals	Number Final Agency Decision (FAD) Dismissals (no AJ)	% FAD Dismissals	Number Final Orders (FOs) of AJ Dismissals	% FOs of AJ Dismissals	Number FOs Fully Implementing (FI) AJ Dismissals	% FOs FI AJ Dismissals	Number FOs Not Fully Implementing (NFI) AJ Dismissals	% FOs NFI AJ Dismissals
National Credit Union Administration	7	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
National Endowment for the Arts	3	1	1	100.00%	0	0.00%	0	0.00%	0	0.00%
National Endowment for the Humanities	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
National Foundation on the Arts & the Humanities	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Gallery of Art	6	1	1	100.00%	0	0.00%	0	0.00%	0	0.00%
National Indian Gaming Commission	1	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
National Labor Relations Board	8	1	1	100.00%	0	0.00%	0	0.00%	0	0.00%
National Mediation Board	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
National Reconnaissance Office	7	2	2	100.00%	0	0.00%	0	0.00%	0	0.00%
National Science Foundation	6	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
National Transportation Safety Board	2	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Navajo and Hopi Indian Relocation Commission	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Nuclear Regulatory Commission	16	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Nuclear Waste Technical Review Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Occupational Safety & Health Review Commission	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Office of Government Ethics	2	2	2	100.00%	0	0.00%	0	0.00%	0	0.00%
Office of Personnel Management	28	6	6	100.00%	0	0.00%	0	0.00%	0	0.00%
Office of Special Counsel	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Office of the Director of National Intelligence	4	1	1	100.00%	0	0.00%	0	0.00%	0	0.00%
Overseas Private Investment Corporation	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Peace Corps	4	1	0	0.00%	1	100.00%	1	100.00%	0	0.00%
Pension Benefit Guaranty Corporation	20	6	6	100.00%	0	0.00%	0	0.00%	0	0.00%
Postal Regulatory Commission	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Presidio Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Railroad Retirement Board	1	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Securities and Exchange Commission	4	2	1	50.00%	1	50.00%	1	100.00%	0	0.00%
Selective Service System	2	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Small Business Administration	38	14	14	100.00%	0	0.00%	0	0.00%	0	0.00%
Smithsonian Institution	15	4	4	100.00%	0	0.00%	0	0.00%	0	0.00%
Social Security Administration	414	58	49	84.48%	9	15.52%	9	100.00%	0	0.00%
Tennessee Valley Authority	58	5	5	100.00%	0	0.00%	0	0.00%	0	0.00%
Trade and Development Agency	0	0	0	0.00%	0	0.00%	0	0.00%	0	0.00%
U.S. Postal Service	4,579	1,588	1,570	98.87%	18	1.13%	18	100.00%	0	0.00%

Table B-13 FY 2012 Complaints Closed with Dismissals

Agency or Department	Total Complaint Closures	Number All Dismissals	Number Final Agency Decision (FAD) Dismissals (no AJ)	% FAD Dismissals	Number Final Orders (FOs) of AJ Dismissals	% FOs of AJ Dismissals	Number FOs Fully Implementing (FI) AJ Dismissals	% FOs FI AJ Dismissals	Number FOs Not Fully Implementing (NFI) AJ Dismissals	% FOs NFI AJ Dismissals
Utah Reclamation Mitigation and Conservation Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Valles Caldera Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Cabinet Level Subtotal	14,651	3,333	3,245	97.36%	88	2.64%	88	100.00%	0	0.00%
Midsize Agencies Subtotal	774	122	111	90.98%	11	9.02%	11	100.00%	0	0.00%
Small Agencies Subtotal	276	57	54	94.74%	3	5.26%	3	100.00%	0	0.00%
Micro Agencies Subtotal	5	3	2	66.67%	1	33.33%	1	100.00%	0	0.00%
Government-wide	15,706	3,515	3,412	97.07%	103	2.93%	103	100.00%	0	0.00%

NRF = No Report Filed

Table B-14 FY 2012 Timeliness of Merit Final Agency Decisions (FAD) (No AJ Decision)

Agency or Department	Total Number Agency Merit Decisions (No AJ Decision)	APD from Date Complaint Filed/Remanded	APD From Date FAD Required	Number Timely Completed Where FAD Requested	Number Timely Completed Where No Election Made	Number Timely Completed Where AJ Ordered FAD	Number Timely Completed Where Mixed Case	Total Number Timely Agency Merit Decisions (No AJ Decision)	% Timely Agency Merit Decisions (No AJ Decision)
Advisory Council on Historic Preservation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
African Development Foundation	0	0	0	0	0	0	0	0	0.00%
Agency for International Development	1	830	62	0	0	0	0	0	0.00%
American Battle Monuments Commission	0	0	0	0	0	0	0	0	0.00%
Appalachian Regional Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Architectural and Transportation Barriers Compliance Board	0	0	0	0	0	0	0	0	0.00%
Arctic Research Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Armed Forces Retirement Home	4	243.5	48.25	0	4	0	0	4	100.00%
Barry Goldwater Scholarship and Excellence in Education Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Broadcasting Board of Governors	2	326	51	0	1	1	0	2	100.00%
Central Intelligence Agency	6	590.33	59.67	1	1	2	0	4	66.67%
Chemical Safety and Hazard Investigation Board	0	0	0	0	0	0	0	0	0.00%
Christopher Columbus Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission of Fine Arts	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission on Civil Rights	0	0	0	0	0	0	0	0	0.00%
Committee for Purchase from People Who Are Blind or Severely Disabled	0	0	0	0	0	0	0	0	0.00%
Commodity Futures Trading Commission	2	314	68.5	1	0	0	0	1	50.00%
Consumer Financial Protection Bureau	3	301	57	3	0	0	0	3	100.00%
Consumer Product Safety Commission	1	416	25	0	0	1	0	1	100.00%
Corporation for National and Community Service	3	431.67	169.33	0	0	0	0	0	0.00%
Court Services and Offender Supervision Agency for the District of Columbia	2	393	46	2	0	0	0	2	100.00%
Defense Army and Air Force Exchange	14	346.29	59.07	7	5	1	0	13	92.86%
Defense Commissary Agency	27	349.44	29.81	3	18	5	0	26	96.30%
Defense Contract Audit Agency	7	357.57	67.71	5	0	0	0	5	71.43%
Defense Contract Management Agency	8	496.63	21.88	6	1	1	0	8	100.00%
Defense Finance and Accounting Service	8	309.25	37.75	1	6	1	0	8	100.00%
Defense Human Resources Activity	0	0	0	0	0	0	0	0	0.00%
Defense Information Systems Agency	0	0	0	0	0	0	0	0	0.00%
Defense Intelligence Agency	7	681.29	239.57	1	0	0	0	1	14.29%
Defense Joint Task Force National Capital Region Medical	0	0	0	0	0	0	0	0	0.00%
Defense Logistics Agency	38	493.92	195.84	0	3	0	0	3	7.89%
Defense Media Activity	0	0	0	0	0	0	0	0	0.00%

Table B-14 FY 2012 Timeliness of Merit Final Agency Decisions (FAD) (No AJ Decision)

Agency or Department	Total Number Agency Merit Decisions (No AJ Decision)	APD from Date Complaint Filed/Remanded	APD From Date FAD Required	Number Timely Completed Where FAD Requested	Number Timely Completed Where No Election Made	Number Timely Completed Where AJ Ordered FAD	Number Timely Completed Where Mixed Case	Total Number Timely Agency Merit Decisions (No AJ Decision)	% Timely Agency Merit Decisions (No AJ Decision)
Defense Missile Defense Agency	0	0	0	0	0	0	0	0	0.00%
Defense National Geospatial-Intelligence Agency	4	666.75	42.25	1	0	3	0	4	100.00%
Defense National Guard Bureau	3	361.67	321.67	0	0	0	0	0	0.00%
Defense National Security Agency	5	376.4	60	3	2	0	0	5	100.00%
Defense Nuclear Facilities Safety Board	0	0	0	0	0	0	0	0	0.00%
Defense Office of the Inspector General	0	0	0	0	0	0	0	0	0.00%
Defense Office of the Secretary - Wash. Hqtrs. Services	6	663.5	157.5	0	0	0	0	0	0.00%
Defense Security Service	3	200	57.67	1	2	0	0	3	100.00%
Defense Technical Information Center	0	0	0	0	0	0	0	0	0.00%
Defense Threat Reduction Agency	0	0	0	0	0	0	0	0	0.00%
Defense TRICARE Management Activity	0	0	0	0	0	0	0	0	0.00%
Defense Uniformed Services University	0	0	0	0	0	0	0	0	0.00%
Department of Agriculture	151	638.32	244.41	22	16	4	0	42	27.81%
Department of Commerce	189	569.24	242.79	4	4	18	0	26	13.76%
Department of Defense Education Activity	12	385.67	58.33	3	4	0	0	7	58.33%
Department of Education	17	358.24	36.12	7	1	9	0	17	100.00%
Department of Energy	18	371.67	91.72	2	0	3	0	5	27.78%
Department of Health and Human Services	96	404.14	63.85	20	13	17	4	54	56.25%
Department of Homeland Security	337	493.66	142.91	64	37	58	4	163	48.37%
Department of Housing and Urban Development	25	624.24	190.32	2	0	0	0	2	8.00%
Department of Justice	362	775.83	382.55	7	13	7	1	28	7.73%
Department of Labor	44	357.14	59.48	9	15	9	5	38	86.36%
Department of State	40	460.58	167.78	0	0	1	0	1	2.50%
Department of the Air Force	96	839.44	455.29	5	5	2	0	12	12.50%
Department of the Army	181	528.11	108.17	4	4	5	8	21	11.60%
Department of the Interior	104	574.44	173.24	5	7	0	0	12	11.54%
Department of the Navy	117	477.23	53.45	52	44	17	4	117	100.00%
Department of the Treasury	123	355.41	41.02	20	52	26	10	108	87.80%
Department of Transportation	89	413.53	75.36	7	21	19	0	47	52.81%
Department of Veterans Affairs	597	464.04	177.88	9	6	7	8	30	5.03%
Election Assistance Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Environmental Protection Agency	13	899.31	476.77	0	0	0	0	0	0.00%
Equal Employment Opportunity Commission	5	529.8	155.4	0	0	0	0	0	0.00%
Export-Import Bank of the US	0	0	0	0	0	0	0	0	0.00%
Farm Credit Administration	0	0	0	0	0	0	0	0	0.00%
Farm Credit System Insurance Corporation	0	0	0	0	0	0	0	0	0.00%

Table B-14 FY 2012 Timeliness of Merit Final Agency Decisions (FAD) (No AJ Decision)

Agency or Department	Total Number Agency Merit Decisions (No AJ Decision)	APD from Date Complaint Filed/Remanded	APD From Date FAD Required	Number Timely Completed Where FAD Requested	Number Timely Completed Where No Election Made	Number Timely Completed Where AJ Ordered FAD	Number Timely Completed Where Mixed Case	Total Number Timely Agency Merit Decisions (No AJ Decision)	% Timely Agency Merit Decisions (No AJ Decision)
Federal Communications Commission	0	0	0	0	0	0	0	0	0.00%
Federal Deposit Insurance Corporation	12	407.42	49.83	2	5	5	0	12	100.00%
Federal Election Commission	0	0	0	0	0	0	0	0	0.00%
Federal Energy Regulatory Commission	6	200	60	0	6	0	0	6	100.00%
Federal Financial Institutions Examination Council	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Housing Finance Agency	0	0	0	0	0	0	0	0	0.00%
Federal Labor Relations Authority	0	0	0	0	0	0	0	0	0.00%
Federal Maritime Commission	0	0	0	0	0	0	0	0	0.00%
Federal Mediation and Conciliation Service	0	0	0	0	0	0	0	0	0.00%
Federal Mine Safety & Health Review Commission	0	0	0	0	0	0	0	0	0.00%
Federal Reserve System--Board of Governors	0	0	0	0	0	0	0	0	0.00%
Federal Retirement Thrift Investment Board	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Trade Commission	0	0	0	0	0	0	0	0	0.00%
General Services Administration	21	397.57	59.19	8	4	2	1	15	71.43%
Government Printing Office	11	358.45	158.55	0	3	0	0	3	27.27%
Harry S. Truman Scholarship Foundation	0	0	0	0	0	0	0	0	0.00%
Holocaust Memorial Museum U.S.	0	0	0	0	0	0	0	0	0.00%
Institute of Museum and Library Services	0	0	0	0	0	0	0	0	0.00%
Inter-American Foundation	0	0	0	0	0	0	0	0	0.00%
International Boundary and Water Commission	0	0	0	0	0	0	0	0	0.00%
International Joint Commission: US and Canada	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
International Trade Commission	0	0	0	0	0	0	0	0	0.00%
James Madison Memorial Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Japan-United States Friendship Commission	0	0	0	0	0	0	0	0	0.00%
John F. Kennedy Center for the Performing Arts	0	0	0	0	0	0	0	0	0.00%
Marine Mammal Commission	0	0	0	0	0	0	0	0	0.00%
Merit Systems Protection Board	0	0	0	0	0	0	0	0	0.00%
Millennium Challenge Corporation	0	0	0	0	0	0	0	0	0.00%
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Aeronautics and Space Administration	11	516.36	181	0	0	0	0	0	0.00%
National Archives and Records Administration	3	636	58.33	1	0	2	0	3	100.00%
National Capital Planning Commission	0	0	0	0	0	0	0	0	0.00%
National Council on Disability	0	0	0	0	0	0	0	0	0.00%
National Credit Union Administration	1	541	75	0	0	0	0	0	0.00%
National Endowment for the Arts	0	0	0	0	0	0	0	0	0.00%
National Endowment for the Humanities	0	0	0	0	0	0	0	0	0.00%

Table B-14 FY 2012 Timeliness of Merit Final Agency Decisions (FAD) (No AJ Decision)

Agency or Department	Total Number Agency Merit Decisions (No AJ Decision)	APD from Date Complaint Filed/Remanded	APD From Date FAD Required	Number Timely Completed Where FAD Requested	Number Timely Completed Where No Election Made	Number Timely Completed Where AJ Ordered FAD	Number Timely Completed Where Mixed Case	Total Number Timely Agency Merit Decisions (No AJ Decision)	% Timely Agency Merit Decisions (No AJ Decision)
National Foundation on the Arts and the Humanities	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Gallery of Art	3	760.67	89.33	0	0	0	0	0	0.00%
National Indian Gaming Commission	0	0	0	0	0	0	0	0	0.00%
National Labor Relations Board	2	234.5	55.5	2	0	0	0	2	100.00%
National Mediation Board	0	0	0	0	0	0	0	0	0.00%
National Reconnaissance Office	2	333.5	84.5	1	0	0	0	1	50.00%
National Science Foundation	0	0	0	0	0	0	0	0	0.00%
National Transportation Safety Board	1	276	40	1	0	0	0	1	100.00%
Navajo and Hopi Indian Relocation Commission	0	0	0	0	0	0	0	0	0.00%
Nuclear Regulatory Commission	0	0	0	0	0	0	0	0	0.00%
Nuclear Waste Technical Review Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Occupational Safety & Health Review Commission	0	0	0	0	0	0	0	0	0.00%
Office of Government Ethics	0	0	0	0	0	0	0	0	0.00%
Office of Personnel Management	8	1,128.25	353.88	0	0	0	0	0	0.00%
Office of Special Counsel	0	0	0	0	0	0	0	0	0.00%
Office of the Director of National Intelligence	1	269	27	0	1	0	0	1	100.00%
Overseas Private Investment Corporation	0	0	0	0	0	0	0	0	0.00%
Peace Corps	3	367	130	1	0	0	0	1	33.33%
Pension Benefit Guaranty Corporation	5	361.8	40.4	4	0	1	0	5	100.00%
Postal Regulatory Commission	0	0	0	0	0	0	0	0	0.00%
Presidio Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Railroad Retirement Board	0	0	0	0	0	0	0	0	0.00%
Securities and Exchange Commission	2	334.5	66.5	1	0	0	0	1	50.00%
Selective Service System	0	0	0	0	0	0	0	0	0.00%
Small Business Administration	7	329	25.14	0	2	3	1	6	85.71%
Smithsonian Institution	5	213.2	41.4	2	1	0	2	5	100.00%
Social Security Administration	136	459.63	175.1	5	26	2	3	36	26.47%
Tennessee Valley Authority	20	236.25	56.2	13	5	2	0	20	100.00%
Trade and Development Agency	0	0	0	0	0	0	0	0	0.00%
U.S. Postal Service	1,088	277.48	32.41	123	515	315	109	1,062	97.61%

Table B-14 FY 2012 Timeliness of Merit Final Agency Decisions (FAD) (No AJ Decision)

Agency or Department	Total Number Agency Merit Decisions (No AJ Decision)	APD from Date Complaint Filed/Remanded	APD From Date FAD Required	Number Timely Completed Where FAD Requested	Number Timely Completed Where No Election Made	Number Timely Completed Where AJ Ordered FAD	Number Timely Completed Where Mixed Case	Total Number Timely Agency Merit Decisions (No AJ Decision)	% Timely Agency Merit Decisions (No AJ Decision)
Utah Reclamation Mitigation and Conservation Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Valles Caldera Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Cabinet Level Subtotal	3,816	462.61	143.51	393	794	528	153	1,868	48.95%
Midsize Agencies Subtotal	236	470.94	162.51	33	43	14	7	97	41.10%
Small Agencies Subtotal	66	407.67	90.12	15	16	7	0	38	57.58%
Micro Agencies Subtotal	0	0	0	0	0	0	0	0	0.00%
Government-wide	4,118	462.21	143.74	441	853	549	160	2,003	48.64%

NRF = No Report Filed

Table B-14a FY 2012 Timeliness of Merit Final Agency Decisions (FAD) (No AJ Decision) - Sub-Component Data									
Agency or Department	Total Number Agency Merit Decisions (No AJ Decision)	APD from Date Complaint Filed/Remanded	APD From Date FAD Required	Number Timely Completed Where FAD Requested	Number Timely Completed Where No Election Made	Number Timely Completed Where AJ Ordered FAD	Number Timely Completed Where Mixed Case	Total Number Timely Agency Merit Decisions (No AJ Decision)	% Timely Agency Merit Decisions (No AJ Decision)
Defense Logistics Agency Wide	**38**	**493.92**	**195.84**	**0**	**3**	**0**	**0**	**3**	**7.89%**
DLA Aviation	7	452.71	160.86	0	1	0	0	1	14.29%
DLA Disposition Services	6	576.17	214.33	0	1	0	0	1	16.67%
DLA Distribution	14	549.14	249.86	0	1	0	0	1	7.14%
DLA Headquarters Operations Division	1	419	163	0	0	0	0	0	0.00%
DLA Land and Maritime	3	432.67	156.33	0	0	0	0	0	0.00%
DLA Logistics Information Service	4	454.25	156.25	0	0	0	0	0	0.00%
DLA Troop Support	3	307	91.67	0	0	0	0	0	0.00%
Defense National Guard Bureau Wide	**3**	**361.67**	**321.67**	**0**	**0**	**0**	**0**	**0**	**0.00%**
Alabama National Guard	0	0	0	0	0	0	0	0	0.00%
Alaska National Guard	0	0	0	0	0	0	0	0	0.00%
Arizona National Guard	0	0	0	0	0	0	0	0	0.00%
Arkansas National Guard	0	0	0	0	0	0	0	0	0.00%
California National Guard	0	0	0	0	0	0	0	0	0.00%
Colorado National Guard	0	0	0	0	0	0	0	0	0.00%
Connecticut National Guard	0	0	0	0	0	0	0	0	0.00%
DC National Guard	0	0	0	0	0	0	0	0	0.00%
Delaware National Guard	0	0	0	0	0	0	0	0	0.00%
Florida National Guard	0	0	0	0	0	0	0	0	0.00%
Georgia National Guard	0	0	0	0	0	0	0	0	0.00%
Guam National Guard	0	0	0	0	0	0	0	0	0.00%
Hawaii National Guard	0	0	0	0	0	0	0	0	0.00%
Idaho National Guard	0	0	0	0	0	0	0	0	0.00%
Illinois National Guard	0	0	0	0	0	0	0	0	0.00%
Indiana National Guard	0	0	0	0	0	0	0	0	0.00%
Iowa National Guard	0	0	0	0	0	0	0	0	0.00%
Kansas National Guard	0	0	0	0	0	0	0	0	0.00%
Kentucky National Guard	0	0	0	0	0	0	0	0	0.00%
Louisiana National Guard	0	0	0	0	0	0	0	0	0.00%
Maine National Guard	0	0	0	0	0	0	0	0	0.00%
Maryland National Guard	0	0	0	0	0	0	0	0	0.00%
Massachusetts National Guard	0	0	0	0	0	0	0	0	0.00%

Table B-14a FY 2012 Timeliness of Merit Final Agency Decisions (FAD) (No AJ Decision) - Sub-Component Data									
Agency or Department	Total Number Agency Merit Decisions (No AJ Decision)	APD from Date Complaint Filed/Remanded	APD From Date FAD Required	Number Timely Completed Where FAD Requested	Number Timely Completed Where No Election Made	Number Timely Completed Where AJ Ordered FAD	Number Timely Completed Where Mixed Case	Total Number Timely Agency Merit Decisions (No AJ Decision)	% Timely Agency Merit Decisions (No AJ Decision)
Michigan National Guard	0	0	0	0	0	0	0	0	0.00%
Minnesota National Guard	0	0	0	0	0	0	0	0	0.00%
Mississippi National Guard	0	0	0	0	0	0	0	0	0.00%
Missouri National Guard	0	0	0	0	0	0	0	0	0.00%
Montana National Guard	0	0	0	0	0	0	0	0	0.00%
Nebraska National Guard	0	0	0	0	0	0	0	0	0.00%
Nevada National Guard	0	0	0	0	0	0	0	0	0.00%
New Hampshire National Guard	0	0	0	0	0	0	0	0	0.00%
New Jersey National Guard	0	0	0	0	0	0	0	0	0.00%
New Mexico National Guard	0	0	0	0	0	0	0	0	0.00%
New York National Guard	0	0	0	0	0	0	0	0	0.00%
North Carolina National Guard	0	0	0	0	0	0	0	0	0.00%
North Dakota National Guard	0	0	0	0	0	0	0	0	0.00%
Ohio National Guard	0	0	0	0	0	0	0	0	0.00%
Oklahoma National Guard	0	0	0	0	0	0	0	0	0.00%
Oregon National Guard	0	0	0	0	0	0	0	0	0.00%
Pennsylvania National Guard	0	0	0	0	0	0	0	0	0.00%
Puerto Rico National Guard	0	0	0	0	0	0	0	0	0.00%
Rhode Island National Guard	0	0	0	0	0	0	0	0	0.00%
South Carolina National Guard	0	0	0	0	0	0	0	0	0.00%
South Dakota National Guard	0	0	0	0	0	0	0	0	0.00%
Tennessee National Guard	3	361.67	321.67	0	0	0	0	0	0.00%
Texas National Guard	0	0	0	0	0	0	0	0	0.00%
Utah National Guard	0	0	0	0	0	0	0	0	0.00%
Vermont National Guard	0	0	0	0	0	0	0	0	0.00%
Virgin Islands National Guard	0	0	0	0	0	0	0	0	0.00%
Virginia National Guard	0	0	0	0	0	0	0	0	0.00%
Washington State National Guard	0	0	0	0	0	0	0	0	0.00%
West Virginia National Guard	0	0	0	0	0	0	0	0	0.00%
Wisconsin National Guard	0	0	0	0	0	0	0	0	0.00%
Wyoming National Guard	0	0	0	0	0	0	0	0	0.00%

Table B-14a FY 2012 Timeliness of Merit Final Agency Decisions (FAD) (No AJ Decision) - Sub-Component Data									
Agency or Department	Total Number Agency Merit Decisions (No AJ Decision)	APD from Date Complaint Filed/Remanded	APD From Date FAD Required	Number Timely Completed Where FAD Requested	Number Timely Completed Where No Election Made	Number Timely Completed Where AJ Ordered FAD	Number Timely Completed Where Mixed Case	Total Number Timely Agency Merit Decisions (No AJ Decision)	% Timely Agency Merit Decisions (No AJ Decision)
Department of Agriculture Wide	**151**	**638.32**	**244.41**	**22**	**16**	**4**	**0**	**42**	**27.81%**
USDA - Office Of Inspector General	2	1,188.50	269	0	0	0	0	0	0.00%
USDA Agricultural Marketing Service	5	298.2	115.6	0	0	0	0	0	0.00%
USDA Agricultural Research Service	9	486.33	337.56	0	0	0	0	0	0.00%
USDA Agriculture Headquarters	7	1,243.57	44	0	7	0	0	7	100.00%
USDA Animal and Plant Health Inspection Service	17	602.76	276.76	5	1	1	0	7	41.18%
USDA Economic Research Service	0	0	0	0	0	0	0	0	0.00%
USDA Farm Service Agency	9	931.33	637.11	2	0	0	0	2	22.22%
USDA Food and Nutrition Service	2	356	126.5	0	0	0	0	0	0.00%
USDA Food Safety And Inspection Service	19	525.11	130.47	4	0	2	0	6	31.58%
USDA Foreign Agricultural Service	1	499	55	1	0	0	0	1	100.00%
USDA Forest Service	45	570.91	215.71	4	6	1	0	11	24.44%
USDA Grain Inspection, Packers & Stockyards Admin	3	761.67	373.33	0	0	0	0	0	0.00%
USDA National Agricultural Statistics Service	0	0	0	0	0	0	0	0	0.00%
USDA National Appeals Division	0	0	0	0	0	0	0	0	0.00%
USDA National Institute of Food and Agriculture	0	0	0	0	0	0	0	0	0.00%
USDA Natural Resources Conservation Service	8	602.75	295.88	2	2	0	0	4	50.00%
USDA Office Of The Chief Financial Officer	6	527.67	527.67	0	0	0	0	0	0.00%
USDA Risk Management Agency	3	755.33	43.67	3	0	0	0	3	100.00%
USDA Rural Development	15	759.27	181.8	1	0	0	0	1	6.67%
Department of Commerce Wide	**189**	**569.24**	**242.79**	**4**	**4**	**18**	**0**	**26**	**13.76%**
DOC All Other Commerce Bureaus	7	461.29	176.71	0	0	2	0	2	28.57%
DOC Bureau of the Census	22	476.36	214.27	2	0	1	0	3	13.64%
DOC Decennial Census	125	631.04	278.11	1	1	7	0	9	7.20%
DOC International Trade Administration	2	360	156.5	0	0	0	0	0	0.00%
DOC National Institute of Standards & Technology	5	457	202.6	0	0	1	0	1	20.00%
DOC National Oceanic & Atmospheric Administration	19	409.37	176.47	0	0	2	0	2	10.53%
DOC U. S. Patent and Trademark Office	9	468.22	54.78	1	3	5	0	9	100.00%

Table B-14a FY 2012 Timeliness of Merit Final Agency Decisions (FAD) (No AJ Decision) - Sub-Component Data									
Agency or Department	Total Number Agency Merit Decisions (No AJ Decision)	APD from Date Complaint Filed/Remanded	APD From Date FAD Required	Number Timely Completed Where FAD Requested	Number Timely Completed Where No Election Made	Number Timely Completed Where AJ Ordered FAD	Number Timely Completed Where Mixed Case	Total Number Timely Agency Merit Decisions (No AJ Decision)	% Timely Agency Merit Decisions (No AJ Decision)
Department of Energy Wide	**18**	**371.67**	**91.72**	**2**	**0**	**3**	**0**	**5**	**27.78%**
DOE Bonneville Power Administration	3	354	146.33	0	0	0	0	0	0.00%
DOE Chicago Operations Office	0	0	0	0	0	0	0	0	0.00%
DOE EM Consolidated Business Center	0	0	0	0	0	0	0	0	0.00%
DOE Golden Field Office	0	0	0	0	0	0	0	0	0.00%
DOE Headquarters	5	525.2	121.2	0	0	0	0	0	0.00%
DOE Idaho Operations Office	0	0	0	0	0	0	0	0	0.00%
DOE National Energy Technology Lab	0	0	0	0	0	0	0	0	0.00%
DOE NNSA Service Center	3	294.33	75	0	0	1	0	1	33.33%
DOE Oak Ridge Operations	0	0	0	0	0	0	0	0	0.00%
DOE OSTI	0	0	0	0	0	0	0	0	0.00%
DOE Richland Operations Office	0	0	0	0	0	0	0	0	0.00%
DOE Savannah River Operations	2	352	38	0	0	2	0	2	100.00%
DOE Southeastern Power Administration	0	0	0	0	0	0	0	0	0.00%
DOE Southwestern Power Administration	1	400	60	1	0	0	0	1	100.00%
DOE Strategic Petroleum Reserve	0	0	0	0	0	0	0	0	0.00%
DOE Western Area Power Administration	4	253.75	61.25	1	0	0	0	1	25.00%
Department of Health and Human Services Wide	**96**	**404.14**	**63.85**	**20**	**13**	**17**	**4**	**54**	**56.25%**
HHS Administration for Children and Families	3	920	94.67	0	2	0	0	2	66.67%
HHS Agency for Healthcare Research and Quality	0	0	0	0	0	0	0	0	0.00%
HHS Centers for Disease Control and Prevention	11	423.27	64.09	4	3	1	0	8	72.73%
HHS Centers for Medicare & Medicaid Services	8	518.5	61	1	1	3	0	5	62.50%
HHS Food and Drug Administration	5	557.6	122.8	0	0	0	0	0	0.00%
HHS Health Resources and Services Administration	7	341.71	31.14	1	0	5	0	6	85.71%
HHS Indian Health Service	29	268.59	28	13	6	3	0	22	75.86%
HHS National Institutes of Health	21	404.95	101.9	1	0	2	0	3	14.29%
HHS Office of the Secretary of Health &Human Srvcs	11	493.27	72.27	0	1	3	4	8	72.73%
HHS Program Support Center	0	0	0	0	0	0	0	0	0.00%
HHS Substance Abuse & Mental Health Srvcs Admin	1	334	74	0	0	0	0	0	0.00%

Table B-14a FY 2012 Timeliness of Merit Final Agency Decisions (FAD) (No AJ Decision) - Sub-Component Data									
Agency or Department	Total Number Agency Merit Decisions (No AJ Decision)	APD from Date Complaint Filed/Remanded	APD From Date FAD Required	Number Timely Completed Where FAD Requested	Number Timely Completed Where No Election Made	Number Timely Completed Where AJ Ordered FAD	Number Timely Completed Where Mixed Case	Total Number Timely Agency Merit Decisions (No AJ Decision)	% Timely Agency Merit Decisions (No AJ Decision)
Department of Homeland Security Wide	**337**	**493.66**	**142.91**	**64**	**37**	**58**	**4**	**163**	**48.37%**
DHS Federal Emergency Management Agency	36	811.06	233.78	1	1	6	0	8	22.22%
DHS Federal Law Enforcement Training Center	1	292	78	0	0	0	0	0	0.00%
DHS Headquarters	10	455.5	100.7	2	2	1	0	5	50.00%
DHS Transportation Security Administration	109	461.31	111.5	25	12	16	2	55	50.46%
DHS U.S. Citizenship and Immigration Services	19	383.42	75.84	5	1	5	0	11	57.89%
DHS U.S. Coast Guard	17	313.53	60.29	4	7	1	1	13	76.47%
DHS U.S. Customs and Border Protection	91	400.19	157.2	24	9	20	1	54	59.34%
DHS U.S. Immigration and Customs Enforcement	42	638.21	212.33	2	2	9	0	13	30.95%
DHS U.S. Secret Service	12	516.42	68	1	3	0	0	4	33.33%
Department of Justice Wide	**362**	**775.83**	**382.55**	**7**	**13**	**7**	**1**	**28**	**7.73%**
DOJ Alcohol, Tobacco, Firearms and Explosives	19	362.11	217.63	0	2	0	0	2	10.53%
DOJ Bureau of Prisons	143	737.02	491.06	1	6	0	1	8	5.59%
DOJ Drug Enforcement Administration	17	769.29	382	0	0	0	0	0	0.00%
DOJ Executive Office for Immigration Review	9	526.44	130.33	0	0	0	0	0	0.00%
DOJ Executive Office for U.S. Attorneys	19	812.11	384.89	1	0	1	0	2	10.53%
DOJ Federal Bureau of Investigation	115	916.68	312.7	5	3	2	0	10	8.70%
DOJ Office of Justice Programs	1	376	60	0	1	0	0	1	100.00%
DOJ Offices, Boards, and Divisions	8	400	85	0	1	0	0	1	12.50%
DOJ U.S. Marshals Service	31	849.52	401.45	0	0	4	0	4	12.90%
Department of Labor Wide	**44**	**357.14**	**59.48**	**9**	**15**	**9**	**5**	**38**	**86.36%**
DOL (DM and others)	17	335.35	61.82	3	6	2	2	13	76.47%
DOL Bureau of Labor Statistics	0	0	0	0	0	0	0	0	0.00%
DOL Employment and Training Administration	8	441.38	58.63	2	2	4	0	8	100.00%
DOL Mine Safety and Health Administration	4	296	66.25	0	3	0	0	3	75.00%
DOL Occupational Safety and Health Administration	4	295.5	54.25	1	1	0	1	3	75.00%
DOL Office of Workers Compensation Programs	8	356.63	54.38	1	3	2	2	8	100.00%
DOL Wage and Hour Division	3	421	60	2	0	1	0	3	100.00%

Table B-14a FY 2012 Timeliness of Merit Final Agency Decisions (FAD) (No AJ Decision) - Sub-Component Data									
Agency or Department	Total Number Agency Merit Decisions (No AJ Decision)	APD from Date Complaint Filed/Remanded	APD From Date FAD Required	Number Timely Completed Where FAD Requested	Number Timely Completed Where No Election Made	Number Timely Completed Where AJ Ordered FAD	Number Timely Completed Where Mixed Case	Total Number Timely Agency Merit Decisions (No AJ Decision)	% Timely Agency Merit Decisions (No AJ Decision)
Department of the Army Wide	**181**	**528.11**	**108.17**	**4**	**4**	**5**	**8**	**21**	**11.60%**
Eighth U.S. Army (KOREA)	1	364	101	0	0	0	0	0	0.00%
Headquarters, Department of Army	14	468.43	108.14	0	0	0	1	1	7.14%
U.S. Army Corps of Engineers	20	487.8	92.25	0	2	1	1	4	20.00%
U.S. Army Europe	0	0	0	0	0	0	0	0	0.00%
U.S. Army Forces Command	11	357.36	113.09	1	0	0	1	2	18.18%
U.S. Army Installation Management Command	39	537.59	111.44	0	1	2	0	3	7.69%
U.S. Army Intelligence and Security Command	4	337.75	87.5	1	0	0	0	1	25.00%
U.S. Army Material Command	34	529.79	106.68	0	1	0	2	3	8.82%
U.S. Army Medical Command	34	608.35	108.06	2	0	1	2	5	14.71%
U.S. Army Network Enterprise Technology Command	2	379	132	0	0	0	0	0	0.00%
U.S. Army Pacific (USARPAC)	0	0	0	0	0	0	0	0	0.00%
U.S. Army Space and Missile Defense Command	0	0	0	0	0	0	0	0	0.00%
U.S. Army Special Operations Command (USASOC)	0	0	0	0	0	0	0	0	0.00%
U.S. Army Test and Evaluation Command	3	817.67	104.33	0	0	0	0	0	0.00%
U.S. Army Training and Doctrine Command	19	566	121.05	0	0	1	1	2	10.53%
Department of the Interior Wide	**104**	**574.44**	**173.24**	**5**	**7**	**0**	**0**	**12**	**11.54%**
Bureau of Ocean Energy Management	0	0	0	0	0	0	0	0	0.00%
Bureau of Safety and Environmental Enforcement	0	0	0	0	0	0	0	0	0.00%
DOI Bureau Of Indian Affairs	20	873.95	197.5	2	3	0	0	5	25.00%
DOI Bureau Of Land Management	12	389.33	158	1	1	0	0	2	16.67%
DOI Bureau Of Reclamation	16	378.94	150.63	0	0	0	0	0	0.00%
DOI Fish And Wildlife Service	11	317.55	122.45	0	0	0	0	0	0.00%
DOI Geological Survey	3	337.67	78	0	0	0	0	0	0.00%
DOI National Park Service	22	724.5	217.73	0	1	0	0	1	4.55%
DOI Office Of Surface Mining, Reclamation& Enforce	0	0	0	0	0	0	0	0	0.00%
DOI-Office Of The Secretary	20	554.15	169.5	2	2	0	0	4	20.00%
Department of the Navy Wide	**117**	**477.23**	**53.45**	**52**	**44**	**17**	**4**	**117**	**100.00%**
Chief Of Naval Operations	5	325.8	57.8	4	1	0	0	5	100.00%
Commander Naval Installations Command	17	515.18	55.65	6	8	3	0	17	100.00%

Table B-14a FY 2012 Timeliness of Merit Final Agency Decisions (FAD) (No AJ Decision) - Sub-Component Data									
Agency or Department	Total Number Agency Merit Decisions (No AJ Decision)	APD from Date Complaint Filed/Remanded	APD From Date FAD Required	Number Timely Completed Where FAD Requested	Number Timely Completed Where No Election Made	Number Timely Completed Where AJ Ordered FAD	Number Timely Completed Where Mixed Case	Total Number Timely Agency Merit Decisions (No AJ Decision)	% Timely Agency Merit Decisions (No AJ Decision)
Commander Naval Reserve	0	0	0	0	0	0	0	0	0.00%
Commander Pacific Fleet	8	339.63	54.25	3	3	1	1	8	100.00%
DON Assistant for Administration	6	444.67	51.5	4	1	0	1	6	100.00%
DON Bureau of Medicine & Surgery	12	519.5	48.75	4	3	5	0	12	100.00%
DON SPAWAR	1	334	58	1	0	0	0	1	100.00%
DON Strategic Systems Project Office	0	0	0	0	0	0	0	0	0.00%
Fleet Cyber Command	0	0	0	0	0	0	0	0	0.00%
Fleet Forces Command	5	428	53	0	4	1	0	5	100.00%
Marine Corps HQ	21	501.33	51.1	12	6	2	1	21	100.00%
Military Sealift Command	2	419.5	59	0	1	1	0	2	100.00%
Naval Air Systems Command	10	490.2	53.3	6	3	1	0	10	100.00%
Naval Education & Training Command	1	307	53	0	1	0	0	1	100.00%
Naval Sea Systems Command	7	467.71	52.57	2	3	1	1	7	100.00%
Naval Special Warfare Command	0	0	0	0	0	0	0	0	0.00%
Naval Supply Systems Command	10	476.7	58.5	5	4	1	0	10	100.00%
Naval Systems Management Activity	0	0	0	0	0	0	0	0	0.00%
Navy Facilities & Engineering Command	9	617.33	53.44	4	4	1	0	9	100.00%
Navy Military Personnel Command	1	378	41	0	1	0	0	1	100.00%
Office Of Naval Intelligence	1	464	56	0	1	0	0	1	100.00%
Office Of Naval Research	1	341	60	1	0	0	0	1	100.00%
Department of the Treasury Wide	**123**	**355.41**	**41.02**	**20**	**52**	**26**	**10**	**108**	**87.80%**
Treas - Alcohol and Tobacco Tax and Trade Bureau	0	0	0	0	0	0	0	0	0.00%
Treas - Bureau of Engraving and Printing	3	301.33	98.33	0	2	0	0	2	66.67%
Treas - Bureau of the Public Debt	1	240	55	0	1	0	0	1	100.00%
Treas - Departmental Offices	4	242	38.25	0	2	0	1	3	75.00%
Treas - Financial Crimes Enforcement Network	2	515	32.5	0	0	1	1	2	100.00%
Treas - Financial Management Service	2	321	57	0	1	0	0	1	50.00%
Treas - Inspector General For Tax Administration	0	0	0	0	0	0	0	0	0.00%
Treas - Internal Revenue Service	95	368.08	39.08	19	37	22	7	85	89.47%
Treas - Office of the Comptroller of the Currency	2	185.5	27	0	1	0	1	2	100.00%
Treas - Special Inspector General for the Trouble Assets Relief Program	0	0	0	0	0	0	0	0	0.00%

Table B-14a FY 2012 Timeliness of Merit Final Agency Decisions (FAD) (No AJ Decision) - Sub-Component Data									
Agency or Department	Total Number Agency Merit Decisions (No AJ Decision)	APD from Date Complaint Filed/Remanded	APD From Date FAD Required	Number Timely Completed Where FAD Requested	Number Timely Completed Where No Election Made	Number Timely Completed Where AJ Ordered FAD	Number Timely Completed Where Mixed Case	Total Number Timely Agency Merit Decisions (No AJ Decision)	% Timely Agency Merit Decisions (No AJ Decision)
Treas - U. S. Mint	12	341.17	44.58	1	6	3	0	10	83.33%
Treas -Internal Revenue Service Office of the Chief	2	249.5	30.5	0	2	0	0	2	100.00%
Treas- Office of the Inspector General	0	0	0	0	0	0	0	0	0.00%
Department of Transportation Wide	**89**	**413.53**	**75.36**	**7**	**21**	**19**	**0**	**47**	**52.81%**
DOT Federal Aviation Administration	75	417.48	79.64	7	15	13	0	35	46.67%
DOT Federal Highway Administration	4	426	62.25	0	1	1	0	2	50.00%
DOT Federal Motor Carrier Safety Administration	2	221	41.5	0	2	0	0	2	100.00%
DOT Federal Railroad Administrataion	1	254	39	0	1	0	0	1	100.00%
DOT Federal Transit Administration	0	0	0	0	0	0	0	0	0.00%
DOT Maritime Administration	1	671	48	0	0	1	0	1	100.00%
DOT National Highway Traffic Safety Administration	1	169	54	0	1	0	0	1	100.00%
DOT Office of Inspector General	1	469	43	0	0	1	0	1	100.00%
DOT Office of the Secretary	1	275	59	0	1	0	0	1	100.00%
DOT Pipeline& Hazardous Materials Safety Admin	0	0	0	0	0	0	0	0	0.00%
DOT Research& Innovative Technology Administration	3	503	53	0	0	3	0	3	100.00%
DOT St. Lawrence Development Corporation	0	0	0	0	0	0	0	0	0.00%
Department of Veterans Affairs Wide	**597**	**464.04**	**177.88**	**9**	**6**	**7**	**8**	**30**	**5.03%**
VA-HQ and Others	18	402.39	181	2	0	0	0	2	11.11%
VA-NCA	6	593.83	175	0	0	0	0	0	0.00%
VA-Veterans Benefits Administration	44	468.64	196.05	1	1	1	1	4	9.09%
VA-Veterans Health Administration	529	464.29	176.3	6	5	6	7	24	4.54%
Federal Housing Finance Agency Wide	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0.00%**
Federal Housing Finance Agency Hqtrs	0	0	0	0	0	0	0	0	0.00%
Federal Housing Finance Agency OIG	0	0	0	0	0	0	0	0	0.00%

Table B-14a FY 2012 Timeliness of Merit Final Agency Decisions (FAD) (No AJ Decision) - Sub-Component Data									
Agency or Department	Total Number Agency Merit Decisions (No AJ Decision)	APD from Date Complaint Filed/Remanded	APD From Date FAD Required	Number Timely Completed Where FAD Requested	Number Timely Completed Where No Election Made	Number Timely Completed Where AJ Ordered FAD	Number Timely Completed Where Mixed Case	Total Number Timely Agency Merit Decisions (No AJ Decision)	% Timely Agency Merit Decisions (No AJ Decision)
General Services Administration Wide	**21**	**397.57**	**59.19**	**8**	**4**	**2**	**1**	**15**	**71.43%**
GSA Central Office	6	478	67.17	0	3	1	0	4	66.67%
GSA National Capital Region	5	388.8	48	3	0	0	0	3	60.00%
GSA Region 1	0	0	0	0	0	0	0	0	0.00%
GSA Region 10	0	0	0	0	0	0	0	0	0.00%
GSA Region 2	0	0	0	0	0	0	0	0	0.00%
GSA Region 3	5	398.2	66.6	3	1	0	0	4	80.00%
GSA Region 4	0	0	0	0	0	0	0	0	0.00%
GSA Region 5	1	285	90	0	0	0	0	0	0.00%
GSA Region 6	1	228	58	1	0	0	0	1	100.00%
GSA Region 7	0	0	0	0	0	0	0	0	0.00%
GSA Region 8	0	0	0	0	0	0	0	0	0.00%
GSA Region 9	3	344.33	39.67	1	0	1	1	3	100.00%
U.S. Postal Service Wide	**1,088**	**277.48**	**32.41**	**123**	**515**	**315**	**109**	**1,062**	**97.61%**
USPS Capital Metro Area Operations	132	307.36	36.21	16	54	43	15	128	96.97%
USPS Eastern Area	167	306.01	30.74	23	74	48	11	156	93.41%
USPS Great Lakes Area	146	311.41	36.18	18	58	53	14	143	97.95%
USPS Headquarters	21	281.52	32.43	4	10	5	2	21	100.00%
USPS Northeast Area	86	277.94	33.33	13	50	19	4	86	100.00%
USPS Office of Inspector General	1	153	49	0	1	0	0	1	100.00%
USPS Pacific Area	101	257.64	29.73	4	51	21	23	99	98.02%
USPS Southern Area	288	246.79	30.9	29	141	85	29	284	98.61%
USPS Western Area	146	258.17	31.27	16	76	41	11	144	98.63%

Table B-15 FY 2012 Complaints Closed with Findings of Discrimination

Agency or Department	Total Number Merit Complaint Closures	Number Merit Final Agency Decisions (FADs) (no AJ)	Number Merit FADs Finding Discrimination	% Merit FADs Finding Discrimination	Number Final Orders (FOs) of AJ Merit Decisions	Number FOs of AJ Merit Decisions Finding Discrimination	% FOs of AJ Merit Decisions Finding Discrimination	Number FOs Fully Implementing (FI) AJ Merit Decisions Finding Discrimination	% FOs FI AJ Merit Decisions Finding Discrimination	Number FOs Not Fully Implementing (NFI) AJ Merit Decisions Finding Discrimination	% FOs NFI AJ Merit Decisions Finding Discrimination
Advisory Council on Historic Preservation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
African Development Foundation	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Agency for International Development	2	1	0	0.00%	1	0	0.00%	0	0.00%	0	0.00%
American Battle Monuments Commission	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Appalachian Regional Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Architectural and Transportation Barriers Compliance Board	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Arctic Research Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Armed Forces Retirement Home	4	4	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Barry Goldwater Scholarship and Excellence in Education Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Broadcasting Board of Governors	3	2	0	0.00%	1	0	0.00%	0	0.00%	0	0.00%
Central Intelligence Agency	17	6	0	0.00%	11	0	0.00%	0	0.00%	0	0.00%
Chemical Safety and Hazard Investigation Board	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Christopher Columbus Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission of Fine Arts	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission on Civil Rights	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Committee for Purchase from People Who Are Blind or Severely Disabled	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Commodity Futures Trading Commission	2	2	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Consumer Financial Protection Bureau	3	3	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Consumer Product Safety Commission	1	1	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Corporation for National and Community Service	3	3	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Court Services and Offender Supervision Agency for the District of Columbia	7	2	0	0.00%	5	1	20.00%	1	100.00%	0	0.00%
Defense Army and Air Force Exchange	27	14	1	7.14%	13	0	0.00%	0	0.00%	0	0.00%
Defense Commissary Agency	45	27	0	0.00%	18	1	5.56%	1	100.00%	0	0.00%
Defense Contract Audit Agency	10	7	0	0.00%	3	0	0.00%	0	0.00%	0	0.00%
Defense Contract Management Agency	8	8	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Finance and Accounting Service	14	8	1	12.50%	6	0	0.00%	0	0.00%	0	0.00%
Defense Human Resources Activity	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Information Systems Agency	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Intelligence Agency	14	7	0	0.00%	7	2	28.57%	0	0.00%	2	100.00%
Defense Joint Task Force National Capital Region Medical	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Logistics Agency	61	38	2	5.26%	23	0	0.00%	0	0.00%	0	0.00%
Defense Media Activity	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Missile Defense Agency	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense National Geospatial-Intelligence Agency	7	4	0	0.00%	3	0	0.00%	0	0.00%	0	0.00%
Defense National Guard Bureau	3	3	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense National Security Agency	9	5	0	0.00%	4	2	50.00%	0	0.00%	2	100.00%
Defense Nuclear Facilities Safety Board	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Office of the Inspector General	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Office of the Secretary - Wash. Hqtrs. Services	13	6	0	0.00%	7	0	0.00%	0	0.00%	0	0.00%

Table B-15 FY 2012 Complaints Closed with Findings of Discrimination

Agency or Department	Total Number Merit Complaint Closures	Number Merit Final Agency Decisions (FADs) (no AJ)	Number Merit FADs Finding Discrimination	% Merit FADs Finding Discrimination	Number Final Orders (FOs) of AJ Merit Decisions	Number FOs of AJ Merit Decisions Finding Discrimination	% FOs of AJ Merit Decisions Finding Discrimination	Number FOs Fully Implementing (FI) AJ Merit Decisions Finding Discrimination	% FOs FI AJ Merit Decisions Finding Discrimination	Number FOs Not Fully Implementing (NFI) AJ Merit Decisions Finding Discrimination	% FOs NFI AJ Merit Decisions Finding Discrimination
Defense Security Service	3	3	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Technical Information Center	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Threat Reduction Agency	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense TRICARE Management Activity	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Uniformed Services University	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Department of Agriculture	206	151	10	6.62%	55	1	1.82%	1	100.00%	0	0.00%
Department of Commerce	289	189	1	0.53%	100	7	7.00%	6	85.71%	1	14.29%
Department of Defense Education Activity	18	12	0	0.00%	6	0	0.00%	0	0.00%	0	0.00%
Department of Education	29	17	0	0.00%	12	0	0.00%	0	0.00%	0	0.00%
Department of Energy	21	18	2	11.11%	3	0	0.00%	0	0.00%	0	0.00%
Department of Health and Human Services	130	96	2	2.08%	34	2	5.88%	2	100.00%	0	0.00%
Department of Homeland Security	555	337	1	0.30%	218	12	5.50%	9	75.00%	3	25.00%
Department of Housing and Urban Development	40	25	0	0.00%	15	0	0.00%	0	0.00%	0	0.00%
Department of Justice	506	362	10	2.76%	144	7	4.86%	4	57.14%	3	42.86%
Department of Labor	56	44	0	0.00%	12	0	0.00%	0	0.00%	0	0.00%
Department of State	54	40	0	0.00%	14	3	21.43%	2	66.67%	1	33.33%
Department of the Air Force	193	96	0	0.00%	97	7	7.22%	7	100.00%	0	0.00%
Department of the Army	303	181	2	1.10%	122	8	6.56%	5	62.50%	3	37.50%
Department of the Interior	146	104	2	1.92%	42	1	2.38%	1	100.00%	0	0.00%
Department of the Navy	193	117	0	0.00%	76	8	10.53%	7	87.50%	1	12.50%
Department of the Treasury	226	123	5	4.07%	103	1	0.97%	1	100.00%	0	0.00%
Department of Transportation	142	89	0	0.00%	53	3	5.66%	3	100.00%	0	0.00%
Department of Veterans Affairs	973	597	16	2.68%	376	26	6.91%	23	88.46%	3	11.54%
Election Assistance Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Environmental Protection Agency	23	13	1	7.69%	10	0	0.00%	0	0.00%	0	0.00%
Equal Employment Opportunity Commission	8	5	0	0.00%	3	0	0.00%	0	0.00%	0	0.00%
Export-Import Bank of the US	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Farm Credit Administration	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Farm Credit System Insurance Corporation	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Communications Commission	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Deposit Insurance Corporation	14	12	0	0.00%	2	0	0.00%	0	0.00%	0	0.00%
Federal Election Commission	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Energy Regulatory Commission	6	6	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Financial Institutions Examination Council	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Housing Finance Agency	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Labor Relations Authority	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Maritime Commission	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Mediation and Conciliation Service	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Mine Safety & Health Review Commission	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Reserve System--Board of Governors	1	0	0	0.00%	1	0	0.00%	0	0.00%	0	0.00%
Federal Retirement Thrift Investment Board	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Trade Commission	1	0	0	0.00%	1	0	0.00%	0	0.00%	0	0.00%

Table B-15 FY 2012 Complaints Closed with Findings of Discrimination

Agency or Department	Total Number Merit Complaint Closures	Number Merit Final Agency Decisions (FADs) (no AJ)	Number Merit FADs Finding Discrimination	% Merit FADs Finding Discrimination	Number Final Orders (FOs) of AJ Merit Decisions	Number FOs of AJ Merit Decisions Finding Discrimination	% FOs of AJ Merit Decisions Finding Discrimination	Number FOs Fully Implementing (FI) AJ Merit Decisions Finding Discrimination	% FOs FI AJ Merit Decisions Finding Discrimination	Number FOs Not Fully Implementing (NFI) AJ Merit Decisions Finding Discrimination	% FOs NFI AJ Merit Decisions Finding Discrimination
General Services Administration	44	21	0	0.00%	23	0	0.00%	0	0.00%	0	0.00%
Government Printing Office	13	11	0	0.00%	2	0	0.00%	0	0.00%	0	0.00%
Harry S. Truman Scholarship Foundation	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Holocaust Memorial Museum U.S.	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Institute of Museum and Library Services	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Inter-American Foundation	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
International Boundary and Water Commission	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
International Joint Commission: US and Canada	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
International Trade Commission	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
James Madison Memorial Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Japan-United States Friendship Commission	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
John F. Kennedy Center for the Performing Arts	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Marine Mammal Commission	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Merit Systems Protection Board	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Millennium Challenge Corporation	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Aeronautics and Space Administration	21	11	0	0.00%	10	0	0.00%	0	0.00%	0	0.00%
National Archives and Records Administration	6	3	0	0.00%	3	0	0.00%	0	0.00%	0	0.00%
National Capital Planning Commission	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Council on Disability	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Credit Union Administration	1	1	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Endowment for the Arts	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Endowment for the Humanities	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Foundation on the Arts & the Humanities	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Gallery of Art	3	3	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Indian Gaming Commission	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Labor Relations Board	3	2	1	50.00%	1	0	0.00%	0	0.00%	0	0.00%
National Mediation Board	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Reconnaissance Office	4	2	0	0.00%	2	0	0.00%	0	0.00%	0	0.00%
National Science Foundation	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Transportation Safety Board	1	1	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Navajo and Hopi Indian Relocation Commission	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Nuclear Regulatory Commission	1	0	0	0.00%	1	0	0.00%	0	0.00%	0	0.00%
Nuclear Waste Technical Review Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Occupational Safety & Health Review Commission	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Office of Government Ethics	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Office of Personnel Management	13	8	0	0.00%	5	0	0.00%	0	0.00%	0	0.00%
Office of Special Counsel	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Office of the Director of National Intelligence	1	1	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Overseas Private Investment Corporation	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%

Table B-15 FY 2012 Complaints Closed with Findings of Discrimination

Agency or Department	Total Number Merit Complaint Closures	Number Merit Final Agency Decisions (FADs) (no AJ)	Number Merit FADs Finding Discrimination	% Merit FADs Finding Discrimination	Number Final Orders (FOs) of AJ Merit Decisions	Number FOs of AJ Merit Decisions Finding Discrimination	% FOs of AJ Merit Decisions Finding Discrimination	Number FOs Fully Implementing (FI) AJ Merit Decisions Finding Discrimination	% FOs FI AJ Merit Decisions Finding Discrimination	Number FOs Not Fully Implementing (NFI) AJ Merit Decisions Finding Discrimination	% FOs NFI AJ Merit Decisions Finding Discrimination
Peace Corps	3	3	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Pension Benefit Guaranty Corporation	11	5	1	20.00%	6	1	16.67%	0	0.00%	1	100.00%
Postal Regulatory Commission	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Presidio Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Railroad Retirement Board	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Securities and Exchange Commission	2	2	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Selective Service System	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Small Business Administration	12	7	0	0.00%	5	0	0.00%	0	0.00%	0	0.00%
Smithsonian Institution	8	5	0	0.00%	3	0	0.00%	0	0.00%	0	0.00%
Social Security Administration	252	136	0	0.00%	116	12	10.34%	4	33.33%	8	66.67%
Tennessee Valley Authority	34	20	1	5.00%	14	0	0.00%	0	0.00%	0	0.00%
Trade and Development Agency	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
U.S. Postal Service	1,936	1,088	0	0.00%	848	50	5.90%	47	94.00%	3	6.00%
Utah Reclamation Mitigation and Conservation Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Valles Caldera Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Cabinet Level Subtotal	6,230	3,816	55	1.44%	2,414	141	5.84%	119	84.40%	22	15.60%
Midsize Agencies Subtotal	424	236	2	0.85%	188	12	6.38%	4	33.33%	8	66.67%
Small Agencies Subtotal	104	66	2	3.03%	38	2	5.26%	1	50.00%	1	50.00%
Micro Agencies Subtotal	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Government-wide	6,758	4,118	59	1.43%	2,640	155	5.87%	124	80.00%	31	20.00%

NRF = No Report Filed

Table B-16 FY 2012 Complaints Closed with Findings of No Discrimination

Agency or Department	Total Number Merit Complaint Closures	Number Merit Final Agency Decisions (FADs) (no AJ)	Number Merit FADs Finding No Discrimination	% Merit FADs Finding No Discrimination	Number Final Orders (FOs) of AJ Merit Decisions	FOs of AJ Merit Decisions Finding No Discrimination	% FOs of AJ Merit Decisions Finding No Discrimination	Number FOs Fully Implementing (FI) AJ Merit Decisions Finding No Discrimination	% FOs FI AJ Merit Decisions Finding No Discrimination	Number FOs Not Fully Implementing (NFI) AJ Merit Decisions Finding No Discrimination	% FOs NFI AJ Merit Decisions Finding No Discrimination
Advisory Council on Historic Preservation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
African Development Foundation	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Agency for International Development	2	1	1	100.00%	1	1	100.00%	1	100.00%	0	0.00%
American Battle Monuments Commission	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Appalachian Regional Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Architectural and Transportation Barriers Compliance Board	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Arctic Research Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Armed Forces Retirement Home	4	4	4	100.00%	0	0	0.00%	0	0.00%	0	0.00%
Barry Goldwater Scholarship and Excellence in Education Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Broadcasting Board of Governors	3	2	2	100.00%	1	1	100.00%	1	100.00%	0	0.00%
Central Intelligence Agency	17	6	6	100.00%	11	11	100.00%	11	100.00%	0	0.00%
Chemical Safety and Hazard Investigation Board	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Christopher Columbus Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission of Fine Arts	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission on Civil Rights	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Committee for Purchase from People Who Are Blind or Severely Disabled	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Commodity Futures Trading Commission	2	2	2	100.00%	0	0	0.00%	0	0.00%	0	0.00%
Consumer Financial Protection Bureau	3	3	3	100.00%	0	0	0.00%	0	0.00%	0	0.00%
Consumer Product Safety Commission	1	1	1	100.00%	0	0	0.00%	0	0.00%	0	0.00%
Corporation for National and Community Service	3	3	3	100.00%	0	0	0.00%	0	0.00%	0	0.00%
Court Services and Offender Supervision Agency for the District of Columbia	7	2	2	100.00%	5	4	80.00%	4	100.00%	0	0.00%
Defense Army and Air Force Exchange	27	14	13	92.86%	13	13	100.00%	13	100.00%	0	0.00%
Defense Commissary Agency	45	27	27	100.00%	18	17	94.44%	17	100.00%	0	0.00%
Defense Contract Audit Agency	10	7	7	100.00%	3	3	100.00%	3	100.00%	0	0.00%
Defense Contract Management Agency	8	8	8	100.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Finance and Accounting Service	14	8	7	87.50%	6	6	100.00%	6	100.00%	0	0.00%
Defense Human Resources Activity	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Information Systems Agency	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Intelligence Agency	14	7	7	100.00%	7	5	71.43%	5	100.00%	0	0.00%
Defense Joint Task Force National Capital Region Medical	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Logistics Agency	61	38	36	94.74%	23	23	100.00%	23	100.00%	0	0.00%
Defense Media Activity	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Missile Defense Agency	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense National Geospatial-Intelligence Agency	7	4	4	100.00%	3	3	100.00%	3	100.00%	0	0.00%
Defense National Guard Bureau	3	3	3	100.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense National Security Agency	9	5	5	100.00%	4	2	50.00%	2	100.00%	0	0.00%

Table B-16 FY 2012 Complaints Closed with Findings of No Discrimination

Agency or Department	Total Number Merit Complaint Closures	Number Merit Final Agency Decisions (FADs) (no AJ)	Number Merit FADs Finding No Discrimination	% Merit FADs Finding No Discrimination	Number Final Orders (FOs) of AJ Merit Decisions	FOs of AJ Merit Decisions Finding No Discrimination	% FOs of AJ Merit Decisions Finding No Discrimination	Number FOs Fully Implementing (FI) AJ Merit Decisions Finding No Discrimination	% FOs FI AJ Merit Decisions Finding No Discrimination	Number FOs Not Fully Implementing (NFI) AJ Merit Decisions Finding No Discrimination	% FOs NFI AJ Merit Decisions Finding No Discrimination
Defense Nuclear Facilities Safety Board	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Office of the Inspector General	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Office of the Secretary - Wash. Hqtrs. Services	13	6	6	100.00%	7	7	100.00%	7	100.00%	0	0.00%
Defense Security Service	3	3	3	100.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Technical Information Center	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Threat Reduction Agency	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense TRICARE Management Activity	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Uniformed Services University	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Department of Agriculture	206	151	141	93.38%	55	54	98.18%	54	100.00%	0	0.00%
Department of Commerce	289	189	188	99.47%	100	93	93.00%	92	98.92%	1	1.08%
Department of Defense Education Activity	18	12	12	100.00%	6	6	100.00%	6	100.00%	0	0.00%
Department of Education	29	17	17	100.00%	12	12	100.00%	12	100.00%	0	0.00%
Department of Energy	21	18	16	88.89%	3	3	100.00%	3	100.00%	0	0.00%
Department of Health and Human Services	130	96	94	97.92%	34	32	94.12%	32	100.00%	0	0.00%
Department of Homeland Security	555	337	336	99.70%	218	206	94.50%	206	100.00%	0	0.00%
Department of Housing and Urban Development	40	25	25	100.00%	15	15	100.00%	15	100.00%	0	0.00%
Department of Justice	506	362	352	97.24%	144	137	95.14%	136	99.27%	1	0.73%
Department of Labor	56	44	44	100.00%	12	12	100.00%	12	100.00%	0	0.00%
Department of State	54	40	40	100.00%	14	11	78.57%	11	100.00%	0	0.00%
Department of the Air Force	193	96	96	100.00%	97	90	92.78%	89	98.89%	1	1.11%
Department of the Army	303	181	179	98.90%	122	114	93.44%	113	99.12%	1	0.88%
Department of the Interior	146	104	102	98.08%	42	41	97.62%	41	100.00%	0	0.00%
Department of the Navy	193	117	117	100.00%	76	68	89.47%	68	100.00%	0	0.00%
Department of the Treasury	226	123	118	95.93%	103	102	99.03%	102	100.00%	0	0.00%
Department of Transportation	142	89	89	100.00%	53	50	94.34%	50	100.00%	0	0.00%
Department of Veterans Affairs	973	597	581	97.32%	376	350	93.09%	350	100.00%	0	0.00%
Election Assistance Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Environmental Protection Agency	23	13	12	92.31%	10	10	100.00%	10	100.00%	0	0.00%
Equal Employment Opportunity Commission	8	5	5	100.00%	3	3	100.00%	3	100.00%	0	0.00%
Export-Import Bank of the US	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Farm Credit Administration	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Farm Credit System Insurance Corporation	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Communications Commission	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Deposit Insurance Corporation	14	12	12	100.00%	2	2	100.00%	2	100.00%	0	0.00%
Federal Election Commission	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Energy Regulatory Commission	6	6	6	100.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Financial Institutions Examination Council	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Housing Finance Agency	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Labor Relations Authority	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Maritime Commission	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%

Table B-16 FY 2012 Complaints Closed with Findings of No Discrimination

Agency or Department	Total Number Merit Complaint Closures	Number Merit Final Agency Decisions (FADs) (no AJ)	Number Merit FADs Finding No Discrimination	% Merit FADs Finding No Discrimination	Number Final Orders (FOs) of AJ Merit Decisions	FOs of AJ Merit Decisions Finding No Discrimination	% FOs of AJ Merit Decisions Finding No Discrimination	Number FOs Fully Implementing (FI) AJ Merit Decisions Finding No Discrimination	% FOs FI AJ Merit Decisions Finding No Discrimination	Number FOs Not Fully Implementing (NFI) AJ Merit Decisions Finding No Discrimination	% FOs NFI AJ Merit Decisions Finding No Discrimination
Federal Mediation and Conciliation Service	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Mine Safety&Health Review Commission	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Reserve System--Board of Governors	1	0	0	0.00%	1	1	100.00%	1	100.00%	0	0.00%
Federal Retirement Thrift Investment Board	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Trade Commission	1	0	0	0.00%	1	1	100.00%	1	100.00%	0	0.00%
General Services Administration	44	21	21	100.00%	23	23	100.00%	23	100.00%	0	0.00%
Government Printing Office	13	11	11	100.00%	2	2	100.00%	2	100.00%	0	0.00%
Harry S. Truman Scholarship Foundation	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Holocaust Memorial Museum U.S.	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Institute of Museum and Library Services	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Inter-American Foundation	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
International Boundary and Water Commission	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
International Joint Commission: US and Canada	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
International Trade Commission	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
James Madison Memorial Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Japan-United States Friendship Commission	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
John F. Kennedy Center for the Performing Arts	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Marine Mammal Commission	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Merit Systems Protection Board	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Millennium Challenge Corporation	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Aeronautics and Space Administration	21	11	11	100.00%	10	10	100.00%	10	100.00%	0	0.00%
National Archives and Records Administration	6	3	3	100.00%	3	3	100.00%	3	100.00%	0	0.00%
National Capital Planning Commission	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Council on Disability	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Credit Union Administration	1	1	1	100.00%	0	0	0.00%	0	0.00%	0	0.00%
National Endowment for the Arts	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Endowment for the Humanities	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Foundation on the Arts& the Humanities	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Gallery of Art	3	3	3	100.00%	0	0	0.00%	0	0.00%	0	0.00%
National Indian Gaming Commission	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Labor Relations Board	3	2	1	50.00%	1	1	100.00%	1	100.00%	0	0.00%
National Mediation Board	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Reconnaissance Office	4	2	2	100.00%	2	2	100.00%	2	100.00%	0	0.00%
National Science Foundation	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Transportation Safety Board	1	1	1	100.00%	0	0	0.00%	0	0.00%	0	0.00%
Navajo and Hopi Indian Relocation Commission	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Nuclear Regulatory Commission	1	0	0	0.00%	1	1	100.00%	1	100.00%	0	0.00%
Nuclear Waste Technical Review Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Occupational Safety & Health Review Commission	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%

Table B-16 FY 2012 Complaints Closed with Findings of No Discrimination

Agency or Department	Total Number Merit Complaint Closures	Number Merit Final Agency Decisions (FADs) (no AJ)	Number Merit FADs Finding No Discrimination	% Merit FADs Finding No Discrimination	Number Final Orders (FOs) of AJ Merit Decisions	FOs of AJ Merit Decisions Finding No Discrimination	% FOs of AJ Merit Decisions Finding No Discrimination	Number FOs Fully Implementing (FI) AJ Merit Decisions Finding No Discrimination	% FOs FI AJ Merit Decisions Finding No Discrimination	Number FOs Not Fully Implementing (NFI) AJ Merit Decisions Finding No Discrimination	% FOs NFI AJ Merit Decisions Finding No Discrimination
Office of Government Ethics	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Office of Personnel Management	13	8	8	100.00%	5	5	100.00%	5	100.00%	0	0.00%
Office of Special Counsel	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Office of the Director of National Intelligence	1	1	1	100.00%	0	0	0.00%	0	0.00%	0	0.00%
Overseas Private Investment Corporation	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Peace Corps	3	3	3	100.00%	0	0	0.00%	0	0.00%	0	0.00%
Pension Benefit Guaranty Corporation	11	5	4	80.00%	6	5	83.33%	5	100.00%	0	0.00%
Postal Regulatory Commission	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Presidio Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Railroad Retirement Board	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Securities and Exchange Commission	2	2	2	100.00%	0	0	0.00%	0	0.00%	0	0.00%
Selective Service System	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Small Business Administration	12	7	7	100.00%	5	5	100.00%	5	100.00%	0	0.00%
Smithsonian Institution	8	5	5	100.00%	3	3	100.00%	3	100.00%	0	0.00%
Social Security Administration	252	136	136	100.00%	116	104	89.66%	104	100.00%	0	0.00%
Tennessee Valley Authority	34	20	19	95.00%	14	14	100.00%	14	100.00%	0	0.00%
Trade and Development Agency	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
U.S. Postal Service	1,936	1,088	1,088	100.00%	848	798	94.10%	798	100.00%	0	0.00%
Utah Reclamation Mitigation and Conservation Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Valles Caldera Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Cabinet Level Subtotal	6,230	3,816	3,761	98.56%	2,414	2,273	94.16%	2,269	99.82%	4	0.18%
Midsize Agencies Subtotal	424	236	234	99.15%	188	176	93.62%	176	100.00%	0	0.00%
Small Agencies Subtotal	104	66	64	96.97%	38	36	94.74%	36	100.00%	0	0.00%
Micro Agencies Subtotal	0	0	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Government-wide	6,758	4,118	4,059	98.57%	2,640	2,485	94.13%	2,481	99.84%	4	0.16%

NRF = No Report Filed

Table B-17 FY 2012 Average Processing Days (APD) Final Agency Decisions (FADs) and Final Orders (FOs) Fully Implementing (FI) AJ Decisions

Agency or Department	APD All Final Agency Decisions (FADs) (No AJ)	APD Merit FADs Finding Discrimination	APD Merit FADs Finding No Discrimination	APD Merit FADs From Date of Complaint Filed/ Remanded	APD FAD Dismissals	APD ALL Final Orders (FOs) of AJ Decisions	APD FOs Fully Implementing (FI) Merit Decisions	APD FI AJ Merit Decisions Finding Discrimination	APD FI AJ Merit Decisions Finding No Discrimination	APD FOs FI AJ Dismissals
Advisory Council on Historic Preservation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
African Development Foundation	0	0	0	0	0	934	934	0	0	934
Agency for International Development	184.38	0	830	830	92.14	1,525.00	1,525.00	0	1,525.00	0
American Battle Monuments Commission	0	0	0	0	0	0	0	0	0	0
Appalachian Regional Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Architectural and Transportation Barriers Compliance Board	0	0	0	0	0	0	0	0	0	0
Arctic Research Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Armed Forces Retirement Home	243.5	0	243.5	243.5	0	0	0	0	0	0
Barry Goldwater Scholarship and Excellence in Education Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Broadcasting Board of Governors	261.57	0	326	326	235.8	939	939	0	939	0
Central Intelligence Agency	258.13	0	590.33	590.33	36.67	1,186.50	1,186.50	0	1,186.82	1,183.00
Chemical Safety and Hazard Investigation Board	0	0	0	0	0	0	0	0	0	0
Christopher Columbus Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission of Fine Arts	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission on Civil Rights	0	0	0	0	0	0	0	0	0	0
Committee for Purchase from People Who Are Blind or Severely Disabled	0	0	0	0	0	0	0	0	0	0
Commodity Futures Trading Commission	314	0	314	314	0	0	0	0	0	0
Consumer Financial Protection Bureau	301	0	301	301	0	0	0	0	0	0
Consumer Product Safety Commission	416	0	416	416	0	0	0	0	0	0
Corporation for National and Community Service	431.67	0	431.67	431.67	0	0	0	0	0	0
Court Services and Offender Supervision Agency for the District of Columbia	239	0	393	393	85	901.8	901.8	1,745.00	691	0
Defense Army and Air Force Exchange	186.88	324	348	346.29	75.3	886.31	886.31	0	886.31	0
Defense Commissary Agency	198.35	0	349.44	349.44	12.91	728.11	728.11	913	717.24	0
Defense Contract Audit Agency	242.36	0	357.57	357.57	40.75	503.33	503.33	0	503.33	0
Defense Contract Management Agency	245.33	0	496.63	496.63	119.69	0	0	0	0	0
Defense Finance and Accounting Service	151.94	375	299.86	309.25	12.11	697.83	697.83	0	697.83	0
Defense Human Resources Activity	32	0	0	0	32	0	0	0	0	0
Defense Information Systems Agency	996.4	0	0	0	996.4	0	0	0	0	0
Defense Intelligence Agency	298	0	681.29	681.29	54.09	1,004.00	810.8	0	810.8	0
Defense Joint Task Force National Capital Region Medical	53	0	0	0	53	0	0	0	0	0
Defense Logistics Agency	383.06	384	500.03	493.92	82.14	682.26	682.26	0	682.26	0
Defense Media Activity	0	0	0	0	0	0	0	0	0	0
Defense Missile Defense Agency	0	0	0	0	0	0	0	0	0	0
Defense National Geospatial-Intelligence Agency	359.11	0	666.75	666.75	113	684.67	684.67	0	684.67	0

Table B-17 FY 2012 Average Processing Days (APD) Final Agency Decisions (FADs) and Final Orders (FOs) Fully Implementing (FI) AJ Decisions

Agency or Department	APD All Final Agency Decisions (FADs) (No AJ)	APD Merit FADs Finding Discrimination	APD Merit FADs Finding No Discrimination	APD Merit FADs From Date of Complaint Filed/ Remanded	APD FAD Dismissals	APD ALL Final Orders (FOs) of AJ Decisions	APD FOs Fully Implementing (FI) Merit Decisions	APD FI AJ Merit Decisions Finding Discrimination	APD FI AJ Merit Decisions Finding No Discrimination	APD FOs FI AJ Dismissals
Defense National Guard Bureau	355.54	0	361.67	361.67	354.74	0	0	0	0	0
Defense National Security Agency	291.38	0	376.4	376.4	149.67	1,268.60	930.33	0	980	831
Defense Nuclear Facilities Safety Board	0	0	0	0	0	0	0	0	0	0
Defense Office of the Inspector General	8	0	0	0	8	0	0	0	0	0
Defense Office of the Secretary - Wash. Hqtrs. Services	377.26	0	663.5	663.5	245.15	1,174.14	1,174.14	0	1,174.14	0
Defense Security Service	160	0	200	200	100	0	0	0	0	0
Defense Technical Information Center	0	0	0	0	0	0	0	0	0	0
Defense Threat Reduction Agency	868.75	0	0	0	868.75	0	0	0	0	0
Defense TRICARE Management Activity	107.8	0	0	0	107.8	0	0	0	0	0
Defense Uniformed Services University	0	0	0	0	0	0	0	0	0	0
Department of Agriculture	511.33	909.7	619.07	638.32	111.85	849.15	849.15	1,309.00	840.63	0
Department of Commerce	465.55	290	570.72	569.24	65.63	644.96	645.33	533.33	649.86	677.25
Department of Defense Education Activity	234.77	0	385.67	385.67	53.7	843.17	843.17	0	843.17	0
Department of Education	330.21	0	358.24	358.24	92	1,057.08	1,057.08	0	1,057.08	0
Department of Energy	339.25	354.5	373.81	371.67	242	638.67	638.67	0	638.67	0
Department of Health and Human Services	234.63	824.5	395.19	404.14	61.51	711.14	711.14	1,311.50	669.19	853
Department of Homeland Security	374.12	557	493.47	493.66	128.5	743.04	743.37	900	741.47	679.81
Department of Housing and Urban Development	599.54	0	624.24	624.24	393.67	747.73	747.73	0	747.73	0
Department of Justice	626.69	700.6	777.96	775.83	135.89	759.65	753.83	710.25	755.11	0
Department of Labor	302.82	0	357.14	357.14	85.55	791.15	791.15	0	752.08	849.75
Department of State	335.88	0	460.58	460.58	24.13	700.64	618.69	341.5	669.09	0
Department of the Air Force	534.65	0	839.44	839.44	97.94	711	714.1	953.71	715.83	510.56
Department of the Army	254.97	628.5	526.99	528.11	43.69	744.1	730.65	1,095.20	713.88	754.67
Department of the Interior	478.93	820	569.63	574.44	147.8	841.93	841.93	727	824.34	1,678.00
Department of the Navy	243.05	0	477.23	477.23	56.65	928.68	925.53	1,416.86	874.96	0
Department of the Treasury	296.11	453.8	351.25	355.41	130.34	801.19	801.19	993	780.22	1,079.43
Department of Transportation	270.87	0	413.53	413.53	121.51	675.02	675.02	1,037.33	651.02	731.5
Department of Veterans Affairs	315.02	544.69	461.82	464.04	88.05	678.38	672.6	878.96	659.89	651.29
Election Assistance Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Environmental Protection Agency	809.93	1,373.00	859.83	899.31	229	866.27	866.27	0	868.4	845
Equal Employment Opportunity Commission	345.5	0	529.8	529.8	161.2	601	601	0	601	0
Export-Import Bank of the US	330	0	0	0	330	0	0	0	0	0
Farm Credit Administration	0	0	0	0	0	0	0	0	0	0
Farm Credit System Insurance Corporation	0	0	0	0	0	0	0	0	0	0
Federal Communications Commission	90	0	0	0	90	0	0	0	0	0
Federal Deposit Insurance Corporation	276.39	0	407.42	407.42	133.45	585	585	0	660.5	434
Federal Election Commission	0	0	0	0	0	0	0	0	0	0
Federal Energy Regulatory Commission	165	0	200	200	60	0	0	0	0	0

Table B-17 FY 2012 Average Processing Days (APD) Final Agency Decisions (FADs) and Final Orders (FOs) Fully Implementing (FI) AJ Decisions

Agency or Department	APD All Final Agency Decisions (FADs) (No AJ)	APD Merit FADs Finding Discrimination	APD Merit FADs Finding No Discrimination	APD Merit FADs From Date of Complaint Filed/ Remanded	APD FAD Dismissals	APD ALL Final Orders (FOs) of AJ Decisions	APD FOs Fully Implementing (FI) Merit Decisions	APD FI AJ Merit Decisions Finding Discrimination	APD FI AJ Merit Decisions Finding No Discrimination	APD FOs FI AJ Dismissals
Federal Financial Institutions Examination Council	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Housing Finance Agency	170	0	0	0	170	0	0	0	0	0
Federal Labor Relations Authority	0	0	0	0	0	0	0	0	0	0
Federal Maritime Commission	0	0	0	0	0	0	0	0	0	0
Federal Mediation and Conciliation Service	0	0	0	0	0	0	0	0	0	0
Federal Mine Safety &Health Review Commission	0	0	0	0	0	0	0	0	0	0
Federal Reserve System--Board of Governors	0	0	0	0	0	792	792	0	792	0
Federal Retirement Thrift Investment Board	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Trade Commission	0	0	0	0	0	1,115.00	1,115.00	0	1,115.00	0
General Services Administration	275.63	0	397.57	397.57	42.82	740.43	740.43	0	740.43	0
Government Printing Office	257	0	358.45	358.45	33.8	1,000.00	1,000.00	0	1,000.00	0
Harry S. Truman Scholarship Foundation	0	0	0	0	0	0	0	0	0	0
Holocaust Memorial Museum U.S.	0	0	0	0	0	0	0	0	0	0
Institute of Museum and Library Services	0	0	0	0	0	0	0	0	0	0
Inter-American Foundation	0	0	0	0	0	0	0	0	0	0
International Boundary and Water Commission	0	0	0	0	0	0	0	0	0	0
International Joint Commission: US and Canada	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
International Trade Commission	0	0	0	0	0	0	0	0	0	0
James Madison Memorial Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Japan-United States Friendship Commission	0	0	0	0	0	0	0	0	0	0
John F. Kennedy Center for the Performing Arts	0	0	0	0	0	0	0	0	0	0
Marine Mammal Commission	0	0	0	0	0	0	0	0	0	0
Merit Systems Protection Board	0	0	0	0	0	0	0	0	0	0
Millennium Challenge Corporation	0	0	0	0	0	0	0	0	0	0
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Aeronautics and Space Administration	328.5	0	516.36	516.36	98.89	1,214.40	1,214.40	0	1,214.40	0
National Archives and Records Administration	407.2	0	636	636	64	1,161.33	1,161.33	0	1,161.33	0
National Capital Planning Commission	0	0	0	0	0	0	0	0	0	0
National Council on Disability	0	0	0	0	0	0	0	0	0	0
National Credit Union Administration	541	0	541	541	0	0	0	0	0	0
National Endowment for the Arts	77	0	0	0	77	0	0	0	0	0
National Endowment for the Humanities	0	0	0	0	0	0	0	0	0	0
National Foundation on the Arts&the Humanities	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Gallery of Art	575.75	0	760.67	760.67	21	0	0	0	0	0
National Indian Gaming Commission	0	0	0	0	0	0	0	0	0	0
National Labor Relations Board	163.67	242	227	234.5	22	554	554	0	554	0
National Mediation Board	0	0	0	0	0	0	0	0	0	0
National Reconnaissance Office	204.25	0	333.5	333.5	75	1,094.00	1,094.00	0	1,094.00	0

Table B-17 FY 2012 Average Processing Days (APD) Final Agency Decisions (FADs) and Final Orders (FOs) Fully Implementing (FI) AJ Decisions

Agency or Department	APD All Final Agency Decisions (FADs) (No AJ)	APD Merit FADs Finding Discrimination	APD Merit FADs Finding No Discrimination	APD Merit FADs From Date of Complaint Filed/ Remanded	APD FAD Dismissals	APD ALL Final Orders (FOs) of AJ Decisions	APD FOs Fully Implementing (FI) Merit Decisions	APD FI AJ Merit Decisions Finding Discrimination	APD FI AJ Merit Decisions Finding No Discrimination	APD FOs FI AJ Dismissals
National Science Foundation	0	0	0	0	0	0	0	0	0	0
National Transportation Safety Board	276	0	276	276	0	0	0	0	0	0
Navajo and Hopi Indian Relocation Commission	0	0	0	0	0	0	0	0	0	0
Nuclear Regulatory Commission	0	0	0	0	0	632	632	0	632	0
Nuclear Waste Technical Review Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Occupational Safety& Health Review Commission	0	0	0	0	0	0	0	0	0	0
Office of Government Ethics	15	0	0	0	15	0	0	0	0	0
Office of Personnel Management	700.93	0	1,128.25	1,128.25	131.17	134.8	134.8	0	134.8	0
Office of Special Counsel	0	0	0	0	0	0	0	0	0	0
Office of the Director of National Intelligence	213	0	269	269	157	0	0	0	0	0
Overseas Private Investment Corporation	0	0	0	0	0	0	0	0	0	0
Peace Corps	367	0	367	367	0	934	934	0	0	934
Pension Benefit Guaranty Corporation	183.18	226	395.75	361.8	34.33	927.17	960	0	960	0
Postal Regulatory Commission	0	0	0	0	0	0	0	0	0	0
Presidio Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Railroad Retirement Board	0	0	0	0	0	0	0	0	0	0
Securities and Exchange Commission	245	0	334.5	334.5	66	498	498	0	0	498
Selective Service System	0	0	0	0	0	0	0	0	0	0
Small Business Administration	123.67	0	329	329	21	581	581	0	581	0
Smithsonian Institution	135.56	0	213.2	213.2	38.5	662.33	662.33	0	662.33	0
Social Security Administration	353.37	0	459.63	459.63	58.45	784.74	761.32	931.75	767.72	611.67
Tennessee Valley Authority	192.32	302	232.79	236.25	16.6	546.36	546.36	0	546.36	0
Trade and Development Agency	0	0	0	0	0	0	0	0	0	0
U.S. Postal Service	141.86	0	277.48	277.48	47.88	632.62	630.97	966.32	609.43	710.28
Utah Reclamation Mitigation and Conservation Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Valles Caldera Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Cabinet Level Subtotal	283.71	630.11	460.16	462.61	73.33	704.84	700.41	942.89	686.55	729.95
Midsize Agencies Subtotal	341.82	837.5	467.81	470.94	67.29	762.64	747.37	931.75	751.35	616.73
Small Agencies Subtotal	265.27	234	413.09	407.67	91.22	994.49	1,000.28	1,745.00	990.31	871.67
Micro Agencies Subtotal	15	0	0	0	15	934	934	0	0	934
Government-wide	286.02	623.71	459.86	462.21	73.38	713.45	708.24	949	695.55	723.97

NRF = No Report Filed

Table B-18 FY 2012 Average Processing Days (APD) Final Orders (FOs) Not Fully Implementing (NFI) AJ Decisions

Agency or Department	APD All Final Orders (FOs) of AJ Decisions	APD All FOs Not Fully Implementing (NFI) AJ Merit Decisions	APD FOs NFI AJ Merit Decisions Finding Discrimination	APD Agency Appeal of Finding in AJ Merit Decisions	APD Agency Appeal of Remedy in AJ Merit Decisions	APD Agency Appeal of Remedy and Finding in AJ Merit Decisions	APD FOs NFI AJ Merit Decisions Finding No Discrimination	APD FOs NFI AJ Dismissals
Advisory Council on Historic Preservation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
African Development Foundation	934	0	0	0	0	0	0	0
Agency for International Development	1,525.00	0	0	0	0	0	0	0
American Battle Monuments Commission	0	0	0	0	0	0	0	0
Appalachian Regional Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Architectural and Transportation Barriers Compliance Board	0	0	0	0	0	0	0	0
Arctic Research Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Armed Forces Retirement Home	0	0	0	0	0	0	0	0
Barry Goldwater Scholarship and Excellence in Education Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Broadcasting Board of Governors	939	0	0	0	0	0	0	0
Central Intelligence Agency	1,186.50	0	0	0	0	0	0	0
Chemical Safety and Hazard Investigation Board	0	0	0	0	0	0	0	0
Christopher Columbus Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission of Fine Arts	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission on Civil Rights	0	0	0	0	0	0	0	0
Committee for Purchase from People Who Are Blind or Severely Disabled	0	0	0	0	0	0	0	0
Commodity Futures Trading Commission	0	0	0	0	0	0	0	0
Consumer Financial Protection Bureau	0	0	0	0	0	0	0	0
Consumer Product Safety Commission	0	0	0	0	0	0	0	0
Corporation for National and Community Service	0	0	0	0	0	0	0	0
Court Services and Offender Supervision Agency for the District of Columbia	901.8	0	0	0	0	0	0	0
Defense Army and Air Force Exchange	886.31	0	0	0	0	0	0	0
Defense Commissary Agency	728.11	0	0	0	0	0	0	0
Defense Contract Audit Agency	503.33	0	0	0	0	0	0	0
Defense Contract Management Agency	0	0	0	0	0	0	0	0

Table B-18 FY 2012 Average Processing Days (APD) Final Orders (FOs) Not Fully Implementing (NFI) AJ Decisions

Agency or Department	APD All Final Orders (FOs) of AJ Decisions	APD All FOs Not Fully Implementing (NFI) AJ Merit Decisions	APD FOs NFI AJ Merit Decisions Finding Discrimination	APD Agency Appeal of Finding in AJ Merit Decisions	APD Agency Appeal of Remedy in AJ Merit Decisions	APD Agency Appeal of Remedy and Finding in AJ Merit Decisions	APD FOs NFI AJ Merit Decisions Finding No Discrimination	APD FOs NFI AJ Dismissals
Defense Finance and Accounting Service	697.83	0	0	0	0	0	0	0
Defense Human Resources Activity	0	0	0	0	0	0	0	0
Defense Information Systems Agency	0	0	0	0	0	0	0	0
Defense Intelligence Agency	1,004.00	1,487.00	1,487.00	0	0	1,487.00	0	0
Defense Joint Task Force National Capital Region Medical	0	0	0	0	0	0	0	0
Defense Logistics Agency	682.26	0	0	0	0	0	0	0
Defense Media Activity	0	0	0	0	0	0	0	0
Defense Missile Defense Agency	0	0	0	0	0	0	0	0
Defense National Geospatial-Intelligence Agency	684.67	0	0	0	0	0	0	0
Defense National Guard Bureau	0	0	0	0	0	0	0	0
Defense National Security Agency	1,268.60	1,776.00	1,776.00	0	0	1,776.00	0	0
Defense Nuclear Facilities Safety Board	0	0	0	0	0	0	0	0
Defense Office of the Inspector General	0	0	0	0	0	0	0	0
Defense Office of the Secretary - Wash. Hqtrs. Services	1,174.14	0	0	0	0	0	0	0
Defense Security Service	0	0	0	0	0	0	0	0
Defense Technical Information Center	0	0	0	0	0	0	0	0
Defense Threat Reduction Agency	0	0	0	0	0	0	0	0
Defense TRICARE Management Activity	0	0	0	0	0	0	0	0
Defense Uniformed Services University	0	0	0	0	0	0	0	0
Department of Agriculture	849.15	0	0	0	0	0	0	0
Department of Commerce	644.96	625.5	795	0	795	0	456	0
Department of Defense Education Activity	843.17	0	0	0	0	0	0	0
Department of Education	1,057.08	0	0	0	0	0	0	0
Department of Energy	638.67	0	0	0	0	0	0	0
Department of Health and Human Services	711.14	0	0	0	0	0	0	0
Department of Homeland Security	743.04	717.33	717.33	0	544	804	0	0

Table B-18 FY 2012 Average Processing Days (APD) Final Orders (FOs) Not Fully Implementing (NFI) AJ Decisions

Agency or Department	APD All Final Orders (FOs) of AJ Decisions	APD All FOs Not Fully Implementing (NFI) AJ Merit Decisions	APD FOs NFI AJ Merit Decisions Finding Discrimination	APD Agency Appeal of Finding in AJ Merit Decisions	APD Agency Appeal of Remedy in AJ Merit Decisions	APD Agency Appeal of Remedy and Finding in AJ Merit Decisions	APD FOs NFI AJ Merit Decisions Finding No Discrimination	APD FOs NFI AJ Dismissals
Department of Housing and Urban Development	747.73	0	0	0	0	0	0	0
Department of Justice	759.65	963.25	1,100.67	901	1,467.00	934	551	0
Department of Labor	791.15	0	0	0	0	0	0	0
Department of State	700.64	1,766.00	1,766.00	0	0	1,766.00	0	0
Department of the Air Force	711	386	0	0	0	0	386	0
Department of the Army	744.1	1,150.75	1,027.33	0	1,050.00	1,016.00	1,521.00	0
Department of the Interior	841.93	0	0	0	0	0	0	0
Department of the Navy	928.68	1,165.00	1,165.00	0	1,165.00	0	0	0
Department of the Treasury	801.19	0	0	0	0	0	0	0
Department of Transportation	675.02	0	0	0	0	0	0	0
Department of Veterans Affairs	678.38	1,424.33	1,424.33	548	2,400.00	1,325.00	0	0
Election Assistance Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Environmental Protection Agency	866.27	0	0	0	0	0	0	0
Equal Employment Opportunity Commission	601	0	0	0	0	0	0	0
Export-Import Bank of the US	0	0	0	0	0	0	0	0
Farm Credit Administration	0	0	0	0	0	0	0	0
Farm Credit System Insurance Corporation	0	0	0	0	0	0	0	0
Federal Communications Commission	0	0	0	0	0	0	0	0
Federal Deposit Insurance Corporation	585	0	0	0	0	0	0	0
Federal Election Commission	0	0	0	0	0	0	0	0
Federal Energy Regulatory Commission	0	0	0	0	0	0	0	0
Federal Financial Institutions Examination Council	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Housing Finance Agency	0	0	0	0	0	0	0	0
Federal Labor Relations Authority	0	0	0	0	0	0	0	0
Federal Maritime Commission	0	0	0	0	0	0	0	0
Federal Mediation and Conciliation Service	0	0	0	0	0	0	0	0
Federal Mine Safety & Health Review Commission	0	0	0	0	0	0	0	0
Federal Reserve System--Board of Governors	792	0	0	0	0	0	0	0

Table B-18 FY 2012 Average Processing Days (APD) Final Orders (FOs) Not Fully Implementing (NFI) AJ Decisions

Agency or Department	APD All Final Orders (FOs) of AJ Decisions	APD All FOs Not Fully Implementing (NFI) AJ Merit Decisions	APD FOs NFI AJ Merit Decisions Finding Discrimination	APD Agency Appeal of Finding in AJ Merit Decisions	APD Agency Appeal of Remedy in AJ Merit Decisions	APD Agency Appeal of Remedy and Finding in AJ Merit Decisions	APD FOs NFI AJ Merit Decisions Finding No Discrimination	APD FOs NFI AJ Dismissals
Federal Retirement Thrift Investment Board	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Trade Commission	1,115.00	0	0	0	0	0	0	0
General Services Administration	740.43	0	0	0	0	0	0	0
Government Printing Office	1,000.00	0	0	0	0	0	0	0
Harry S. Truman Scholarship Foundation	0	0	0	0	0	0	0	0
Holocaust Memorial Museum U.S.	0	0	0	0	0	0	0	0
Institute of Museum and Library Services	0	0	0	0	0	0	0	0
Inter-American Foundation	0	0	0	0	0	0	0	0
International Boundary and Water Commission	0	0	0	0	0	0	0	0
International Joint Commission: US and Canada	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
International Trade Commission	0	0	0	0	0	0	0	0
James Madison Memorial Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Japan-United States Friendship Commission	0	0	0	0	0	0	0	0
John F. Kennedy Center for the Performing Arts	0	0	0	0	0	0	0	0
Marine Mammal Commission	0	0	0	0	0	0	0	0
Merit Systems Protection Board	0	0	0	0	0	0	0	0
Millennium Challenge Corporation	0	0	0	0	0	0	0	0
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Aeronautics and Space Administration	1,214.40	0	0	0	0	0	0	0
National Archives and Records Administration	1,161.33	0	0	0	0	0	0	0
National Capital Planning Commission	0	0	0	0	0	0	0	0
National Council on Disability	0	0	0	0	0	0	0	0
National Credit Union Administration	0	0	0	0	0	0	0	0
National Endowment for the Arts	0	0	0	0	0	0	0	0
National Endowment for the Humanities	0	0	0	0	0	0	0	0
National Foundation on the Arts & the Humanities	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Gallery of Art	0	0	0	0	0	0	0	0

Table B-18 FY 2012 Average Processing Days (APD) Final Orders (FOs) Not Fully Implementing (NFI) AJ Decisions

Agency or Department	APD All Final Orders (FOs) of AJ Decisions	APD All FOs Not Fully Implementing (NFI) AJ Merit Decisions	APD FOs NFI AJ Merit Decisions Finding Discrimination	APD Agency Appeal of Finding in AJ Merit Decisions	APD Agency Appeal of Remedy in AJ Merit Decisions	APD Agency Appeal of Remedy and Finding in AJ Merit Decisions	APD FOs NFI AJ Merit Decisions Finding No Discrimination	APD FOs NFI AJ Dismissals
National Indian Gaming Commission	0	0	0	0	0	0	0	0
National Labor Relations Board	554	0	0	0	0	0	0	0
National Mediation Board	0	0	0	0	0	0	0	0
National Reconnaissance Office	1,094.00	0	0	0	0	0	0	0
National Science Foundation	0	0	0	0	0	0	0	0
National Transportation Safety Board	0	0	0	0	0	0	0	0
Navajo and Hopi Indian Relocation Commission	0	0	0	0	0	0	0	0
Nuclear Regulatory Commission	632	0	0	0	0	0	0	0
Nuclear Waste Technical Review Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Occupational Safety & Health Review Commission	0	0	0	0	0	0	0	0
Office of Government Ethics	0	0	0	0	0	0	0	0
Office of Personnel Management	134.8	0	0	0	0	0	0	0
Office of Special Counsel	0	0	0	0	0	0	0	0
Office of the Director of National Intelligence	0	0	0	0	0	0	0	0
Overseas Private Investment Corporation	0	0	0	0	0	0	0	0
Peace Corps	934	0	0	0	0	0	0	0
Pension Benefit Guaranty Corporation	927.17	763	763	0	0	763	0	0
Postal Regulatory Commission	0	0	0	0	0	0	0	0
Presidio Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Railroad Retirement Board	0	0	0	0	0	0	0	0
Securities and Exchange Commission	498	0	0	0	0	0	0	0
Selective Service System	0	0	0	0	0	0	0	0
Small Business Administration	581	0	0	0	0	0	0	0
Smithsonian Institution	662.33	0	0	0	0	0	0	0
Social Security Administration	784.74	1,127.25	1,127.25	0	0	1,127.25	0	0
Tennessee Valley Authority	546.36	0	0	0	0	0	0	0
Trade and Development Agency	0	0	0	0	0	0	0	0
U.S. Postal Service	632.62	1,106.33	1,106.33	0	1,046.00	1,136.50	0	0

Table B-18 FY 2012 Average Processing Days (APD) Final Orders (FOs) Not Fully Implementing (NFI) AJ Decisions

Agency or Department	APD All Final Orders (FOs) of AJ Decisions	APD All FOs Not Fully Implementing (NFI) AJ Merit Decisions	APD FOs NFI AJ Merit Decisions Finding Discrimination	APD Agency Appeal of Finding in AJ Merit Decisions	APD Agency Appeal of Remedy in AJ Merit Decisions	APD Agency Appeal of Remedy and Finding in AJ Merit Decisions	APD FOs NFI AJ Merit Decisions Finding No Discrimination	APD FOs NFI AJ Dismissals
Utah Reclamation Mitigation and Conservation Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Valles Caldera Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Cabinet Level Subtotal	704.84	1,126.69	1,199.09	724.5	1,209.57	1,266.46	728.5	0
Midsize Agencies Subtotal	762.64	1,127.25	1,127.25	0	0	1,127.25	0	0
Small Agencies Subtotal	994.49	763	763	0	0	763	0	0
Micro Agencies Subtotal	934	0	0	0	0	0	0	0
Government-wide	713.45	1,116.43	1,166.48	724.5	1,209.57	1,192.95	728.5	0

NRF = No Report Filed

Table B-19 FY 2012 Total Complaint Closures Accepted/Participated in ADR

Agency or Department	Total Complaint Closures	Number Complaint Closures Offered ADR	% Complaint Closures Offered ADR (Offer Rate)	Number Offers Rejected by Complainant	Total Complaint Closures Accepted / Participated in ADR Program	% Complaint Closures Accepted into ADR Program (Participation Rate)
Advisory Council on Historic Preservation	NRF	NRF	NRF	NRF	NRF	NRF
African Development Foundation	3	0	0.00%	0	0	0.00%
Agency for International Development	16	1	6.25%	1	0	0.00%
American Battle Monuments Commission	0	0	0.00%	0	0	0.00%
Appalachian Regional Commission	NRF	NRF	NRF	NRF	NRF	NRF
Architectural and Transportation Barriers Compliance Board	0	0	0.00%	0	0	0.00%
Arctic Research Commission	NRF	NRF	NRF	NRF	NRF	NRF
Armed Forces Retirement Home	4	0	0.00%	0	0	0.00%
Barry Goldwater Scholarship and Excellence in Education Foundation	NRF	NRF	NRF	NRF	NRF	NRF
Broadcasting Board of Governors	14	14	100.00%	14	0	0.00%
Central Intelligence Agency	39	0	0.00%	0	0	0.00%
Chemical Safety and Hazard Investigation Board	0	0	0.00%	0	0	0.00%
Christopher Columbus Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF
Commission of Fine Arts	NRF	NRF	NRF	NRF	NRF	NRF
Commission on Civil Rights	0	0	0.00%	0	0	0.00%
Committee for Purchase from People Who Are Blind or Severely Disabled	0	0	0.00%	0	0	0.00%
Commodity Futures Trading Commission	2	0	0.00%	0	0	0.00%
Consumer Financial Protection Bureau	7	6	85.71%	5	1	14.29%
Consumer Product Safety Commission	2	0	0.00%	0	0	0.00%
Corporation for National and Community Service	3	0	0.00%	0	0	0.00%
Court Services and Offender Supervision Agency for the District of Columbia	15	0	0.00%	0	0	0.00%
Defense Army and Air Force Exchange	89	80	89.89%	66	14	15.73%
Defense Commissary Agency	120	22	18.33%	3	19	15.83%
Defense Contract Audit Agency	32	9	28.13%	0	9	28.13%
Defense Contract Management Agency	38	7	18.42%	0	7	18.42%

Table B-19 FY 2012 Total Complaint Closures Accepted/Participated in ADR						
Agency or Department	**Total Complaint Closures**	**Number Complaint Closures Offered ADR**	**% Complaint Closures Offered ADR (Offer Rate)**	**Number Offers Rejected by Complainant**	**Total Complaint Closures Accepted / Participated in ADR Program**	**% Complaint Closures Accepted into ADR Program (Participation Rate)**
Defense Finance and Accounting Service	39	0	0.00%	0	0	0.00%
Defense Human Resources Activity	5	5	100.00%	1	4	80.00%
Defense Information Systems Agency	8	0	0.00%	0	0	0.00%
Defense Intelligence Agency	34	4	11.76%	4	0	0.00%
Defense Joint Task Force National Capital Region Medical	7	6	85.71%	0	6	85.71%
Defense Logistics Agency	136	35	25.74%	6	29	21.32%
Defense Media Activity	3	2	66.67%	0	2	66.67%
Defense Missile Defense Agency	0	0	0.00%	0	0	0.00%
Defense National Geospatial-Intelligence Agency	20	0	0.00%	0	0	0.00%
Defense National Guard Bureau	33	10	30.30%	5	5	15.15%
Defense National Security Agency	17	3	17.65%	1	2	11.76%
Defense Nuclear Facilities Safety Board	0	0	0.00%	0	0	0.00%
Defense Office of the Inspector General	3	0	0.00%	0	0	0.00%
Defense Office of the Secretary - Wash. Hqtrs. Services	45	2	4.44%	0	2	4.44%
Defense Security Service	6	0	0.00%	0	0	0.00%
Defense Technical Information Center	1	0	0.00%	0	0	0.00%
Defense Threat Reduction Agency	8	0	0.00%	0	0	0.00%
Defense TRICARE Management Activity	7	5	71.43%	0	5	71.43%
Defense Uniformed Services University	0	0	0.00%	0	0	0.00%
Department of Agriculture	453	147	32.45%	71	76	16.78%
Department of Commerce	432	13	3.01%	0	13	3.01%
Department of Defense Education Activity	55	9	16.36%	4	5	9.09%
Department of Education	46	21	45.65%	19	2	4.35%
Department of Energy	63	35	55.56%	26	9	14.29%
Department of Health and Human Services	409	105	25.67%	65	40	9.78%
Department of Homeland Security	1,097	291	26.53%	232	58	5.29%
Department of Housing and Urban Development	73	63	86.30%	58	5	6.85%

Table B-19 FY 2012 Total Complaint Closures Accepted/Participated in ADR						
Agency or Department	**Total Complaint Closures**	**Number Complaint Closures Offered ADR**	**% Complaint Closures Offered ADR (Offer Rate)**	**Number Offers Rejected by Complainant**	**Total Complaint Closures Accepted / Participated in ADR Program**	**% Complaint Closures Accepted into ADR Program (Participation Rate)**
Department of Justice	857	117	13.65%	61	56	6.53%
Department of Labor	134	134	100.00%	85	49	36.57%
Department of State	110	15	13.64%	0	15	13.64%
Department of the Air Force	500	244	48.80%	158	86	17.20%
Department of the Army	1,116	254	22.76%	85	169	15.14%
Department of the Interior	307	196	63.84%	168	28	9.12%
Department of the Navy	904	29	3.21%	9	20	2.21%
Department of the Treasury	407	330	81.08%	289	41	10.07%
Department of Transportation	335	7	2.09%	0	7	2.09%
Department of Veterans Affairs	2,123	96	4.52%	1	95	4.47%
Election Assistance Commission	NRF	NRF	NRF	NRF	NRF	NRF
Environmental Protection Agency	49	1	2.04%	0	1	2.04%
Equal Employment Opportunity Commission	20	2	10.00%	0	2	10.00%
Export-Import Bank of the US	1	1	100.00%	1	0	0.00%
Farm Credit Administration	0	0	0.00%	0	0	0.00%
Farm Credit System Insurance Corporation	0	0	0.00%	0	0	0.00%
Federal Communications Commission	2	0	0.00%	0	0	0.00%
Federal Deposit Insurance Corporation	42	17	40.48%	9	8	19.05%
Federal Election Commission	0	0	0.00%	0	0	0.00%
Federal Energy Regulatory Commission	10	3	30.00%	0	3	30.00%
Federal Financial Institutions Examination Council	NRF	NRF	NRF	NRF	NRF	NRF
Federal Housing Finance Agency	6	5	83.33%	3	2	33.33%
Federal Labor Relations Authority	0	0	0.00%	0	0	0.00%
Federal Maritime Commission	0	0	0.00%	0	0	0.00%
Federal Mediation and Conciliation Service	2	0	0.00%	0	0	0.00%
Federal Mine Safety& Health Review Commission	0	0	0.00%	0	0	0.00%
Federal Reserve System--Board of Governors	6	0	0.00%	0	0	0.00%
Federal Retirement Thrift Investment Board	NRF	NRF	NRF	NRF	NRF	NRF
Federal Trade Commission	1	0	0.00%	0	0	0.00%

Table B-19 FY 2012 Total Complaint Closures Accepted/Participated in ADR						
Agency or Department	**Total Complaint Closures**	**Number Complaint Closures Offered ADR**	**% Complaint Closures Offered ADR (Offer Rate)**	**Number Offers Rejected by Complainant**	**Total Complaint Closures Accepted / Participated in ADR Program**	**% Complaint Closures Accepted into ADR Program (Participation Rate)**
General Services Administration	85	3	3.53%	1	2	2.35%
Government Printing Office	29	0	0.00%	0	0	0.00%
Harry S. Truman Scholarship Foundation	0	0	0.00%	0	0	0.00%
Holocaust Memorial Museum U.S.	0	0	0.00%	0	0	0.00%
Institute of Museum and Library Services	0	0	0.00%	0	0	0.00%
Inter-American Foundation	0	0	0.00%	0	0	0.00%
International Boundary and Water Commission	0	0	0.00%	0	0	0.00%
International Joint Commission: US and Canada	NRF	NRF	NRF	NRF	NRF	NRF
International Trade Commission	1	0	0.00%	0	0	0.00%
James Madison Memorial Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF
Japan-United States Friendship Commission	0	0	0.00%	0	0	0.00%
John F. Kennedy Center for the Performing Arts	0	0	0.00%	0	0	0.00%
Marine Mammal Commission	0	0	0.00%	0	0	0.00%
Merit Systems Protection Board	1	1	100.00%	1	0	0.00%
Millennium Challenge Corporation	0	0	0.00%	0	0	0.00%
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation	NRF	NRF	NRF	NRF	NRF	NRF
National Aeronautics and Space Administration	38	8	21.05%	5	3	7.89%
National Archives and Records Administration	11	0	0.00%	0	0	0.00%
National Capital Planning Commission	0	0	0.00%	0	0	0.00%
National Council on Disability	0	0	0.00%	0	0	0.00%
National Credit Union Administration	7	0	0.00%	0	0	0.00%
National Endowment for the Arts	3	0	0.00%	0	0	0.00%
National Endowment for the Humanities	0	0	0.00%	0	0	0.00%
National Foundation on the Arts & the Humanities	NRF	NRF	NRF	NRF	NRF	NRF
National Gallery of Art	6	0	0.00%	0	0	0.00%
National Indian Gaming Commission	1	0	0.00%	0	0	0.00%
National Labor Relations Board	8	8	100.00%	7	1	12.50%
National Mediation Board	0	0	0.00%	0	0	0.00%

Table B-19 FY 2012 Total Complaint Closures Accepted/Participated in ADR						
Agency or Department	**Total Complaint Closures**	**Number Complaint Closures Offered ADR**	**% Complaint Closures Offered ADR (Offer Rate)**	**Number Offers Rejected by Complainant**	**Total Complaint Closures Accepted / Participated in ADR Program**	**% Complaint Closures Accepted into ADR Program (Participation Rate)**
National Reconnaissance Office	7	3	42.86%	2	1	14.29%
National Science Foundation	6	2	33.33%	0	2	33.33%
National Transportation Safety Board	2	0	0.00%	0	0	0.00%
Navajo and Hopi Indian Relocation Commission	0	0	0.00%	0	0	0.00%
Nuclear Regulatory Commission	16	16	100.00%	15	1	6.25%
Nuclear Waste Technical Review Commission	NRF	NRF	NRF	NRF	NRF	NRF
Occupational Safety & Health Review Commission	0	0	0.00%	0	0	0.00%
Office of Government Ethics	2	2	100.00%	2	0	0.00%
Office of Personnel Management	28	0	0.00%	0	0	0.00%
Office of Special Counsel	0	0	0.00%	0	0	0.00%
Office of the Director of National Intelligence	4	0	0.00%	0	0	0.00%
Overseas Private Investment Corporation	0	0	0.00%	0	0	0.00%
Peace Corps	4	4	100.00%	4	0	0.00%
Pension Benefit Guaranty Corporation	20	13	65.00%	13	0	0.00%
Postal Regulatory Commission	0	0	0.00%	0	0	0.00%
Presidio Trust	NRF	NRF	NRF	NRF	NRF	NRF
Railroad Retirement Board	1	0	0.00%	0	0	0.00%
Securities and Exchange Commission	4	0	0.00%	0	0	0.00%
Selective Service System	2	0	0.00%	0	0	0.00%
Small Business Administration	38	1	2.63%	0	1	2.63%
Smithsonian Institution	15	14	93.33%	7	7	46.67%
Social Security Administration	414	338	81.64%	302	36	8.70%
Tennessee Valley Authority	58	58	100.00%	58	0	0.00%
Trade and Development Agency	0	0	0.00%	0	0	0.00%
U.S. Postal Service	4,579	376	8.21%	57	319	6.97%

Table B-19 FY 2012 Total Complaint Closures Accepted/Participated in ADR						
Agency or Department	**Total Complaint Closures**	**Number Complaint Closures Offered ADR**	**% Complaint Closures Offered ADR (Offer Rate)**	**Number Offers Rejected by Complainant**	**Total Complaint Closures Accepted / Participated in ADR Program**	**% Complaint Closures Accepted into ADR Program (Participation Rate)**
Utah Reclamation Mitigation and Conservation Commission	NRF	NRF	NRF	NRF	NRF	NRF
Valles Caldera Trust	NRF	NRF	NRF	NRF	NRF	NRF
Cabinet Level Subtotal	14,651	2,672	18.24%	1,474	1,197	8.17%
Midsize Agencies Subtotal	774	446	57.62%	387	59	7.62%
Small Agencies Subtotal	276	73	26.45%	61	12	4.35%
Micro Agencies Subtotal	5	2	40.00%	2	0	0.00%
Government-wide	15,706	3,193	20.33%	1,924	1,268	8.07%

NRF = No Report Filed

Table B-20 FY 2012 ADR Complaint Resolutions (Formal Phase)							
Agency Name	**Number ADR Closures**	**Number ADR Settlements**	**% ADR Settlements**	**Number ADR Withdrawals**	**% ADR Withdrawals**	**Total Number ADR Resolutions**	**% ADR Resolutions (Resolution Rate)**
Advisory Council on Historic Preservation	NRF	NRF	NRF	NRF	NRF	NRF	NRF
African Development Foundation	0	0	0.00%	0	0.00%	0	0.00%
Agency for International Development	0	0	0.00%	0	0.00%	0	0.00%
American Battle Monuments Commission	0	0	0.00%	0	0.00%	0	0.00%
Appalachian Regional Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Architectural and Transportation Barriers Compliance Board	0	0	0.00%	0	0.00%	0	0.00%
Arctic Research Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Armed Forces Retirement Home	0	0	0.00%	0	0.00%	0	0.00%
Barry Goldwater Scholarship and Excellence in Education Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Broadcasting Board of Governors	0	0	0.00%	0	0.00%	0	0.00%
Central Intelligence Agency	0	0	0.00%	0	0.00%	0	0.00%
Chemical Safety and Hazard Investigation Board	0	0	0.00%	0	0.00%	0	0.00%
Christopher Columbus Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission of Fine Arts	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission on Civil Rights	0	0	0.00%	0	0.00%	0	0.00%
Committee for Purchase from People Who Are Blind or Severely Disabled	0	0	0.00%	0	0.00%	0	0.00%
Commodity Futures Trading Commission	0	0	0.00%	0	0.00%	0	0.00%
Consumer Financial Protection Bureau	1	0	0.00%	0	0.00%	0	0.00%
Consumer Product Safety Commission	0	0	0.00%	0	0.00%	0	0.00%
Corporation for National and Community Service	0	0	0.00%	0	0.00%	0	0.00%
Court Services and Offender Supervision Agency for the District of Columbia	0	0	0.00%	0	0.00%	0	0.00%
Defense Army and Air Force Exchange	14	11	78.57%	3	21.43%	14	100.00%
Defense Commissary Agency	19	9	47.37%	2	10.53%	11	57.89%
Defense Contract Audit Agency	9	8	88.89%	0	0.00%	8	88.89%
Defense Contract Management Agency	7	5	71.43%	0	0.00%	5	71.43%
Defense Finance and Accounting Service	0	0	0.00%	0	0.00%	0	0.00%
Defense Human Resources Activity	4	1	25.00%	3	75.00%	4	100.00%

Table B-20 FY 2012 ADR Complaint Resolutions (Formal Phase)

Agency Name	Number ADR Closures	Number ADR Settlements	% ADR Settlements	Number ADR Withdrawals	% ADR Withdrawals	Total Number ADR Resolutions	% ADR Resolutions (Resolution Rate)
Defense Information Systems Agency	0	0	0.00%	0	0.00%	0	0.00%
Defense Intelligence Agency	0	0	0.00%	0	0.00%	0	0.00%
Defense Joint Task Force National Capital Region Medical	6	0	0.00%	0	0.00%	0	0.00%
Defense Logistics Agency	29	16	55.17%	0	0.00%	16	55.17%
Defense Media Activity	2	2	100.00%	0	0.00%	2	100.00%
Defense Missile Defense Agency	0	0	0.00%	0	0.00%	0	0.00%
Defense National Geospatial-Intelligence Agency	0	0	0.00%	0	0.00%	0	0.00%
Defense National Guard Bureau	5	5	100.00%	0	0.00%	5	100.00%
Defense National Security Agency	2	0	0.00%	0	0.00%	0	0.00%
Defense Nuclear Facilities Safety Board	0	0	0.00%	0	0.00%	0	0.00%
Defense Office of the Inspector General	0	0	0.00%	0	0.00%	0	0.00%
Defense Office of the Secretary - Wash. Hqtrs. Services	2	1	50.00%	0	0.00%	1	50.00%
Defense Security Service	0	0	0.00%	0	0.00%	0	0.00%
Defense Technical Information Center	0	0	0.00%	0	0.00%	0	0.00%
Defense Threat Reduction Agency	0	0	0.00%	0	0.00%	0	0.00%
Defense TRICARE Management Activity	5	1	20.00%	0	0.00%	1	20.00%
Defense Uniformed Services University	0	0	0.00%	0	0.00%	0	0.00%
Department of Agriculture	76	28	36.84%	0	0.00%	28	36.84%
Department of Commerce	13	4	30.77%	0	0.00%	4	30.77%
Department of Defense Education Activity	5	1	20.00%	0	0.00%	1	20.00%
Department of Education	2	0	0.00%	0	0.00%	0	0.00%
Department of Energy	9	6	66.67%	0	0.00%	6	66.67%
Department of Health and Human Services	40	15	37.50%	0	0.00%	15	37.50%
Department of Homeland Security	58	18	31.03%	3	5.17%	21	36.21%
Department of Housing and Urban Development	5	3	60.00%	0	0.00%	3	60.00%
Department of Justice	56	36	64.29%	1	1.79%	37	66.07%
Department of Labor	49	49	100.00%	0	0.00%	49	100.00%
Department of State	15	8	53.33%	0	0.00%	8	53.33%
Department of the Air Force	86	61	70.93%	0	0.00%	61	70.93%

Table B-20 FY 2012 ADR Complaint Resolutions (Formal Phase)

Agency Name	Number ADR Closures	Number ADR Settlements	% ADR Settlements	Number ADR Withdrawals	% ADR Withdrawals	Total Number ADR Resolutions	% ADR Resolutions (Resolution Rate)
Department of the Army	169	113	66.86%	6	3.55%	119	70.41%
Department of the Interior	28	10	35.71%	0	0.00%	10	35.71%
Department of the Navy	20	4	20.00%	0	0.00%	4	20.00%
Department of the Treasury	41	16	39.02%	1	2.44%	17	41.46%
Department of Transportation	7	1	14.29%	0	0.00%	1	14.29%
Department of Veterans Affairs	95	50	52.63%	3	3.16%	53	55.79%
Election Assistance Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Environmental Protection Agency	1	0	0.00%	0	0.00%	0	0.00%
Equal Employment Opportunity Commission	2	2	100.00%	0	0.00%	2	100.00%
Export-Import Bank of the US	0	0	0.00%	0	0.00%	0	0.00%
Farm Credit Administration	0	0	0.00%	0	0.00%	0	0.00%
Farm Credit System Insurance Corporation	0	0	0.00%	0	0.00%	0	0.00%
Federal Communications Commission	0	0	0.00%	0	0.00%	0	0.00%
Federal Deposit Insurance Corporation	8	5	62.50%	0	0.00%	5	62.50%
Federal Election Commission	0	0	0.00%	0	0.00%	0	0.00%
Federal Energy Regulatory Commission	3	1	33.33%	0	0.00%	1	33.33%
Federal Financial Institutions Examination Council	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Housing Finance Agency	2	2	100.00%	0	0.00%	2	100.00%
Federal Labor Relations Authority	0	0	0.00%	0	0.00%	0	0.00%
Federal Maritime Commission	0	0	0.00%	0	0.00%	0	0.00%
Federal Mediation and Conciliation Service	0	0	0.00%	0	0.00%	0	0.00%
Federal Mine Safety & Health Review Comm	0	0	0.00%	0	0.00%	0	0.00%
Federal Reserve System--Board of Governors	0	0	0.00%	0	0.00%	0	0.00%
Federal Retirement Thrift Investment Board	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Trade Commission	0	0	0.00%	0	0.00%	0	0.00%
General Services Administration	2	0	0.00%	0	0.00%	0	0.00%
Government Printing Office	0	0	0.00%	0	0.00%	0	0.00%
Harry S. Truman Scholarship Foundation	0	0	0.00%	0	0.00%	0	0.00%
Holocaust Memorial Museum U.S.	0	0	0.00%	0	0.00%	0	0.00%
Institute of Museum and Library Services	0	0	0.00%	0	0.00%	0	0.00%
Inter-American Foundation	0	0	0.00%	0	0.00%	0	0.00%

Table B-20 FY 2012 ADR Complaint Resolutions (Formal Phase)

Agency Name	Number ADR Closures	Number ADR Settlements	% ADR Settlements	Number ADR Withdrawals	% ADR Withdrawals	Total Number ADR Resolutions	% ADR Resolutions (Resolution Rate)
International Boundary and Water Commission	0	0	0.00%	0	0.00%	0	0.00%
International Joint Commission: US and Canada	NRF	NRF	NRF	NRF	NRF	NRF	NRF
International Trade Commission	0	0	0.00%	0	0.00%	0	0.00%
James Madison Memorial Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Japan-United States Friendship Commission	0	0	0.00%	0	0.00%	0	0.00%
John F. Kennedy Center for the Performing Arts	0	0	0.00%	0	0.00%	0	0.00%
Marine Mammal Commission	0	0	0.00%	0	0.00%	0	0.00%
Merit Systems Protection Board	0	0	0.00%	0	0.00%	0	0.00%
Millennium Challenge Corporation	0	0	0.00%	0	0.00%	0	0.00%
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Aeronautics and Space Administration	3	0	0.00%	0	0.00%	0	0.00%
National Archives and Records Administration	0	0	0.00%	0	0.00%	0	0.00%
National Capital Planning Commission	0	0	0.00%	0	0.00%	0	0.00%
National Council on Disability	0	0	0.00%	0	0.00%	0	0.00%
National Credit Union Administration	0	0	0.00%	0	0.00%	0	0.00%
National Endowment for the Arts	0	0	0.00%	0	0.00%	0	0.00%
National Endowment for the Humanities	0	0	0.00%	0	0.00%	0	0.00%
National Foundation on the Arts & the Humanities	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Gallery of Art	0	0	0.00%	0	0.00%	0	0.00%
National Indian Gaming Commission	0	0	0.00%	0	0.00%	0	0.00%
National Labor Relations Board	1	0	0.00%	1	100.00%	1	100.00%
National Mediation Board	0	0	0.00%	0	0.00%	0	0.00%
National Reconnaissance Office	1	1	100.00%	0	0.00%	1	100.00%
National Science Foundation	2	2	100.00%	0	0.00%	2	100.00%
National Transportation Safety Board	0	0	0.00%	0	0.00%	0	0.00%

Table B-20 FY 2012 ADR Complaint Resolutions (Formal Phase)							
Agency Name	**Number ADR Closures**	**Number ADR Settlements**	**% ADR Settlements**	**Number ADR Withdrawals**	**% ADR Withdrawals**	**Total Number ADR Resolutions**	**% ADR Resolutions (Resolution Rate)**
Navajo and Hopi Indian Relocation Commission	0	0	0.00%	0	0.00%	0	0.00%
Nuclear Regulatory Commission	1	1	100.00%	0	0.00%	1	100.00%
Nuclear Waste Technical Review Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Occupational Safety & Health Review Comm	0	0	0.00%	0	0.00%	0	0.00%
Office of Government Ethics	0	0	0.00%	0	0.00%	0	0.00%
Office of Personnel Management	0	0	0.00%	0	0.00%	0	0.00%
Office of Special Counsel	0	0	0.00%	0	0.00%	0	0.00%
Office of the Director of National Intelligence	0	0	0.00%	0	0.00%	0	0.00%
Overseas Private Investment Corporation	0	0	0.00%	0	0.00%	0	0.00%
Peace Corps	0	0	0.00%	0	0.00%	0	0.00%
Pension Benefit Guaranty Corporation	0	0	0.00%	0	0.00%	0	0.00%
Postal Regulatory Commission	0	0	0.00%	0	0.00%	0	0.00%
Presidio Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Railroad Retirement Board	0	0	0.00%	0	0.00%	0	0.00%
Securities and Exchange Commission	0	0	0.00%	0	0.00%	0	0.00%
Selective Service System	0	0	0.00%	0	0.00%	0	0.00%
Small Business Administration	1	0	0.00%	0	0.00%	0	0.00%
Smithsonian Institution	7	0	0.00%	0	0.00%	0	0.00%
Social Security Administration	36	2	5.56%	0	0.00%	2	5.56%
Tennessee Valley Authority	0	0	0.00%	0	0.00%	0	0.00%
Trade and Development Agency	0	0	0.00%	0	0.00%	0	0.00%
U.S. Postal Service	319	196	61.44%	6	1.88%	202	63.32%

Table B-20 FY 2012 ADR Complaint Resolutions (Formal Phase)							
Agency Name	**Number ADR Closures**	**Number ADR Settlements**	**% ADR Settlements**	**Number ADR Withdrawals**	**% ADR Withdrawals**	**Total Number ADR Resolutions**	**% ADR Resolutions (Resolution Rate)**
Utah Reclamation Mitigation & Conservation Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Valles Caldera Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Cabinet Level Subtotal	1,197	678	56.64%	28	2.34%	706	58.98%
Midsize Agencies Subtotal	59	7	11.86%	0	0.00%	7	11.86%
Small Agencies Subtotal	12	9	75.00%	1	8.33%	10	83.33%
Micro Agencies Subtotal	0	0	0.00%	0	0.00%	0	0.00%
Government-wide	1,268	694	54.73%	29	2.29%	723	57.02%

NRF = No Report Filed

Table B-21 FY 2012 Complaint Closures with Benefits

Agency or Department	Number Complaint Closures with Benefits	Number Complaint Closures w/ Monetary Benefits	Total Amount Back Pay / Front Pay	Total Amount Lump Sum Payments	Total Amount Compensatory Damages	Total Amount Attorney's Fees and Costs	Total Amount All Monetary Benefits	Average Monetary Benefits Per Complaint Closures With Benefits	Number Complaint Closures with Non-Monetary Benefits	% Complaint Closures with Non-Monetary Benefits
Advisory Council on Historic Preservation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
African Development Foundation	2	2	$0.00	$27,010.74	$0.00	$24,489.26	$51,500.00	$25,750.00	0	0.00%
Agency for International Development	4	4	$12,500.00	$144,000.00	$50,000.00	$46,524.17	$253,024.17	$63,256.04	0	0.00%
American Battle Monuments Commission	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Appalachian Regional Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Architectural and Transportation Barriers Compliance Board	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Arctic Research Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Armed Forces Retirement Home	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Barry Goldwater Scholarship and Excellence in Education Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Broadcasting Board of Governors	6	1	$0.00	$35,000.00	$0.00	$0.00	$35,000.00	$5,833.33	6	100.00%
Central Intelligence Agency	10	8	$10,700.00	$11,500.00	$198,000.00	$38,000.00	$258,200.00	$25,820.00	6	60.00%
Chemical Safety and Hazard Investigation Board	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Christopher Columbus Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission of Fine Arts	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission on Civil Rights	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Committee for Purchase from People Who Are Blind or Severely Disabled	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Commodity Futures Trading Commission	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Consumer Financial Protection Bureau	3	2	$0.00	$25,000.00	$0.00	$15,000.00	$40,000.00	$13,333.33	3	100.00%
Consumer Product Safety Commission	1	1	$0.00	$0.00	$0.00	$500.00	$500.00	$500.00	1	100.00%
Corporation for National and Community Service	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Court Services and Offender Supervision Agency for the District of Columbia	6	5	$0.00	$2,000.00	$20,409.77	$40,331.00	$62,740.77	$10,456.80	1	16.67%
Defense Army and Air Force Exchange	27	16	$8,564.25	$52,041.00	$55,250.00	$5,059.00	$120,914.25	$4,478.31	11	40.74%
Defense Commissary Agency	37	19	$63,700.00	$465,300.00	$76,586.00	$213,193.82	$818,779.82	$22,129.18	27	72.97%
Defense Contract Audit Agency	12	7	$0.00	$21,000.00	$850.00	$0.00	$21,850.00	$1,820.83	5	41.67%
Defense Contract Management Agency	9	4	$0.00	$12,500.00	$30,739.00	$25,000.00	$68,239.00	$7,582.11	5	55.56%
Defense Finance and Accounting Service	14	11	$49,450.65	$115,026.29	$2,000.00	$23,500.00	$189,976.94	$13,569.78	9	64.29%
Defense Human Resources Activity	1	1	$0.00	$20,000.00	$0.00	$0.00	$20,000.00	$20,000.00	0	0.00%
Defense Information Systems Agency	2	1	$0.00	$25,000.00	$0.00	$0.00	$25,000.00	$12,500.00	2	100.00%
Defense Intelligence Agency	6	5	$0.00	$145,000.00	$32,500.00	$95,800.00	$273,300.00	$45,550.00	1	16.67%
Defense Joint Task Force National Capital Region Medical	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Defense Logistics Agency	49	26	$4,753.00	$379,638.79	$0.00	$114,094.46	$498,486.25	$10,173.19	32	65.31%
Defense Media Activity	2	1	$0.00	$0.00	$35,000.00	$19,000.00	$54,000.00	$27,000.00	1	50.00%
Defense Missile Defense Agency	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Defense National Geospatial-Intelligence Agency	7	7	$0.00	$31,350.00	$0.00	$11,300.00	$42,650.00	$6,092.86	2	28.57%
Defense National Guard Bureau	6	2	$0.00	$551,948.43	$4,482.95	$2,580.50	$559,011.88	$93,168.65	4	66.67%

Table B-21 FY 2012 Complaint Closures with Benefits

Agency or Department	Number Complaint Closures with Benefits	Number Complaint Closures w/ Monetary Benefits	Total Amount Back Pay / Front Pay	Total Amount Lump Sum Payments	Total Amount Compensatory Damages	Total Amount Attorney's Fees and Costs	Total Amount All Monetary Benefits	Average Monetary Benefits Per Complaint Closures With Benefits	Number Complaint Closures with Non-Monetary Benefits	% Complaint Closures with Non-Monetary Benefits
Defense National Security Agency	4	4	$0.00	$20,000.00	$0.00	$8,100.00	$28,100.00	$7,025.00	1	25.00%
Defense Nuclear Facilities Safety Board	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Defense Office of the Inspector General	2	2	$0.00	$90,000.00	$7,500.00	$0.00	$97,500.00	$48,750.00	0	0.00%
Defense Office of the Secretary - Wash. Hqtrs. Services	12	8	$0.00	$135,500.00	$0.00	$152,618.75	$288,118.75	$24,009.90	10	83.33%
Defense Security Service	1	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	1	100.00%
Defense Technical Information Center	1	1	$0.00	$3,650.64	$0.00	$0.00	$3,650.64	$3,650.64	0	0.00%
Defense Threat Reduction Agency	4	3	$0.00	$41,000.00	$0.00	$80,000.00	$121,000.00	$30,250.00	4	100.00%
Defense TRICARE Management Activity	1	1	$0.00	$35,000.00	$0.00	$0.00	$35,000.00	$35,000.00	1	100.00%
Defense Uniformed Services University	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Department of Agriculture	181	138	$25,029.91	$1,466,933.17	$281,950.00	$1,120,659.76	$2,894,572.84	$15,992.12	139	76.80%
Department of Commerce	81	61	$197,480.67	$455,172.01	$89,000.00	$313,085.19	$1,054,737.87	$13,021.46	62	76.54%
Department of Defense Education Activity	23	17	$0.00	$177,804.24	$0.00	$212,800.00	$390,604.24	$16,982.79	15	65.22%
Department of Education	10	6	$0.00	$2,200.00	$0.00	$34,600.00	$36,800.00	$3,680.00	8	80.00%
Department of Energy	29	23	$98,367.00	$566,500.00	$0.00	$254,242.55	$919,109.55	$31,693.43	18	62.07%
Department of Health and Human Services	160	115	$132,918.53	$1,408,654.86	$303,000.00	$1,045,493.68	$2,890,067.07	$18,062.92	124	77.50%
Department of Homeland Security	254	133	$235,228.56	$1,493,440.80	$461,435.14	$842,332.48	$3,032,436.98	$11,938.73	207	81.50%
Department of Housing and Urban Development	23	20	$35,001.00	$291,153.00	$105,960.08	$137,128.00	$569,242.08	$24,749.66	19	82.61%
Department of Justice	162	107	$71,854.36	$1,538,126.40	$243,500.00	$356,864.93	$2,210,345.69	$13,644.11	114	70.37%
Department of Labor	49	35	$33,916.43	$348,242.48	$1,700.00	$151,854.02	$535,712.93	$10,932.92	32	65.31%
Department of State	29	15	$0.00	$340,261.89	$0.00	$233,604.00	$573,865.89	$19,788.48	20	68.97%
Department of the Air Force	181	99	$31,102.13	$1,075,161.52	$306,600.00	$662,242.37	$2,075,106.02	$11,464.67	98	54.14%
Department of the Army	483	244	$317,827.61	$2,328,722.40	$716,721.21	$1,175,548.05	$4,538,819.27	$9,397.14	387	80.12%
Department of the Interior	110	75	$14,681.00	$833,239.40	$37,967.53	$190,232.84	$1,076,120.77	$9,782.92	74	67.27%
Department of the Navy	430	303	$197,804.00	$1,661,145.00	$614,371.00	$1,427,605.00	$3,900,925.00	$9,071.92	206	47.91%
Department of the Treasury	102	61	$8,506.00	$209,155.00	$315,137.00	$259,679.00	$792,477.00	$7,769.38	93	91.18%
Department of Transportation	96	68	$58,588.51	$331,478.17	$87,000.00	$458,977.34	$936,044.02	$9,750.46	75	78.13%
Department of Veterans Affairs	559	308	$41,596.33	$5,824,770.09	$1,258,648.30	$1,592,937.10	$8,717,951.82	$15,595.62	360	64.40%
Election Assistance Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Environmental Protection Agency	13	9	$0.00	$22,892.00	$15,000.00	$598,000.00	$635,892.00	$48,914.77	10	76.92%
Equal Employment Opportunity Commission	6	4	$0.00	$13,500.00	$0.00	$6,150.00	$19,650.00	$3,275.00	4	66.67%
Export-Import Bank of the US	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Farm Credit Administration	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Farm Credit System Insurance Corporation	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Federal Communications Commission	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Federal Deposit Insurance Corporation	14	8	$9,912.02	$316,843.98	$0.00	$16,500.00	$343,256.00	$24,518.29	14	100.00%
Federal Election Commission	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Federal Energy Regulatory Commission	1	1	$0.00	$25,000.00	$0.00	$0.00	$25,000.00	$25,000.00	0	0.00%
Federal Financial Institutions Examination Council	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Housing Finance Agency	5	4	$15,785.00	$144,425.00	$0.00	$31,000.00	$191,210.00	$38,242.00	4	80.00%

Table B-21 FY 2012 Complaint Closures with Benefits

Agency or Department	Number Complaint Closures with Benefits	Number Complaint Closures w/ Monetary Benefits	Total Amount Back Pay / Front Pay	Total Amount Lump Sum Payments	Total Amount Compensatory Damages	Total Amount Attorney's Fees and Costs	Total Amount All Monetary Benefits	Average Monetary Benefits Per Complaint Closures With Benefits	Number Complaint Closures with Non-Monetary Benefits	% Complaint Closures with Non-Monetary Benefits
Federal Labor Relations Authority	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Federal Maritime Commission	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Federal Mediation and Conciliation Service	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Federal Mine Safety & Health Review Commission	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Federal Reserve System--Board of Governors	2	2	$0.00	$67,012.50	$0.00	$7,500.00	$74,512.50	$37,256.25	0	0.00%
Federal Retirement Thrift Investment Board	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Trade Commission	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
General Services Administration	18	13	$79,699.84	$114,800.00	$4,336.00	$80,534.23	$279,370.07	$15,520.56	13	72.22%
Government Printing Office	10	7	$0.00	$50,000.00	$0.00	$105,200.00	$155,200.00	$15,520.00	3	30.00%
Harry S. Truman Scholarship Foundation	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Holocaust Memorial Museum U.S.	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Institute of Museum and Library Services	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Inter-American Foundation	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
International Boundary and Water Commission	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
International Joint Commission: US and Canada	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
International Trade Commission	1	1	$0.00	$29,840.00	$0.00	$10,000.00	$39,840.00	$39,840.00	1	100.00%
James Madison Memorial Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Japan-United States Friendship Commission	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
John F. Kennedy Center for the Performing Arts	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Marine Mammal Commission	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Merit Systems Protection Board	1	1	$0.00	$5,000.00	$0.00	$0.00	$5,000.00	$5,000.00	0	0.00%
Millennium Challenge Corporation	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Aeronautics and Space Administration	7	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	7	100.00%
National Archives and Records Administration	3	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	3	100.00%
National Capital Planning Commission	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
National Council on Disability	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
National Credit Union Administration	6	5	$131,277.44	$67,500.00	$0.00	$11,000.00	$209,777.44	$34,962.91	3	50.00%
National Endowment for the Arts	2	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	2	100.00%
National Endowment for the Humanities	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
National Foundation on the Arts & the Humanities	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Gallery of Art	2	2	$0.00	$27,000.00	$0.00	$1,000.00	$28,000.00	$14,000.00	2	100.00%
National Indian Gaming Commission	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
National Labor Relations Board	4	3	$0.00	$7,985.00	$0.00	$44,000.00	$51,985.00	$12,996.25	1	25.00%
National Mediation Board	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
National Reconnaissance Office	1	1	$0.00	$80,000.00	$0.00	$0.00	$80,000.00	$80,000.00	1	100.00%
National Science Foundation	6	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	6	100.00%
National Transportation Safety Board	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Navajo and Hopi Indian Relocation Commission	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%

Table B-21 FY 2012 Complaint Closures with Benefits

Agency or Department	Number Complaint Closures with Benefits	Number Complaint Closures w/ Monetary Benefits	Total Amount Back Pay / Front Pay	Total Amount Lump Sum Payments	Total Amount Compensatory Damages	Total Amount Attorney's Fees and Costs	Total Amount All Monetary Benefits	Average Monetary Benefits Per Complaint Closures With Benefits	Number Complaint Closures with Non-Monetary Benefits	% Complaint Closures with Non-Monetary Benefits
Nuclear Regulatory Commission	11	7	$0.00	$129,211.00	$0.00	$68,200.00	$197,411.00	$17,946.45	7	63.64%
Nuclear Waste Technical Review Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Occupational Safety &Health Review Commission	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Office of Government Ethics	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Office of Personnel Management	3	3	$22,000.00	$20,000.00	$0.00	$2,000.00	$44,000.00	$14,666.67	3	100.00%
Office of Special Counsel	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Office of the Director of National Intelligence	2	2	$0.00	$80,000.00	$0.00	$10,400.00	$90,400.00	$45,200.00	2	100.00%
Overseas Private Investment Corporation	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Peace Corps	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Pension Benefit Guaranty Corporation	2	2	$0.00	$0.00	$1,500.00	$11,067.56	$12,567.56	$6,283.78	1	50.00%
Postal Regulatory Commission	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Presidio Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Railroad Retirement Board	1	1	$0.00	$3,500.00	$0.00	$0.00	$3,500.00	$3,500.00	0	0.00%
Securities and Exchange Commission	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
Selective Service System	2	2	$0.00	$0.00	$0.00	$60,000.00	$60,000.00	$30,000.00	1	50.00%
Small Business Administration	11	6	$0.00	$74,000.00	$25,000.00	$91,200.00	$190,200.00	$17,290.91	9	81.82%
Smithsonian Institution	3	3	$0.00	$255,260.00	$0.00	$0.00	$255,260.00	$85,086.67	3	100.00%
Social Security Administration	54	26	$1,817.65	$693,390.65	$8,500.00	$256,281.86	$959,990.16	$17,777.60	47	87.04%
Tennessee Valley Authority	13	12	$0.00	$136,580.00	$37,500.00	$10,500.00	$184,580.00	$14,198.46	10	76.92%
Trade and Development Agency	0	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	0	0.00%
U.S. Postal Service	862	663	$960,119.93	$502,055.00	$3,346,413.61	$1,386,657.69	$6,195,246.23	$7,187.06	448	51.97%
Utah Reclamation Mitigation and Conservation Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Valles Caldera Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Cabinet Level Subtotal	4,021	2,610	$2,586,489.87	$22,998,170.58	$8,414,311.82	$12,606,790.53	$46,605,762.80	$11,590.59	2,615	65.03%
Midsize Agencies Subtotal	139	82	$113,429.51	$1,658,766.63	$90,336.00	$1,070,016.09	$2,932,548.23	$21,097.47	119	85.61%
Small Agencies Subtotal	95	64	$170,262.44	$922,473.50	$269,909.77	$490,872.73	$1,853,518.44	$19,510.72	55	57.89%
Micro Agencies Subtotal	2	2	$0.00	$27,010.74	$0.00	$24,489.26	$51,500.00	$25,750.00	0	0.00%
Government-wide	4,257	2,758	$2,870,181.82	$25,606,421.45	$8,774,557.59	$14,192,168.61	$51,443,329.47	$12,084.41	2,789	65.52%

NRF = No Report Filed

Table B-22 FY 2012 Complaint Closures By Statute

Agency or Department	Total Complaint Closures	Title VII	ADEA	Rehabilitation Act	EPA	GINA	Total by Statute
Advisory Council on Historic Preservation	NRF	NRF	NRF	NRF	NRF	NRF	NRF
African Development Foundation	3	3	0	0	0	0	3
Agency for International Development	16	15	7	3	0	0	25
American Battle Monuments Commission	0	0	0	0	0	0	0
Appalachian Regional Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Architectural and Transportation Barriers Compliance Board	0	0	0	0	0	0	0
Arctic Research Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Armed Forces Retirement Home	4	4	0	0	0	0	4
Barry Goldwater Scholarship and Excellence in Education Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Broadcasting Board of Governors	14	14	3	0	0	0	17
Central Intelligence Agency	39	29	8	8	0	1	47
Chemical Safety and Hazard Investigation Board	0	0	0	0	0	0	0
Christopher Columbus Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission of Fine Arts	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission on Civil Rights	0	0	0	0	0	0	0
Committee for Purchase from People Who Are Blind or Severely Disabled	0	0	0	0	0	0	0
Commodity Futures Trading Commission	2	2	1	0	0	0	3
Consumer Financial Protection Bureau	7	3	7	0	0	0	10
Consumer Product Safety Commission	2	2	0	1	0	0	3
Corporation for National and Community Service	3	3	1	0	0	0	4
Court Services and Offender Supervision Agency for the District of Columbia	15	12	3	2	0	0	17
Defense Army and Air Force Exchange	89	69	25	31	0	0	125
Defense Commissary Agency	120	103	30	33	0	0	166
Defense Contract Audit Agency	32	23	5	4	0	0	32
Defense Contract Management Agency	38	32	13	10	0	0	55
Defense Finance and Accounting Service	39	34	16	15	0	0	65
Defense Human Resources Activity	5	5	0	1	0	0	6
Defense Information Systems Agency	8	6	1	2	0	0	9
Defense Intelligence Agency	34	33	8	5	0	0	46

Table B-22 FY 2012 Complaint Closures By Statute

Agency or Department	Total Complaint Closures	Title VII	ADEA	Rehabilitation Act	EPA	GINA	Total by Statute
Defense Joint Task Force National Capital Region Medical	7	6	1	0	1	0	8
Defense Logistics Agency	136	118	52	37	0	0	208
Defense Media Activity	3	2	1	1	0	0	4
Defense Missile Defense Agency	0	0	0	0	0	0	0
Defense National Geospatial-Intelligence Agency	20	20	2	0	0	0	22
Defense National Guard Bureau	33	31	4	0	0	0	35
Defense National Security Agency	17	15	5	3	0	1	24
Defense Nuclear Facilities Safety Board	0	0	0	0	0	0	0
Defense Office of the Inspector General	3	3	1	0	0	0	4
Defense Office of the Secretary - Wash. Hqtrs. Services	45	40	10	9	1	0	60
Defense Security Service	6	3	1	2	0	0	6
Defense Technical Information Center	1	1	0	0	0	0	1
Defense Threat Reduction Agency	8	8	0	0	0	0	8
Defense TRICARE Management Activity	7	7	1	2	0	0	10
Defense Uniformed Services University	0	0	0	0	0	0	0
Department of Agriculture	453	380	147	91	2	2	622
Department of Commerce	432	346	165	96	1	0	608
Department of Defense Education Activity	55	45	20	9	0	0	74
Department of Education	46	41	17	11	2	0	71
Department of Energy	63	51	20	12	2	0	85
Department of Health and Human Services	409	350	143	108	11	0	612
Department of Homeland Security	1,097	910	352	247	2	1	1,513
Department of Housing and Urban Development	73	72	35	12	0	0	119
Department of Justice	857	767	221	170	5	4	1,167
Department of Labor	134	121	45	31	2	0	199
Department of State	110	72	28	26	0	0	126
Department of the Air Force	500	417	140	143	3	0	703
Department of the Army	1,116	946	264	273	4	1	1,489
Department of the Interior	307	249	114	78	1	1	444
Department of the Navy	904	780	182	160	6	1	1,129
Department of the Treasury	407	326	115	111	1	1	556

Table B-22 FY 2012 Complaint Closures By Statute

Agency or Department	Total Complaint Closures	Title VII	ADEA	Rehabilitation Act	EPA	GINA	Total by Statute
Department of Transportation	335	289	102	81	6	0	479
Department of Veterans Affairs	2,123	1,203	558	610	13	1	2,387
Election Assistance Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Environmental Protection Agency	49	44	22	10	2	0	78
Equal Employment Opportunity Commission	20	17	4	10	0	0	31
Export-Import Bank of the US	1	0	1	0	0	0	1
Farm Credit Administration	0	0	0	0	0	0	0
Farm Credit System Insurance Corporation	0	0	0	0	0	0	0
Federal Communications Commission	2	8	0	0	0	0	8
Federal Deposit Insurance Corporation	42	39	18	5	0	0	62
Federal Election Commission	0	0	0	0	0	0	0
Federal Energy Regulatory Commission	10	6	1	3	0	0	10
Federal Financial Institutions Examination Council	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Housing Finance Agency	6	5	4	1	1	0	11
Federal Labor Relations Authority	0	0	0	0	0	0	0
Federal Maritime Commission	0	0	0	0	0	0	0
Federal Mediation and Conciliation Service	2	0	2	0	0	0	2
Federal Mine Safety & Health Review Commission	0	0	0	0	0	0	0
Federal Reserve System--Board of Governors	6	5	3	0	0	0	8
Federal Retirement Thrift Investment Board	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Trade Commission	1	1	0	0	0	0	1
General Services Administration	85	69	39	21	0	0	129
Government Printing Office	29	28	6	2	0	0	36
Harry S. Truman Scholarship Foundation	0	0	0	0	0	0	0
Holocaust Memorial Museum U.S.	0	0	0	0	0	0	0
Institute of Museum and Library Services	0	0	0	0	0	0	0
Inter-American Foundation	0	0	0	0	0	0	0
International Boundary and Water Commission	0	0	0	0	0	0	0
International Joint Commission: US and Canada	NRF	NRF	NRF	NRF	NRF	NRF	NRF
International Trade Commission	1	1	1	0	0	0	2
James Madison Memorial Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Japan-United States Friendship Commission	0	0	0	0	0	0	0
John F. Kennedy Center for the Performing Arts	0	0	0	0	0	0	0

Table B-22 FY 2012 Complaint Closures By Statute

Agency or Department	Total Complaint Closures	Title VII	ADEA	Rehabilitation Act	EPA	GINA	Total by Statute
Marine Mammal Commission	0	0	0	0	0	0	0
Merit Systems Protection Board	1	1	1	1	0	0	3
Millennium Challenge Corporation	0	0	0	0	0	0	0
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Aeronautics and Space Administration	38	35	9	11	2	0	57
National Archives and Records Administration	11	6	3	2	0	0	11
National Capital Planning Commission	0	0	0	0	0	0	0
National Council on Disability	0	0	0	0	0	0	0
National Credit Union Administration	7	5	3	4	0	0	12
National Endowment for the Arts	3	3	0	0	0	0	3
National Endowment for the Humanities	0	0	0	0	0	0	0
National Foundation on the Arts& the Humanities	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Gallery of Art	6	5	2	1	0	0	8
National Indian Gaming Commission	1	1	1	0	0	0	2
National Labor Relations Board	8	6	2	5	0	0	13
National Mediation Board	0	0	0	0	0	0	0
National Reconnaissance Office	7	7	2	2	0	0	11
National Science Foundation	6	6	2	2	0	0	10
National Transportation Safety Board	2	2	2	0	0	0	4
Navajo and Hopi Indian Relocation Commission	0	0	0	0	0	0	0
Nuclear Regulatory Commission	16	11	7	7	0	0	25
Nuclear Waste Technical Review Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Occupational Safety &Health Review Commission	0	0	0	0	0	0	0
Office of Government Ethics	2	2	0	0	0	0	2
Office of Personnel Management	28	20	10	8	0	0	38
Office of Special Counsel	0	0	0	0	0	0	0
Office of the Director of National Intelligence	4	2	1	1	0	0	4
Overseas Private Investment Corporation	0	0	0	0	0	0	0
Peace Corps	4	4	1	0	0	0	5
Pension Benefit Guaranty Corporation	20	19	8	2	0	0	29
Postal Regulatory Commission	0	0	0	0	0	0	0
Presidio Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF

Table B-22 FY 2012 Complaint Closures By Statute							
Agency or Department	**Total Complaint Closures**	**Title VII**	**ADEA**	**Rehabilitation Act**	**EPA**	**GINA**	**Total by Statute**
Railroad Retirement Board	1	1	0	0	0	0	1
Securities and Exchange Commission	4	4	3	2	0	0	9
Selective Service System	2	2	0	0	0	0	2
Small Business Administration	38	32	17	13	0	0	62
Smithsonian Institution	15	14	4	5	2	0	26
Social Security Administration	414	334	173	119	0	1	627
Tennessee Valley Authority	58	44	20	10	0	0	74
Trade and Development Agency	0	0	0	0	0	0	0
U.S. Postal Service	4,579	3,817	1,586	1,701	0	30	7,146
Utah Reclamation Mitigation and Conservation Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Valles Caldera Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Cabinet Level Subtotal	14,651	11,741	4,430	4,125	63	43	20,423
Midsize Agencies Subtotal	774	634	319	202	6	1	1,163
Small Agencies Subtotal	276	237	83	59	1	1	382
Micro Agencies Subtotal	5	5	0	0	0	0	5
Government-wide	15,706	12,617	4,832	4,386	70	45	21,973

NRF = No Report Filed

Table B-23 FY 2012 Summary of Pending Complaints By Category

Agency or Department	Pending End of Period			Pending Acknowledgment			Pending Investigation			Pending Hearing			Pending Final Agency Action		
	Number	Total Days	Average Days	Number	Total Days	Average Days	Number	Total Days	Average Days	Number	Total Days	Average Days	Number	Total Days	Average Days
Advisory Council on Historic Preservation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
African Development Foundation	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Agency for International Development	26	13,229	508.81	0	0	0	6	1,212	202	15	9,165	611	5	2,852	570.4
American Battle Monuments Commission	1	120	120	0	0	0	1	120	120	0	0	0	0	0	0
Appalachian Regional Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Architectural and Transportation Barriers Compliance Board	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Arctic Research Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Armed Forces Retirement Home	5	689	137.8	0	0	0	5	689	137.8	0	0	0	0	0	0
Barry Goldwater Scholarship and Excellence in Education Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Broadcasting Board of Governors	11	5,316	483.27	0	0	0	4	278	69.5	6	4,985	830.83	1	53	53
Central Intelligence Agency	48	33,581	699.6	1	33	33	20	5,406	270.3	26	27,122	1,043.15	1	1,020	1,020.00
Chemical Safety and Hazard Investigation Board	1	45	45	0	0	0	1	45	45	0	0	0	0	0	0
Christopher Columbus Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission of Fine Arts	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission on Civil Rights	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Committee for Purchase from People Who Are Blind or Severely Disabled	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Commodity Futures Trading Commission	2	277	138.5	1	1	1	0	0	0	0	0	0	1	276	276
Consumer Financial Protection Bureau	4	301	75.25	2	94	47	2	207	103.5	0	0	0	0	0	0
Consumer Product Safety Commission	4	1,574	393.5	0	0	0	2	248	124	2	1,326	663	0	0	0
Corporation for National and Community Service	7	1,205	172.14	0	0	0	2	10	5	4	1,192	298	1	3	3
Court Services and Offender Supervision Agency for the District of Columbia	14	7,156	511.14	0	0	0	3	468	156	11	6,688	608	0	0	0
Defense Army and Air Force Exchange	88	21,696	246.55	7	424	60.57	48	5,876	122.42	29	14,251	491.41	4	1,145	286.25
Defense Commissary Agency	151	52,335	346.59	0	0	0	70	10,623	151.76	50	31,726	634.52	17	9,051	532.41
Defense Contract Audit Agency	28	8,082	288.64	2	66	33	14	2,319	165.64	8	5,329	666.13	1	354	354
Defense Contract Management Agency	48	14,487	301.81	3	0	0	19	3,694	194.42	17	7,940	467.06	9	2,853	317
Defense Finance and Accounting Service	44	14,657	333.11	0	0	0	21	2,895	137.86	18	10,696	594.22	4	1,061	265.25
Defense Human Resources Activity	6	496	82.67	4	337	84.25	2	159	79.5	0	0	0	0	0	0
Defense Information Systems Agency	49	27,272	556.57	4	599	149.75	13	2,364	181.85	24	15,404	641.83	8	8,905	1,113.13
Defense Intelligence Agency	59	28,141	476.97	12	453	37.75	18	3,970	220.56	24	21,271	886.29	5	2,447	489.4
Defense Joint Task Force National Capital Region Medical	27	4,286	158.74	7	210	30	19	3,673	193.32	1	403	403	0	0	0
Defense Logistics Agency	134	39,735	296.53	8	200	25	67	8,605	128.43	46	27,447	596.67	11	3,466	315.09
Defense Media Activity	3	1,909	636.33	0	0	0	1	32	32	1	1,197	1,197.00	1	680	680
Defense Missile Defense Agency	9	3,339	371	0	0	0	3	560	186.67	6	2,779	463.17	0	0	0
Defense National Geospatial-Intelligence Agency	34	10,016	294.59	0	0	0	9	1,240	137.78	22	8,628	392.18	3	148	49.33
Defense National Guard Bureau	36	12,859	357.19	16	3,985	249.06	8	1,292	161.5	2	1,150	575	9	6,407	711.89
Defense National Security Agency	50	26,683	533.66	2	207	103.5	14	2,249	160.64	34	24,227	712.56	0	0	0
Defense Nuclear Facilities Safety Board	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Defense Office of the Inspector General	8	2,471	308.88	0	0	0	3	433	144.33	3	1,751	583.67	1	285	285

Table B-23 FY 2012 Summary of Pending Complaints By Category

Agency or Department	Pending End of Period			Pending Acknowledgment			Pending Investigation			Pending Hearing			Pending Final Agency Action		
	Number	Total Days	Average Days	Number	Total Days	Average Days	Number	Total Days	Average Days	Number	Total Days	Average Days	Number	Total Days	Average Days
Defense Office of the Secretary - Wash. Hqtrs. Services	64	30,955	483.67	12	549	45.75	14	3,071	219.36	28	19,398	692.79	9	7,919	879.89
Defense Security Service	12	2,740	228.33	0	0	0	6	1,080	180	3	1,504	501.33	3	156	52
Defense Technical Information Center	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Defense Threat Reduction Agency	17	7,564	444.94	0	128	128	6	847	141.17	11	6,589	599	0	0	0
Defense TRICARE Management Activity	10	2,442	244.2	2	121	60.5	6	1,519	253.17	2	802	401	0	0	0
Defense Uniformed Services University	5	2,005	401	0	0	0	4	1,225	306.25	1	780	780	0	0	0
Department of Agriculture	937	574,555	613.19	71	8,283	116.66	250	67,730	270.92	455	373,457	820.78	153	124,634	814.6
Department of Commerce	469	223,485	476.51	12	256	21.33	96	12,395	129.11	174	111,780	642.41	182	99,020	544.07
Department of Defense Education Activity	94	28,311	301.18	8	287	35.88	19	2,068	108.84	40	20,657	516.43	19	5,264	277.05
Department of Education	51	22,390	439.02	3	13	4.33	15	1,890	126	31	19,794	638.52	2	693	346.5
Department of Energy	96	31,199	324.99	20	3,387	169.35	28	4,180	149.29	33	15,787	478.39	14	7,828	559.14
Department of Health and Human Services	502	208,380	415.1	37	2,872	77.62	94	11,442	121.72	289	174,089	602.38	68	19,669	289.25
Department of Homeland Security	1,980	934,552	472	179	23,423	130.85	476	99,742	209.54	979	642,063	655.84	322	168,968	524.75
Department of Housing and Urban Development	148	83,970	567.36	5	115	23	36	5,715	158.75	91	72,246	793.91	16	5,894	368.38
Department of Justice	1,454	807,363	555.27	127	50,586	398.31	251	48,972	195.11	624	478,301	766.51	372	185,090	497.55
Department of Labor	155	58,666	378.49	25	1,454	58.16	41	6,891	168.07	76	47,468	624.58	7	2,762	394.57
Department of State	213	100,309	470.93	24	4,237	176.54	63	11,596	184.06	90	66,094	734.38	36	18,382	510.61
Department of the Air Force	702	302,080	430.31	23	1,142	49.65	292	54,812	187.71	243	172,633	710.42	143	73,427	513.48
Department of the Army	1,308	490,945	375.34	84	4,663	55.51	606	102,482	169.11	500	336,533	673.07	105	46,662	444.4
Department of the Interior	545	350,147	642.47	66	6,180	93.64	151	32,202	213.26	234	252,272	1,078.09	84	59,011	702.51
Department of the Navy	1,026	417,970	407.38	60	2,079	34.65	468	107,041	228.72	394	271,050	687.94	103	37,782	366.82
Department of the Treasury	543	225,679	415.62	37	1,134	30.65	182	25,121	138.03	281	178,621	635.66	38	20,788	547.05
Department of Transportation	582	429,010	737.13	85	13,777	162.08	96	10,057	104.76	329	373,651	1,135.72	69	31,503	456.57
Department of Veterans Affairs	3,116	1,305,599	419	233	6,539	28.06	898	119,480	133.05	1,548	902,856	583.24	435	276,709	636.11
Election Assistance Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Environmental Protection Agency	150	57,293	381.95	20	1,516	75.8	39	7,597	194.79	46	31,712	689.39	43	16,370	380.7
Equal Employment Opportunity Commission	27	8,071	298.93	4	214	53.5	4	399	99.75	8	5,189	648.63	6	2,185	364.17
Export-Import Bank of the US	1	2	2	0	0	0	0	0	0	0	0	0	0	0	0
Farm Credit Administration	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Farm Credit System Insurance Corporation	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Federal Communications Commission	12	1,145	95.42	3	55	18.33	2	35	17.5	5	1,020	204	0	0	0
Federal Deposit Insurance Corporation	49	14,741	300.84	3	107	35.67	23	3,079	133.87	18	9,745	541.39	3	1,791	597
Federal Election Commission	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Federal Energy Regulatory Commission	3	390	130	1	30	30	2	360	180	0	0	0	0	0	0
Federal Financial Institutions Examination Council	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Housing Finance Agency	9	2,890	321.11	2	171	85.5	3	704	234.67	2	556	278	2	1,459	729.5
Federal Labor Relations Authority	1	296	296	0	0	0	0	0	0	0	0	0	1	296	296
Federal Maritime Commission	2	360	180	0	0	0	2	360	180	0	0	0	0	0	0
Federal Mediation and Conciliation Service	2	362	181	0	0	0	2	362	181	0	0	0	0	0	0
Federal Mine Safety& Health Review Commission	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Federal Reserve System--Board of Governors	23	10,984	477.57	6	2,676	446	5	831	166.2	6	4,692	782	6	2,785	464.17
Federal Retirement Thrift Investment Board	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Trade Commission	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Table B-23 FY 2012 Summary of Pending Complaints By Category

Agency or Department	Pending End of Period			Pending Acknowledgment			Pending Investigation			Pending Hearing			Pending Final Agency Action		
	Number	Total Days	Average Days	Number	Total Days	Average Days	Number	Total Days	Average Days	Number	Total Days	Average Days	Number	Total Days	Average Days
General Services Administration	152	68,909	453.35	0	0	0	44	8,106	184.23	87	56,100	644.83	12	4,092	341
Government Printing Office	88	56,123	637.76	5	485	97	15	3,677	245.13	62	49,995	806.37	6	1,966	327.67
Harry S. Truman Scholarship Foundation	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Holocaust Memorial Museum U.S.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Institute of Museum and Library Services	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Inter-American Foundation	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
International Boundary and Water Commission	2	615	307.5	0	0	0	0	0	0	2	615	307.5	0	0	0
International Joint Commission: US and Canada	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
International Trade Commission	1	334	334	0	0	0	0	0	0	1	334	334	0	0	0
James Madison Memorial Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Japan-United States Friendship Commission	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
John F. Kennedy Center for the Performing Arts	1	245	245	0	0	0	0	0	0	1	245	245	0	0	0
Marine Mammal Commission	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Merit Systems Protection Board	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Millennium Challenge Corporation	5	3,329	665.8	0	0	0	0	0	0	5	3,329	665.8	0	0	0
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Aeronautics and Space Administration	46	18,576	403.83	7	577	82.43	9	1,495	166.11	17	11,574	680.82	12	4,917	409.75
National Archives and Records Administration	6	4,750	791.67	0	0	0	2	160	80	4	4,590	1,147.50	0	0	0
National Capital Planning Commission	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
National Council on Disability	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
National Credit Union Administration	4	1,651	412.75	0	0	0	1	109	109	2	1,259	629.5	1	283	283
National Endowment for the Arts	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
National Endowment for the Humanities	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
National Foundation on the Arts & the Humanities	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Gallery of Art	2	1,233	616.5	1	39	39	0	0	0	0	0	0	1	1,194	1,194.00
National Indian Gaming Commission	1	387	387	0	0	0	0	0	0	1	387	387	0	0	0
National Labor Relations Board	7	2,422	346	0	0	0	4	480	120	3	1,942	647.33	0	0	0
National Mediation Board	2	934	467	0	0	0	0	0	0	2	934	467	0	0	0
National Reconnaissance Office	3	3,049	1,016.33	0	0	0	1	10	10	1	1,599	1,599.00	1	1,440	1,440.00
National Science Foundation	17	2,750	161.76	0	0	0	8	974	121.75	6	1,530	255	3	246	82
National Transportation Safety Board	1	101	101	0	0	0	1	101	101	0	0	0	0	0	0
Navajo and Hopi Indian Relocation Commission	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Nuclear Regulatory Commission	14	4,047	289.07	2	97	48.5	6	1,243	207.17	3	1,786	595.33	3	921	307
Nuclear Waste Technical Review Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Occupational Safety & Health Review Commission	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Office of Government Ethics	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Office of Personnel Management	55	26,369	479.44	3	526	175.33	18	1,377	76.5	24	21,001	875.04	10	3,465	346.5
Office of Special Counsel	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Office of the Director of National Intelligence	5	654	130.8	3	29	9.67	1	286	286	1	339	339	0	0	0
Overseas Private Investment Corporation	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Peace Corps	4	1,326	331.5	0	0	0	1	49	49	2	310	155	1	967	967
Pension Benefit Guaranty Corporation	14	7,414	529.57	0	0	0	6	900	150	8	6,514	814.25	0	0	0
Postal Regulatory Commission	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Table B-23 FY 2012 Summary of Pending Complaints By Category

Agency or Department	Pending End of Period			Pending Acknowledgment			Pending Investigation			Pending Hearing			Pending Final Agency Action		
	Number	Total Days	Average Days	Number	Total Days	Average Days	Number	Total Days	Average Days	Number	Total Days	Average Days	Number	Total Days	Average Days
Presidio Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Railroad Retirement Board	6	2,305	384.17	0	0	0	1	195	195	5	2,110	422	0	0	0
Securities and Exchange Commission	25	7,761	310.44	3	192	64	12	1,830	152.5	5	4,260	852	5	1,479	295.8
Selective Service System	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Small Business Administration	56	33,034	589.89	1	4	4	18	3,042	169	30	27,468	915.6	6	2,270	378.33
Smithsonian Institution	13	4,366	335.85	1	23	23	6	484	80.67	6	3,859	643.17	0	0	0
Social Security Administration	862	453,374	525.96	101	5,984	59.25	172	32,527	189.11	397	327,951	826.07	174	86,723	498.41
Tennessee Valley Authority	56	22,910	409.11	4	56	14	18	1,551	86.17	20	13,615	680.75	10	7,042	704.2
Trade and Development Agency	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
U.S. Postal Service	3,874	1,299,901	335.54	1	17	17	949	84,568	89.11	2,264	1,160,501	512.59	298	48,953	164.27
Utah Reclamation Mitigation and Conservation Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Valles Caldera Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Cabinet Level Subtotal	18,677	8,208,681	439.51	1,179	137,723	116.81	5,376	866,110	161.11	9,005	5,873,125	652.21	2,551	1,277,916	500.95
Midsize Agencies Subtotal	1,443	699,873	485.01	142	8,887	62.58	349	59,465	170.39	645	503,025	779.88	270	126,670	469.15
Small Agencies Subtotal	403	188,023	466.56	32	4,022	125.69	121	21,376	176.66	197	143,079	726.29	45	19,425	431.67
Micro Agencies Subtotal	4	1,099	274.75	0	0	0	2	165	82.5	2	934	467	0	0	0
Government-wide	20,527	9,097,676	443.21	1,353	150,632	111.33	5,848	947,116	161.96	9,849	6,520,163	662.01	2,866	1,424,011	496.86

NRF = No Report Filed

Table B-24 FY 2012 Agency Staff Resources

Agency or Department	Agency Counselors							Agency Investigators							Agency Counselors/Investigators						
		Full Time		Part Time		Collateral Duty			Full Time		Part Time		Collateral Duty				Full Time		Part Time		Collateral Duty	
	Total	Number	%	Number	%	Number	%	Total	Number	%	Number	%	Number	%	Total	Number	%	Number	%	Number	%
Advisory Council on Historic Preservation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
African Development Foundation	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Agency for International Development	37	0	0.00%	0	0.00%	37	100.00%	2	0	0.00%	0	0.00%	2	100.00%	0	0	0.00%	0	0.00%	0	0.00%
American Battle Monuments Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Appalachian Regional Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Architectural and Transportation Barriers Compliance Board	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Arctic Research Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Armed Forces Retirement Home	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Barry Goldwater Scholarship and Excellence in Education Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Broadcasting Board of Governors	4	0	0.00%	0	0.00%	4	100.00%	0	0	0.00%	0	0.00%	0	0.00%	4	0	0.00%	0	0.00%	4	100.00%
Central Intelligence Agency	0	0	0.00%	0	0.00%	0	0.00%	1	0	0.00%	0	0.00%	1	100.00%	12	12	100.00%	0	0.00%	0	0.00%
Chemical Safety and Hazard Investigation Board	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Christopher Columbus Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission of Fine Arts	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission on Civil Rights	1	0	0.00%	0	0.00%	1	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Committee for Purchase from People Who Are Blind or Severely Disabled	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Commodity Futures Trading Commission	20	0	0.00%	0	0.00%	20	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Consumer Financial Protection Bureau	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Consumer Product Safety Commission	10	0	0.00%	0	0.00%	10	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Corporation for National and Community Service	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Court Services and Offender Supervision Agency for the District of Columbia	15	2	13.33%	0	0.00%	13	86.67%	0	0	0.00%	0	0.00%	0	0.00%	2	2	100.00%	0	0.00%	0	0.00%
Defense Army and Air Force Exchange	248	0	0.00%	0	0.00%	248	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Commissary Agency	4	4	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Contract Audit Agency	9	9	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Contract Management Agency	4	4	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Finance and Accounting Service	10	2	20.00%	8	80.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Human Resources Activity	7	0	0.00%	7	100.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Information Systems Agency	3	3	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Intelligence Agency	5	5	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Joint Task Force National Capital Region Medical	1	0	0.00%	1	100.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Logistics Agency	44	0	0.00%	16	36.36%	28	63.64%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Media Activity	3	0	0.00%	0	0.00%	3	100.00%	0	0	0.00%	0	0.00%	0	0.00%	1	1	100.00%	0	0.00%	0	0.00%
Defense Missile Defense Agency	2	0	0.00%	1	50.00%	1	50.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense National Geospatial-Intelligence Agency	7	2	28.57%	0	0.00%	5	71.43%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense National Guard Bureau	429	32	7.46%	7	1.63%	390	90.91%	11	1	9.09%	0	0.00%	10	90.91%	26	6	23.08%	4	15.38%	16	61.54%
Defense National Security Agency	1	1	100.00%	0	0.00%	0	0.00%	7	6	85.71%	1	14.29%	0	0.00%	3	3	100.00%	0	0.00%	0	0.00%
Defense Nuclear Facilities Safety Board	3	0	0.00%	0	0.00%	3	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Office of the Inspector General	4	0	0.00%	3	75.00%	1	25.00%	1	1	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Office of the Secretary - Wash. Hqtrs. Services	4	4	100.00%	0	0.00%	0	0.00%	100	100	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Security Service	6	0	0.00%	0	0.00%	6	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Technical Information Center	7	0	0.00%	7	100.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Threat Reduction Agency	3	3	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%

Table B-24 FY 2012 Agency Staff Resources

Agency or Department	Agency Counselors							Agency Investigators							Agency Counselors/Investigators						
		Full Time		Part Time		Collateral Duty			Full Time		Part Time		Collateral Duty				Full Time		Part Time		Collateral Duty	
	Total	Number	%	Number	%	Number	%	Total	Number	%	Number	%	Number	%	Total	Number	%	Number	%	Number	%
Defense TRICARE Management Activity	1	0	0.00%	1	100.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Uniformed Services University	4	0	0.00%	0	0.00%	4	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Department of Agriculture	41	36	87.80%	0	0.00%	5	12.20%	0	0	0.00%	0	0.00%	0	0.00%	5	5	100.00%	0	0.00%	0	0.00%
Department of Commerce	46	20	43.48%	0	0.00%	26	56.52%	4	1	25.00%	0	0.00%	3	75.00%	0	0	0.00%	0	0.00%	0	0.00%
Department of Defense Education Activity	3	3	100.00%	0	0.00%	0	0.00%	7	0	0.00%	7	100.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Department of Education	4	2	50.00%	2	50.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Department of Energy	74	3	4.05%	1	1.35%	70	94.59%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Department of Health and Human Services	138	15	10.87%	10	7.25%	113	81.88%	0	0	0.00%	0	0.00%	0	0.00%	7	7	100.00%	0	0.00%	0	0.00%
Department of Homeland Security	196	73	37.24%	72	36.73%	51	26.02%	26	22	84.62%	0	0.00%	4	15.38%	0	0	0.00%	0	0.00%	0	0.00%
Department of Housing and Urban Development	4	3	75.00%	0	0.00%	1	25.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Department of Justice	257	30	11.67%	5	1.95%	222	86.38%	44	8	18.18%	0	0.00%	36	81.82%	9	5	55.56%	4	44.44%	0	0.00%
Department of Labor	15	1	6.67%	2	13.33%	12	80.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Department of State	513	0	0.00%	10	1.95%	503	98.05%	4	0	0.00%	4	100.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Department of the Air Force	375	298	79.47%	20	5.33%	57	15.20%	140	140	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Department of the Army	845	0	0.00%	0	0.00%	845	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Department of the Interior	165	42	25.45%	4	2.42%	119	72.12%	6	5	83.33%	0	0.00%	1	16.67%	0	0	0.00%	0	0.00%	0	0.00%
Department of the Navy	157	142	90.45%	7	4.46%	8	5.10%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Department of the Treasury	95	33	34.74%	4	4.21%	58	61.05%	21	21	100.00%	0	0.00%	0	0.00%	4	0	0.00%	0	0.00%	4	100.00%
Department of Transportation	79	7	8.86%	0	0.00%	72	91.14%	6	6	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Department of Veterans Affairs	27	27	100.00%	0	0.00%	0	0.00%	51	25	49.02%	26	50.98%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Election Assistance Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Environmental Protection Agency	37	16	43.24%	0	0.00%	21	56.76%	0	0	0.00%	0	0.00%	0	0.00%	8	8	100.00%	0	0.00%	0	0.00%
Equal Employment Opportunity Commission	1	1	100.00%	0	0.00%	0	0.00%	1	1	100.00%	0	0.00%	0	0.00%	1	1	100.00%	0	0.00%	0	0.00%
Export-Import Bank of the US	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Farm Credit Administration	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Farm Credit System Insurance Corporation	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Communications Commission	6	0	0.00%	0	0.00%	6	100.00%	0	0	0.00%	0	0.00%	0	0.00%	6	6	100.00%	0	0.00%	0	0.00%
Federal Deposit Insurance Corporation	6	1	16.67%	0	0.00%	5	83.33%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Election Commission	3	0	0.00%	0	0.00%	3	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Energy Regulatory Commission	5	0	0.00%	0	0.00%	5	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Financial Institutions Examination Council	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Housing Finance Agency	3	0	0.00%	0	0.00%	3	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Labor Relations Authority	3	0	0.00%	0	0.00%	3	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Maritime Commission	3	1	33.33%	0	0.00%	2	66.67%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Mediation and Conciliation Service	4	0	0.00%	0	0.00%	4	100.00%	1	0	0.00%	0	0.00%	1	100.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Mine Safety & Health Review Commission	1	0	0.00%	0	0.00%	1	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Reserve System--Board of Governors	3	3	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Retirement Thrift Investment Board	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Trade Commission	9	1	11.11%	0	0.00%	8	88.89%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
General Services Administration	21	0	0.00%	0	0.00%	21	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Government Printing Office	4	0	0.00%	3	75.00%	1	25.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Harry S. Truman Scholarship Foundation	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	1	0	0.00%	0	0.00%	1	100.00%
Holocaust Memorial Museum U.S.	5	0	0.00%	0	0.00%	5	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Institute of Museum and Library Services	1	0	0.00%	0	0.00%	1	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Inter-American Foundation	3	3	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
International Boundary and Water Commission	6	0	0.00%	0	0.00%	6	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
International Joint Commission: US and Canada	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
International Trade Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%

Table B-24 FY 2012 Agency Staff Resources

Agency or Department	Agency Counselors							Agency Investigators							Agency Counselors/Investigators						
		Full Time		Part Time		Collateral Duty			Full Time		Part Time		Collateral Duty				Full Time		Part Time		Collateral Duty	
	Total	Number	%	Number	%	Number	%	Total	Number	%	Number	%	Number	%	Total	Number	%	Number	%	Number	%
James Madison Memorial Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Japan-United States Friendship Commission	1	1	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
John F. Kennedy Center for the Performing Arts	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Marine Mammal Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Merit Systems Protection Board	3	0	0.00%	0	0.00%	3	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Millennium Challenge Corporation	3	0	0.00%	0	0.00%	3	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Aeronautics and Space Administration	29	10	34.48%	7	24.14%	12	41.38%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Archives and Records Administration	1	1	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Capital Planning Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Council on Disability	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Credit Union Administration	6	0	0.00%	0	0.00%	6	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Endowment for the Arts	2	0	0.00%	0	0.00%	2	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Endowment for the Humanities	2	0	0.00%	0	0.00%	2	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Foundation on the Arts & the Humanities	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Gallery of Art	10	0	0.00%	0	0.00%	10	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Indian Gaming Commission	1	0	0.00%	0	0.00%	1	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Labor Relations Board	43	0	0.00%	0	0.00%	43	100.00%	1	1	100.00%	0	0.00%	0	0.00%	4	4	100.00%	0	0.00%	0	0.00%
National Mediation Board	2	0	0.00%	0	0.00%	2	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Reconnaissance Office	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	3	3	100.00%	0	0.00%	0	0.00%
National Science Foundation	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Transportation Safety Board	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Navajo and Hopi Indian Relocation Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Nuclear Regulatory Commission	22	0	0.00%	0	0.00%	22	100.00%	0	0	0.00%	0	0.00%	0	0.00%	3	0	0.00%	0	0.00%	3	100.00%
Nuclear Waste Technical Review Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Occupational Safety & Health Review Commission	1	0	0.00%	0	0.00%	1	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Office of Government Ethics	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Office of Personnel Management	4	0	0.00%	0	0.00%	4	100.00%	0	0	0.00%	0	0.00%	0	0.00%	5	5	100.00%	0	0.00%	0	0.00%
Office of Special Counsel	5	0	0.00%	0	0.00%	5	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Office of the Director of National Intelligence	4	0	0.00%	0	0.00%	4	100.00%	0	0	0.00%	0	0.00%	0	0.00%	2	0	0.00%	0	0.00%	2	100.00%
Overseas Private Investment Corporation	2	0	0.00%	0	0.00%	2	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Peace Corps	11	0	0.00%	0	0.00%	11	100.00%	0	0	0.00%	0	0.00%	0	0.00%	11	0	0.00%	0	0.00%	11	100.00%
Pension Benefit Guaranty Corporation	2	2	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Postal Regulatory Commission	1	0	0.00%	0	0.00%	1	100.00%	1	0	0.00%	0	0.00%	1	100.00%	0	0	0.00%	0	0.00%	0	0.00%
Presidio Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Railroad Retirement Board	3	0	0.00%	0	0.00%	3	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Securities and Exchange Commission	9	0	0.00%	0	0.00%	9	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Selective Service System	1	0	0.00%	0	0.00%	1	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Small Business Administration	3	0	0.00%	0	0.00%	3	100.00%	2	0	0.00%	0	0.00%	2	100.00%	0	0	0.00%	0	0.00%	0	0.00%
Smithsonian Institution	3	2	66.67%	0	0.00%	1	33.33%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Social Security Administration	234	4	1.71%	0	0.00%	230	98.29%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Tennessee Valley Authority	20	1	5.00%	0	0.00%	19	95.00%	4	1	25.00%	0	0.00%	3	75.00%	0	0	0.00%	0	0.00%	0	0.00%
Trade and Development Agency	2	0	0.00%	0	0.00%	2	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
U.S. Postal Service	112	112	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%

Table B-24 FY 2012 Agency Staff Resources

	Agency Counselors							Agency Investigators							Agency Counselors/Investigators						
		Full Time		Part Time		Collateral Duty			Full Time		Part Time		Collateral Duty			Full Time		Part Time		Collateral Duty	
Agency or Department	**Total**	**Number**	**%**	**Number**	**%**	**Number**	**%**	**Total**	**Number**	**%**	**Number**	**%**	**Number**	**%**	**Total**	**Number**	**%**	**Number**	**%**	**Number**	**%**
Utah Reclamation Mitigation and Conservation Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Valles Caldera Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Cabinet Level Subtotal	3,952	916	23.18%	188	4.76%	2,848	72.06%	428	336	78.50%	38	8.88%	54	12.62%	55	27	49.09%	8	14.55%	20	36.36%
Midsize Agencies Subtotal	357	34	9.52%	7	1.96%	316	88.52%	6	1	16.67%	0	0.00%	5	83.33%	13	13	100.00%	0	0.00%	0	0.00%
Small Agencies Subtotal	266	11	4.14%	3	1.13%	252	94.74%	6	2	33.33%	0	0.00%	4	66.67%	48	28	58.33%	0	0.00%	20	41.67%
Micro Agencies Subtotal	21	4	19.05%	0	0.00%	17	80.95%	1	0	0.00%	0	0.00%	1	100.00%	1	0	0.00%	0	0.00%	1	100.00%
Government-wide	4,596	965	21.00%	198	4.31%	3,433	74.70%	441	339	76.87%	38	8.62%	64	14.51%	117	68	58.12%	8	6.84%	41	35.04%

NRF = No Report Filed

Table B-24a FY 2012 Contract Staff Resources

Agency or Department	Contract Counselors							Contract Investigators							Contract Counselors/Investigators						
		Full Time		Part Time		Collateral Duty			Full Time		Part Time		Collateral Duty				Full Time		Part Time		Collateral Duty	
	Total	Number	%	Number	%	Number	%	Total	Number	%	Number	%	Number	%	Total	Number	%	Number	%	Number	%
Advisory Council on Historic Preservation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
African Development Foundation	1	0	0.00%	1	100.00%	0	0.00%	1	1	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Agency for International Development	0	0	0.00%	0	0.00%	0	0.00%	9	0	0.00%	9	100.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
American Battle Monuments Commission	0	0	0.00%	0	0.00%	0	0.00%	15	0	0.00%	15	100.00%	0	0.00%	3	0	0.00%	3	100.00%	0	0.00%
Appalachian Regional Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Architectural and Transportation Barriers Compliance Board	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Arctic Research Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Armed Forces Retirement Home	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Barry Goldwater Scholarship and Excellence in Education Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Broadcasting Board of Governors	4	0	0.00%	4	100.00%	0	0.00%	5	0	0.00%	5	100.00%	0	0.00%	9	0	0.00%	9	100.00%	0	0.00%
Central Intelligence Agency	0	0	0.00%	0	0.00%	0	0.00%	1	0	0.00%	1	100.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Chemical Safety and Hazard Investigation Board	1	0	0.00%	1	100.00%	0	0.00%	1	0	0.00%	1	100.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Christopher Columbus Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission of Fine Arts	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission on Civil Rights	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Committee for Purchase from People Who Are Blind or Severely Disabled	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	1	0	0.00%	1	100.00%	0	0.00%
Commodity Futures Trading Commission	0	0	0.00%	0	0.00%	0	0.00%	1	1	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Consumer Financial Protection Bureau	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Consumer Product Safety Commission	0	0	0.00%	0	0.00%	0	0.00%	4	4	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Corporation for National and Community Service	10	10	100.00%	0	0.00%	0	0.00%	10	10	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Court Services and Offender Supervision Agency for the District of Columbia	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	1	1	100.00%	0	0.00%	0	0.00%
Defense Army and Air Force Exchange	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Commissary Agency	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Contract Audit Agency	6	0	0.00%	6	100.00%	0	0.00%	6	0	0.00%	6	100.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Contract Management Agency	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Finance and Accounting Service	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Human Resources Activity	0	0	0.00%	0	0.00%	0	0.00%	2	0	0.00%	2	100.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Information Systems Agency	2	2	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Intelligence Agency	0	0	0.00%	0	0.00%	0	0.00%	1	0	0.00%	1	100.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Joint Task Force National Capital Region Medical	0	0	0.00%	0	0.00%	0	0.00%	1	1	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Logistics Agency	3	0	0.00%	3	100.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Media Activity	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Missile Defense Agency	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense National Geospatial-Intelligence Agency	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense National Guard Bureau	2	0	0.00%	2	100.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense National Security Agency	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Nuclear Facilities Safety Board	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Office of the Inspector General	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Office of the Secretary - Wash. Hqtrs. Services	2	2	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Security Service	0	0	0.00%	0	0.00%	0	0.00%	5	5	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Technical Information Center	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Threat Reduction Agency	1	1	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%

Table B-24a FY 2012 Contract Staff Resources

Agency or Department	Contract Counselors							Contract Investigators							Contract Counselors/Investigators						
		Full Time		Part Time		Collateral Duty			Full Time		Part Time		Collateral Duty				Full Time		Part Time		Collateral Duty	
	Total	Number	%	Number	%	Number	%	Total	Number	%	Number	%	Number	%	Total	Number	%	Number	%	Number	%
Defense TRICARE Management Activity	0	0	0.00%	0	0.00%	0	0.00%	1	1	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Defense Uniformed Services University	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Department of Agriculture	12	2	16.67%	10	83.33%	0	0.00%	149	52	34.90%	97	65.10%	0	0.00%	51	6	11.76%	45	88.24%	0	0.00%
Department of Commerce	0	0	0.00%	0	0.00%	0	0.00%	34	0	0.00%	11	32.35%	23	67.65%	0	0	0.00%	0	0.00%	0	0.00%
Department of Defense Education Activity	2	0	0.00%	2	100.00%	0	0.00%	14	0	0.00%	14	100.00%	0	0.00%	2	0	0.00%	2	100.00%	0	0.00%
Department of Education	0	0	0.00%	0	0.00%	0	0.00%	8	8	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Department of Energy	0	0	0.00%	0	0.00%	0	0.00%	25	9	36.00%	16	64.00%	0	0.00%	10	0	0.00%	10	100.00%	0	0.00%
Department of Health and Human Services	103	76	73.79%	0	0.00%	27	26.21%	423	288	68.09%	0	0.00%	135	31.91%	137	96	70.07%	0	0.00%	41	29.93%
Department of Homeland Security	44	43	97.73%	0	0.00%	1	2.27%	216	85	39.35%	110	50.93%	21	9.72%	8	8	100.00%	0	0.00%	0	0.00%
Department of Housing and Urban Development	0	0	0.00%	0	0.00%	0	0.00%	42	19	45.24%	23	54.76%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Department of Justice	0	0	0.00%	0	0.00%	0	0.00%	109	100	91.74%	0	0.00%	9	8.26%	0	0	0.00%	0	0.00%	0	0.00%
Department of Labor	0	0	0.00%	0	0.00%	0	0.00%	38	38	100.00%	0	0.00%	0	0.00%	15	15	100.00%	0	0.00%	0	0.00%
Department of State	0	0	0.00%	0	0.00%	0	0.00%	25	25	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Department of the Air Force	4	4	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Department of the Army	2	0	0.00%	0	0.00%	2	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Department of the Interior	0	0	0.00%	0	0.00%	0	0.00%	55	40	72.73%	15	27.27%	0	0.00%	4	0	0.00%	4	100.00%	0	0.00%
Department of the Navy	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Department of the Treasury	5	0	0.00%	5	100.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Department of Transportation	3	0	0.00%	3	100.00%	0	0.00%	39	39	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Department of Veterans Affairs	37	2	5.41%	28	75.68%	7	18.92%	119	27	22.69%	79	66.39%	13	10.92%	40	8	20.00%	32	80.00%	0	0.00%
Election Assistance Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Environmental Protection Agency	0	0	0.00%	0	0.00%	0	0.00%	12	12	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Equal Employment Opportunity Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Export-Import Bank of the US	1	1	100.00%	0	0.00%	0	0.00%	1	1	100.00%	0	0.00%	0	0.00%	1	1	100.00%	0	0.00%	0	0.00%
Farm Credit Administration	3	3	100.00%	0	0.00%	0	0.00%	10	10	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Farm Credit System Insurance Corporation	3	3	100.00%	0	0.00%	0	0.00%	10	10	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Communications Commission	0	0	0.00%	0	0.00%	0	0.00%	2	2	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Deposit Insurance Corporation	2	2	100.00%	0	0.00%	0	0.00%	15	15	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Election Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Energy Regulatory Commission	1	0	0.00%	0	0.00%	1	100.00%	4	0	0.00%	0	0.00%	4	100.00%	1	0	0.00%	0	0.00%	1	100.00%
Federal Financial Institutions Examination Council	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Housing Finance Agency	1	0	0.00%	0	0.00%	1	100.00%	1	0	0.00%	0	0.00%	1	100.00%	5	0	0.00%	5	100.00%	0	0.00%
Federal Labor Relations Authority	0	0	0.00%	0	0.00%	0	0.00%	1	1	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Maritime Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Mediation and Conciliation Service	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Mine Safety & Health Review Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Reserve System--Board of Governors	0	0	0.00%	0	0.00%	0	0.00%	7	7	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Federal Retirement Thrift Investment Board	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Trade Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
General Services Administration	12	12	100.00%	0	0.00%	0	0.00%	69	69	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Government Printing Office	0	0	0.00%	0	0.00%	0	0.00%	5	5	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Harry S. Truman Scholarship Foundation	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Holocaust Memorial Museum U.S.	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Institute of Museum and Library Services	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Inter-American Foundation	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
International Boundary and Water Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
International Joint Commission: US and Canada	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
International Trade Commission	2	0	0.00%	0	0.00%	2	100.00%	2	0	0.00%	0	0.00%	2	100.00%	0	0	0.00%	0	0.00%	0	0.00%

Table B-24a FY 2012 Contract Staff Resources

Agency or Department	Contract Counselors							Contract Investigators							Contract Counselors/Investigators						
		Full Time		Part Time		Collateral Duty			Full Time		Part Time		Collateral Duty				Full Time		Part Time		Collateral Duty	
	Total	Number	%	Number	%	Number	%	Total	Number	%	Number	%	Number	%	Total	Number	%	Number	%	Number	%
James Madison Memorial Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Japan-United States Friendship Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
John F. Kennedy Center for the Performing Arts	2	0	0.00%	0	0.00%	2	100.00%	1	0	0.00%	0	0.00%	1	100.00%	0	0	0.00%	0	0.00%	0	0.00%
Marine Mammal Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Merit Systems Protection Board	0	0	0.00%	0	0.00%	0	0.00%	1	0	0.00%	0	0.00%	1	100.00%	0	0	0.00%	0	0.00%	0	0.00%
Millennium Challenge Corporation	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Aeronautics and Space Administration	6	3	50.00%	3	50.00%	0	0.00%	18	12	66.67%	0	0.00%	6	33.33%	1	1	100.00%	0	0.00%	0	0.00%
National Archives and Records Administration	0	0	0.00%	0	0.00%	0	0.00%	8	8	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Capital Planning Commission	1	0	0.00%	1	100.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Council on Disability	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Credit Union Administration	1	0	0.00%	1	100.00%	0	0.00%	4	0	0.00%	4	100.00%	0	0.00%	1	0	0.00%	1	100.00%	0	0.00%
National Endowment for the Arts	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Endowment for the Humanities	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Foundation on the Arts& the Humanities	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Gallery of Art	0	0	0.00%	0	0.00%	0	0.00%	1	1	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Indian Gaming Commission	1	1	100.00%	0	0.00%	0	0.00%	2	2	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Labor Relations Board	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Mediation Board	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Reconnaissance Office	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Science Foundation	3	0	0.00%	3	100.00%	0	0.00%	4	0	0.00%	4	100.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
National Transportation Safety Board	3	3	100.00%	0	0.00%	0	0.00%	7	7	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Navajo and Hopi Indian Relocation Commission	1	0	0.00%	0	0.00%	1	100.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Nuclear Regulatory Commission	0	0	0.00%	0	0.00%	0	0.00%	6	0	0.00%	6	100.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Nuclear Waste Technical Review Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Occupational Safety & Health Review Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Office of Government Ethics	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Office of Personnel Management	0	0	0.00%	0	0.00%	0	0.00%	2	0	0.00%	2	100.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Office of Special Counsel	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Office of the Director of National Intelligence	0	0	0.00%	0	0.00%	0	0.00%	1	0	0.00%	1	100.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Overseas Private Investment Corporation	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Peace Corps	1	0	0.00%	0	0.00%	1	100.00%	4	0	0.00%	0	0.00%	4	100.00%	5	0	0.00%	0	0.00%	5	100.00%
Pension Benefit Guaranty Corporation	0	0	0.00%	0	0.00%	0	0.00%	6	6	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Postal Regulatory Commission	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Presidio Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Railroad Retirement Board	0	0	0.00%	0	0.00%	0	0.00%	4	4	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Securities and Exchange Commission	2	0	0.00%	2	100.00%	0	0.00%	10	0	0.00%	10	100.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Selective Service System	1	1	100.00%	0	0.00%	0	0.00%	1	0	0.00%	1	100.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Small Business Administration	0	0	0.00%	0	0.00%	0	0.00%	25	25	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Smithsonian Institution	0	0	0.00%	0	0.00%	0	0.00%	4	4	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Social Security Administration	13	0	0.00%	13	100.00%	0	0.00%	79	0	0.00%	79	100.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Tennessee Valley Authority	0	0	0.00%	0	0.00%	0	0.00%	2	2	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
Trade and Development Agency	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%
U.S. Postal Service	0	0	0.00%	0	0.00%	0	0.00%	167	167	100.00%	0	0.00%	0	0.00%	0	0	0.00%	0	0.00%	0	0.00%

Table B-24a FY 2012 Contract Staff Resources

Agency or Department	Contract Counselors							Contract Investigators							Contract Counselors/Investigators						
		Full Time		Part Time		Collateral Duty			Full Time		Part Time		Collateral Duty				Full Time		Part Time		Collateral Duty	
	Total	Number	%	Number	%	Number	%	Total	Number	%	Number	%	Number	%	Total	Number	%	Number	%	Number	%
Utah Reclamation Mitigation and Conservation Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Valles Caldera Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Cabinet Level Subtotal	228	132	57.89%	59	25.88%	37	16.23%	1,479	904	61.12%	374	25.29%	201	13.59%	267	133	49.81%	93	34.83%	41	15.36%
Midsize Agencies Subtotal	33	17	51.52%	16	48.48%	0	0.00%	226	139	61.50%	81	35.84%	6	2.65%	1	1	100.00%	0	0.00%	0	0.00%
Small Agencies Subtotal	36	19	52.78%	10	27.78%	7	19.44%	123	69	56.10%	41	33.33%	13	10.57%	23	2	8.70%	15	65.22%	6	26.09%
Micro Agencies Subtotal	7	3	42.86%	3	42.86%	1	14.29%	27	11	40.74%	16	59.26%	0	0.00%	4	0	0.00%	4	100.00%	0	0.00%
Government-wide	304	171	56.25%	88	28.95%	45	14.80%	1,855	1,123	60.54%	512	27.60%	220	11.86%	295	136	46.10%	112	37.97%	47	15.93%

NRF = No Report Filed

Table B-25 FY 2012 Agency New Staff Training

Agency or Department	Total	Agency Counselors				Agency Investigators				Agency Counselors/Investigators			
		New Staff Training				New Staff Training				New Staff Training			
	Work Force	Total	32 Hour	8 Hour	None	Total	32 Hour	8 Hour	None	Total	32 Hour	8 Hour	None
Advisory Council on Historic Preservation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
African Development Foundation	73	0	0	0	0	0	0	0	0	0	0	0	0
Agency for International Development	3,983	13	13	0	0	1	1	0	0	0	0	0	0
American Battle Monuments Commission	76	0	0	0	0	0	0	0	0	0	0	0	0
Appalachian Regional Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Architectural and Transportation Barriers Compliance Board	28	0	0	0	0	0	0	0	0	0	0	0	0
Arctic Research Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Armed Forces Retirement Home	282	0	0	0	0	0	0	0	0	0	0	0	0
Barry Goldwater Scholarship and Excellence in Education Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Broadcasting Board of Governors	1,675	0	0	0	0	0	0	0	0	0	0	0	0
Central Intelligence Agency *	0	0	0	0	0	0	0	0	0	5	5	0	0
Chemical Safety and Hazard Investigation Board	46	0	0	0	0	0	0	0	0	0	0	0	0
Christopher Columbus Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission of Fine Arts	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission on Civil Rights	44	0	0	0	0	0	0	0	0	0	0	0	0
Committee for Purchase from People Who Are Blind or Severely Disabled	31	0	0	0	0	0	0	0	0	0	0	0	0
Commodity Futures Trading Commission	707	13	13	0	0	0	0	0	0	0	0	0	0
Consumer Financial Protection Bureau	970	0	0	0	0	0	0	0	0	0	0	0	0
Consumer Product Safety Commission	522	8	8	0	0	0	0	0	0	0	0	0	0
Corporation for National and Community Service	615	0	0	0	0	0	0	0	0	0	0	0	0
Court Services and Offender Supervision Agency for the District of Columbia	1,242	1	1	0	0	0	0	0	0	0	0	0	0
Defense Army and Air Force Exchange	34,273	63	63	0	0	0	0	0	0	0	0	0	0
Defense Commissary Agency	14,382	3	3	0	0	0	0	0	0	0	0	0	0
Defense Contract Audit Agency	5,181	1	0	1	0	0	0	0	0	0	0	0	0
Defense Contract Management Agency	10,452	2	2	0	0	0	0	0	0	0	0	0	0
Defense Finance and Accounting Service	11,982	0	0	0	0	0	0	0	0	0	0	0	0
Defense Human Resources Activity	1,176	0	0	0	0	0	0	0	0	0	0	0	0
Defense Information Systems Agency	6,304	0	0	0	0	0	0	0	0	0	0	0	0
Defense Intelligence Agency *	0	0	0	0	0	0	0	0	0	0	0	0	0
Defense Joint Task Force National Capital Region Medical	4,417	1	1	0	0	0	0	0	0	0	0	0	0
Defense Logistics Agency	25,229	9	1	6	2	0	0	0	0	0	0	0	0
Defense Media Activity	2,000	0	0	0	0	0	0	0	0	1	1	0	0
Defense Missile Defense Agency	2,326	1	1	0	0	0	0	0	0	0	0	0	0
Defense National Geospatial-Intelligence Agency *	0	5	5	0	0	0	0	0	0	0	0	0	0
Defense National Guard Bureau	57,511	81	80	26	3	1	1	0	0	4	4	0	0
Defense National Security Agency *	0	0	0	0	0	2	2	0	0	0	0	0	0

Table B-25 FY 2012 Agency New Staff Training

Agency or Department	Total Work Force	Agency Counselors New Staff Training				Agency Investigators New Staff Training				Agency Counselors/Investigators New Staff Training			
		Total	32 Hour	8 Hour	None	Total	32 Hour	8 Hour	None	Total	32 Hour	8 Hour	None
Defense Nuclear Facilities Safety Board	116	0	0	0	0	0	0	0	0	0	0	0	0
Defense Office of the Inspector General	1,600	0	0	0	0	0	0	0	0	0	0	0	0
Defense Office of the Secretary - Wash. Hqtrs. Services	6,766	0	0	0	0	19	19	0	0	0	0	0	0
Defense Security Service	874	1	1	0	0	0	0	0	0	0	0	0	0
Defense Technical Information Center	204	0	0	0	0	0	0	0	0	0	0	0	0
Defense Threat Reduction Agency	1,299	0	0	0	0	0	0	0	0	0	0	0	0
Defense TRICARE Management Activity	842	0	0	0	0	0	0	0	0	0	0	0	0
Defense Uniformed Services University	794	0	0	0	0	0	0	0	0	0	0	0	0
Department of Agriculture	103,822	6	5	0	1	0	0	0	0	0	0	0	0
Department of Commerce	45,766	5	5	0	0	0	0	0	0	0	0	0	0
Department of Defense Education Activity	16,346	1	1	0	0	0	0	0	0	0	0	0	0
Department of Education	4,373	0	0	0	0	0	0	0	0	0	0	0	0
Department of Energy	15,680	7	6	0	1	0	0	0	0	0	0	0	0
Department of Health and Human Services	83,123	14	14	0	0	0	0	0	0	0	0	0	0
Department of Homeland Security	200,559	18	10	3	5	6	6	0	0	0	0	0	0
Department of Housing and Urban Development	9,061	0	0	0	0	0	0	0	0	0	0	0	0
Department of Justice	116,973	46	46	0	0	0	0	0	0	0	0	0	0
Department of Labor	16,819	1	1	0	0	0	0	0	0	0	0	0	0
Department of State	69,885	231	231	0	0	0	0	0	0	0	0	0	0
Department of the Air Force	173,807	58	19	37	7	9	0	0	9	0	0	0	0
Department of the Army	250,617	137	130	70	0	0	0	0	0	0	0	0	0
Department of the Interior	78,779	15	15	0	0	0	0	0	0	0	0	0	0
Department of the Navy	245,574	37	35	0	2	0	0	0	0	0	0	0	0
Department of the Treasury	115,292	14	14	0	0	6	6	0	0	0	0	0	0
Department of Transportation	57,187	29	15	3	11	2	2	0	0	0	0	0	0
Department of Veterans Affairs	323,154	4	4	0	0	3	3	0	0	0	0	0	0
Election Assistance Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Environmental Protection Agency	17,001	0	0	0	0	0	0	0	0	0	0	0	0
Equal Employment Opportunity Commission	2,291	0	0	0	0	0	0	0	0	0	0	0	0
Export-Import Bank of the US	408	0	0	0	0	0	0	0	0	0	0	0	0
Farm Credit Administration	302	0	0	0	0	0	0	0	0	0	0	0	0
Farm Credit System Insurance Corporation	12	0	0	0	0	0	0	0	0	0	0	0	0
Federal Communications Commission	1,788	0	0	0	0	0	0	0	0	0	0	0	0
Federal Deposit Insurance Corporation	7,846	1	1	0	0	0	0	0	0	0	0	0	0
Federal Election Commission	355	0	0	0	0	0	0	0	0	0	0	0	0
Federal Energy Regulatory Commission	1,483	1	1	0	0	0	0	0	0	0	0	0	0
Federal Financial Institutions Examination Council	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Housing Finance Agency	706	1	1	0	0	0	0	0	0	0	0	0	0
Federal Labor Relations Authority	138	0	0	0	0	0	0	0	0	0	0	0	0
Federal Maritime Commission	124	2	2	0	0	0	0	0	0	0	0	0	0

Table B-25 FY 2012 Agency New Staff Training

Agency or Department	Total Work Force	Agency Counselors New Staff Training				Agency Investigators New Staff Training				Agency Counselors/Investigators New Staff Training			
		Total	32 Hour	8 Hour	None	Total	32 Hour	8 Hour	None	Total	32 Hour	8 Hour	None
Federal Mediation and Conciliation Service	243	0	0	0	0	0	0	0	0	0	0	0	0
Federal Mine Safety & Health Review Commission	78	0	0	0	0	0	0	0	0	0	0	0	0
Federal Reserve System--Board of Governors	2,412	0	0	0	0	0	0	0	0	0	0	0	0
Federal Retirement Thrift Investment Board	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Trade Commission	1,178	0	0	0	0	0	0	0	0	0	0	0	0
General Services Administration	12,416	0	0	0	0	0	0	0	0	0	0	0	0
Government Printing Office	1,879	0	0	0	0	0	0	0	0	0	0	0	0
Harry S. Truman Scholarship Foundation	5	0	0	0	0	0	0	0	0	0	0	0	0
Holocaust Memorial Museum U.S.	397	0	0	0	0	0	0	0	0	0	0	0	0
Institute of Museum and Library Services	88	1	0	1	0	0	0	0	0	0	0	0	0
Inter-American Foundation	43	0	0	0	0	0	0	0	0	0	0	0	0
International Boundary and Water Commission	258	2	2	0	0	0	0	0	0	0	0	0	0
International Joint Commission: US and Canada	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
International Trade Commission	397	0	0	0	0	0	0	0	0	0	0	0	0
James Madison Memorial Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Japan-United States Friendship Commission	4	1	1	0	0	0	0	0	0	0	0	0	0
John F. Kennedy Center for the Performing Arts	2,250	0	0	0	0	0	0	0	0	0	0	0	0
Marine Mammal Commission	14	0	0	0	0	0	0	0	0	0	0	0	0
Merit Systems Protection Board	208	0	0	0	0	0	0	0	0	0	0	0	0
Millennium Challenge Corporation	288	2	2	0	0	0	0	0	0	0	0	0	0
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Aeronautics and Space Administration	18,416	2	0	2	0	0	0	0	0	0	0	0	0
National Archives and Records Administration	3,381	0	0	0	0	0	0	0	0	0	0	0	0
National Capital Planning Commission	39	0	0	0	0	0	0	0	0	0	0	0	0
National Council on Disability	26	0	0	0	0	0	0	0	0	0	0	0	0
National Credit Union Administration	1,195	0	0	0	0	0	0	0	0	0	0	0	0
National Endowment for the Arts	174	0	0	0	0	0	0	0	0	0	0	0	0
National Endowment for the Humanities	199	0	0	0	0	0	0	0	0	0	0	0	0
National Foundation on the Arts & the Humanities	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Gallery of Art	834	5	5	0	0	0	0	0	0	0	0	0	0
National Indian Gaming Commission	97	0	0	0	0	0	0	0	0	0	0	0	0

Table B-25 FY 2012 Agency New Staff Training

Agency or Department	Total Work Force	Agency Counselors New Staff Training				Agency Investigators New Staff Training				Agency Counselors/Investigators New Staff Training			
		Total	32 Hour	8 Hour	None	Total	32 Hour	8 Hour	None	Total	32 Hour	8 Hour	None
National Labor Relations Board	1,702	8	6	2	2	0	0	0	0	0	0	0	0
National Mediation Board	50	2	2	0	0	0	0	0	0	0	0	0	0
National Reconnaissance Office *	0	0	0	0	0	0	0	0	0	0	0	0	0
National Science Foundation	1,663	0	0	0	0	0	0	0	0	0	0	0	0
National Transportation Safety Board	413	0	0	0	0	0	0	0	0	0	0	0	0
Navajo and Hopi Indian Relocation Commission	38	0	0	0	0	0	0	0	0	0	0	0	0
Nuclear Regulatory Commission	3,775	0	0	0	0	0	0	0	0	1	1	0	0
Nuclear Waste Technical Review Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Occupational Safety & Health Review Commission	58	0	0	0	0	0	0	0	0	0	0	0	0
Office of Government Ethics	69	0	0	0	0	0	0	0	0	0	0	0	0
Office of Personnel Management	5,843	2	2	0	0	0	0	0	0	0	0	0	0
Office of Special Counsel	129	1	1	0	0	0	0	0	0	0	0	0	0
Office of the Director of National Intelligence *	0	1	1	0	0	0	0	0	0	0	0	0	0
Overseas Private Investment Corporation	241	0	0	0	0	0	0	0	0	0	0	0	0
Peace Corps	896	5	5	0	0	0	0	0	0	5	5	0	0
Pension Benefit Guaranty Corporation	971	0	0	0	0	0	0	0	0	0	0	0	0
Postal Regulatory Commission	73	1	1	0	0	0	0	0	0	0	0	0	0
Presidio Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Railroad Retirement Board	945	0	0	0	0	0	0	0	0	0	0	0	0
Securities and Exchange Commission	3,826	3	3	0	0	0	0	0	0	0	0	0	0
Selective Service System	121	0	0	0	0	0	0	0	0	0	0	0	0
Small Business Administration	5,228	0	0	0	0	0	0	0	0	0	0	0	0
Smithsonian Institution	6,057	0	0	0	0	0	0	0	0	0	0	0	0
Social Security Administration	65,474	69	69	0	0	0	0	0	0	0	0	0	0
Tennessee Valley Authority	12,762	3	3	0	0	2	2	0	0	0	0	0	0
Trade and Development Agency	46	1	1	0	0	0	0	0	0	0	0	0	0
U.S. Postal Service	625,701	17	17	0	0	0	0	0	0	0	0	0	0
Utah Reclamation Mitigation and Conservation Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Valles Caldera Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Cabinet Level Subtotal	2,740,130	807	725	146	32	48	39	0	9	5	5	0	0
Midsize Agencies Subtotal	152,013	77	75	2	0	2	2	0	0	0	0	0	0
Small Agencies Subtotal	46,564	65	63	2	2	1	1	0	0	11	11	0	0
Micro Agencies Subtotal	1,286	7	6	1	0	0	0	0	0	0	0	0	0
Government-wide	2,939,993	956	869	151	34	51	42	0	9	16	16	0	0

NRF = No Report Filed

* Total work force numbers do not include employees not reported for national security reasons.

Table B-26 FY 2012 Agency Experienced Staff Training

Agency or Department	Total Work Force	Agency Counselors Experienced Staff Training				Agency Investigators Experienced Staff Training				Agency Counselors/Investigators Experienced Staff Training			
		Total	8 Hour	32 Hour	None	Total	8 Hour	32 Hour	None	Total	8 Hour	32 Hour	None
Advisory Council on Historic Preservation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
African Development Foundation	73	0	0	0	0	0	0	0	0	0	0	0	0
Agency for International Development	3,983	24	8	0	16	1	1	0	0	0	0	0	0
American Battle Monuments Commission	76	0	0	0	0	0	0	0	0	0	0	0	0
Appalachian Regional Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Architectural and Transportation Barriers Compliance Board	28	0	0	0	0	0	0	0	0	0	0	0	0
Arctic Research Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Armed Forces Retirement Home	282	0	0	0	0	0	0	0	0	0	0	0	0
Barry Goldwater Scholarship and Excellence in Education Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Broadcasting Board of Governors	1,675	4	2	2	0	0	0	0	0	4	4	0	0
Central Intelligence Agency *	0	0	0	0	0	1	1	0	0	7	7	0	0
Chemical Safety and Hazard Investigation Board	46	0	0	0	0	0	0	0	0	0	0	0	0
Christopher Columbus Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission of Fine Arts	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission on Civil Rights	44	1	1	0	0	0	0	0	0	0	0	0	0
Committee for Purchase from People Who Are Blind or Severely Disabled	31	0	0	0	0	0	0	0	0	0	0	0	0
Commodity Futures Trading Commission	707	7	5	0	2	0	0	0	0	0	0	0	0
Consumer Financial Protection Bureau	970	0	0	0	0	0	0	0	0	0	0	0	0
Consumer Product Safety Commission	522	2	2	0	0	0	0	0	0	0	0	0	0
Corporation for National and Community Service	615	0	0	0	0	0	0	0	0	0	0	0	0
Court Services and Offender Supervision Agency for the District of Columbia	1,242	14	14	0	0	0	0	0	0	2	2	0	0
Defense Army and Air Force Exchange	34,273	185	185	0	0	0	0	0	0	0	0	0	0
Defense Commissary Agency	14,382	1	0	1	0	0	0	0	0	0	0	0	0
Defense Contract Audit Agency	5,181	8	8	0	0	0	0	0	0	0	0	0	0
Defense Contract Management Agency	10,452	2	2	0	0	0	0	0	0	0	0	0	0
Defense Finance and Accounting Service	11,982	10	2	8	0	0	0	0	0	0	0	0	0
Defense Human Resources Activity	1,176	7	7	0	0	0	0	0	0	0	0	0	0
Defense Information Systems Agency	6,304	3	1	2	0	0	0	0	0	0	0	0	0
Defense Intelligence Agency *	0	5	3	2	0	0	0	0	0	0	0	0	0
Defense Joint Task Force National Capital Region Medical	4,417	0	0	0	0	0	0	0	0	0	0	0	0
Defense Logistics Agency	25,229	35	35	0	0	0	0	0	0	0	0	0	0
Defense Media Activity	2,000	3	3	0	0	0	0	0	0	0	0	0	0
Defense Missile Defense Agency	2,326	1	1	0	0	0	0	0	0	0	0	0	0
Defense National Geospatial-Intelligence Agency *	0	2	2	0	0	0	0	0	0	0	0	0	0
Defense National Guard Bureau	57,511	348	221	64	67	10	10	0	0	22	20	2	0

Table B-26 FY 2012 Agency Experienced Staff Training													
	Total Work	Agency Counselors Experienced Staff Training				Agency Investigators Experienced Staff Training				Agency Counselors/Investigators Experienced Staff Training			
Agency or Department	**Force**	**Total**	**8 Hour**	**32 Hour**	**None**	**Total**	**8 Hour**	**32 Hour**	**None**	**Total**	**8 Hour**	**32 Hour**	**None**
Defense National Security Agency *	0	1	1	0	0	5	5	2	0	3	3	0	0
Defense Nuclear Facilities Safety Board	116	3	1	0	2	0	0	0	0	0	0	0	0
Defense Office of the Inspector General	1,600	4	4	0	0	1	1	0	0	0	0	0	0
Defense Office of the Secretary - Wash. Hqtrs. Services	6,766	4	4	0	0	81	80	0	1	0	0	0	0
Defense Security Service	874	5	5	0	0	0	0	0	0	0	0	0	0
Defense Technical Information Center	204	7	7	0	0	0	0	0	0	0	0	0	0
Defense Threat Reduction Agency	1,299	3	3	0	0	0	0	0	0	0	0	0	0
Defense TRICARE Management Activity	842	1	0	1	0	0	0	0	0	0	0	0	0
Defense Uniformed Services University	794	4	4	0	0	0	0	0	0	0	0	0	0
Department of Agriculture	103,822	35	32	3	0	0	0	0	0	5	5	0	0
Department of Commerce	45,766	41	41	0	0	4	4	0	0	0	0	0	0
Department of Defense Education Activity	16,346	2	2	0	0	7	7	0	0	0	0	0	0
Department of Education	4,373	4	4	0	0	0	0	0	0	0	0	0	0
Department of Energy	15,680	67	62	5	0	0	0	0	0	0	0	0	0
Department of Health and Human Services	83,123	124	116	0	8	0	0	0	0	7	7	0	0
Department of Homeland Security	200,559	178	168	8	2	20	12	8	0	0	0	0	0
Department of Housing and Urban Development	9,061	4	4	0	0	0	0	0	0	0	0	0	0
Department of Justice	116,973	211	107	0	104	44	44	0	0	9	9	0	0
Department of Labor	16,819	14	14	0	0	0	0	0	0	0	0	0	0
Department of State	69,885	282	282	0	0	4	4	0	0	0	0	0	0
Department of the Air Force	173,807	317	196	6	120	131	0	0	131	0	0	0	0
Department of the Army	250,617	708	487	144	79	0	0	0	0	0	0	0	0
Department of the Interior	78,779	150	79	49	22	6	1	5	0	0	0	0	0
Department of the Navy	245,574	120	85	35	0	0	0	0	0	0	0	0	0
Department of the Treasury	115,292	81	79	0	2	15	15	0	0	4	4	0	0
Department of Transportation	57,187	50	35	8	7	4	4	0	0	0	0	0	0
Department of Veterans Affairs	323,154	23	23	0	0	48	48	0	0	0	0	0	0
Election Assistance Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Environmental Protection Agency	17,001	37	36	0	1	0	0	0	0	8	8	0	0
Equal Employment Opportunity Commission	2,291	1	1	0	0	1	1	0	0	1	1	0	0
Export-Import Bank of the US	408	0	0	0	0	0	0	0	0	0	0	0	0
Farm Credit Administration	302	0	0	0	0	0	0	0	0	0	0	0	0
Farm Credit System Insurance Corporation	12	0	0	0	0	0	0	0	0	0	0	0	0
Federal Communications Commission	1,788	6	6	0	0	0	0	0	0	6	6	0	0
Federal Deposit Insurance Corporation	7,846	5	5	0	0	0	0	0	0	0	0	0	0
Federal Election Commission	355	3	3	0	0	0	0	0	0	0	0	0	0
Federal Energy Regulatory Commission	1,483	4	4	0	0	0	0	0	0	0	0	0	0
Federal Financial Institutions Examination Council	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Housing Finance Agency	706	2	2	0	0	0	0	0	0	0	0	0	0

Table B-26 FY 2012 Agency Experienced Staff Training													
	Total Work	Agency Counselors Experienced Staff Training				Agency Investigators Experienced Staff Training				Agency Counselors/Investigators Experienced Staff Training			
Agency or Department	**Force**	**Total**	**8 Hour**	**32 Hour**	**None**	**Total**	**8 Hour**	**32 Hour**	**None**	**Total**	**8 Hour**	**32 Hour**	**None**
Federal Labor Relations Authority	138	3	3	0	0	0	0	0	0	0	0	0	0
Federal Maritime Commission	124	1	1	0	0	0	0	0	0	0	0	0	0
Federal Mediation and Conciliation Service	243	4	4	0	0	1	1	0	0	0	0	0	0
Federal Mine Safety & Health Review Commission	78	1	1	0	0	0	0	0	0	0	0	0	0
Federal Reserve System--Board of Governors	2,412	3	2	1	0	0	0	0	0	0	0	0	0
Federal Retirement Thrift Investment Board	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Trade Commission	1,178	9	1	0	8	0	0	0	0	0	0	0	0
General Services Administration	12,416	21	21	0	0	0	0	0	0	0	0	0	0
Government Printing Office	1,879	4	1	3	0	0	0	0	0	0	0	0	0
Harry S. Truman Scholarship Foundation	5	0	0	0	0	0	0	0	0	1	0	0	1
Holocaust Memorial Museum U.S.	397	5	5	0	0	0	0	0	0	0	0	0	0
Institute of Museum and Library Services	88	0	0	0	0	0	0	0	0	0	0	0	0
Inter-American Foundation	43	3	3	0	0	0	0	0	0	0	0	0	0
International Boundary and Water Commission	258	4	4	0	0	0	0	0	0	0	0	0	0
International Joint Commission: US and Canada	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
International Trade Commission	397	0	0	0	0	0	0	0	0	0	0	0	0
James Madison Memorial Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Japan-United States Friendship Commission	4	0	0	0	0	0	0	0	0	0	0	0	0
John F. Kennedy Center for the Performing Arts	2,250	0	0	0	0	0	0	0	0	0	0	0	0
Marine Mammal Commission	14	0	0	0	0	0	0	0	0	0	0	0	0
Merit Systems Protection Board	208	3	3	0	0	0	0	0	0	0	0	0	0
Millennium Challenge Corporation	288	1	1	0	0	0	0	0	0	0	0	0	0
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Aeronautics and Space Administration	18,416	27	16	8	3	0	0	0	0	0	0	0	0
National Archives and Records Administration	3,381	1	1	0	0	0	0	0	0	0	0	0	0
National Capital Planning Commission	39	0	0	0	0	0	0	0	0	0	0	0	0
National Council on Disability	26	0	0	0	0	0	0	0	0	0	0	0	0
National Credit Union Administration	1,195	6	6	0	0	0	0	0	0	0	0	0	0
National Endowment for the Arts	174	2	2	0	0	0	0	0	0	0	0	0	0
National Endowment for the Humanities	199	2	2	0	0	0	0	0	0	0	0	0	0
National Foundation on the Arts & the Humanities	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Gallery of Art	834	5	5	0	0	0	0	0	0	0	0	0	0
National Indian Gaming Commission	97	1	1	0	0	0	0	0	0	0	0	0	0
National Labor Relations Board	1,702	35	26	0	9	1	1	0	0	4	4	0	0
National Mediation Board	50	0	0	0	0	0	0	0	0	0	0	0	0
National Reconnaissance Office *	0	0	0	0	0	0	0	0	0	3	3	0	0
National Science Foundation	1,663	0	0	0	0	0	0	0	0	0	0	0	0
National Transportation Safety Board	413	0	0	0	0	0	0	0	0	0	0	0	0
Navajo and Hopi Indian Relocation Commission	38	0	0	0	0	0	0	0	0	0	0	0	0

Table B-26 FY 2012 Agency Experienced Staff Training													
	Total Work	Agency Counselors Experienced Staff Training				Agency Investigators Experienced Staff Training				Agency Counselors/Investigators Experienced Staff Training			
Agency or Department	**Force**	**Total**	**8 Hour**	**32 Hour**	**None**	**Total**	**8 Hour**	**32 Hour**	**None**	**Total**	**8 Hour**	**32 Hour**	**None**
Nuclear Regulatory Commission	3,775	22	22	0	0	0	0	0	0	2	2	0	0
Nuclear Waste Technical Review Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Occupational Safety & Health Review Commission	58	1	1	0	0	0	0	0	0	0	0	0	0
Office of Government Ethics	69	0	0	0	0	0	0	0	0	0	0	0	0
Office of Personnel Management	5,843	2	2	0	0	0	0	0	0	5	5	0	0
Office of Special Counsel	129	4	2	0	2	0	0	0	0	0	0	0	0
Office of the Director of National Intelligence *	0	3	3	0	0	0	0	0	0	2	2	0	0
Overseas Private Investment Corporation	241	2	1	0	1	0	0	0	0	0	0	0	0
Peace Corps	896	6	6	0	0	0	0	0	0	6	6	0	0
Pension Benefit Guaranty Corporation	971	2	2	0	0	0	0	0	0	0	0	0	0
Postal Regulatory Commission	73	0	0	0	0	1	0	1	0	0	0	0	0
Presidio Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Railroad Retirement Board	945	3	2	0	1	0	0	0	0	0	0	0	0
Securities and Exchange Commission	3,826	6	6	0	0	0	0	0	0	0	0	0	0
Selective Service System	121	1	1	0	0	0	0	0	0	0	0	0	0
Small Business Administration	5,228	3	3	0	0	2	2	0	0	0	0	0	0
Smithsonian Institution	6,057	3	3	0	0	0	0	0	0	0	0	0	0
Social Security Administration	65,474	165	119	40	6	0	0	0	0	0	0	0	0
Tennessee Valley Authority	12,762	17	17	0	0	2	2	0	0	0	0	0	0
Trade and Development Agency	46	1	1	0	0	0	0	0	0	0	0	0	0
U.S. Postal Service	625,701	95	92	0	3	0	0	0	0	0	0	0	0
Utah Reclamation Mitigation and Conservation Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Valles Caldera Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Cabinet Level Subtotal	2,740,130	3,145	2,406	336	414	380	235	15	132	50	48	2	0
Midsize Agencies Subtotal	152,013	280	222	48	10	4	4	0	0	13	13	0	0
Small Agencies Subtotal	46,564	201	158	6	37	5	5	0	0	37	37	0	0
Micro Agencies Subtotal	1,286	14	10	0	4	1	0	1	0	1	0	0	1
Government-wide	2,939,993	3,640	2,796	390	465	390	244	16	132	101	98	2	1

NRF = No Report Filed

* Total work force numbers do not include employees not reported for national security reasons.

Table B-27 FY 2012 Contractor New Staff Training

Agency or Department	Total Work Force	Contract Counselors New Staff Training				Contract Investigators New Staff Training				Contract Counselors/Investigators New Staff Training			
		Total	32 Hour	8 Hour	None	Total	32 Hour	8 Hour	None	Total	32 Hour	8 Hour	None
Advisory Council on Historic Preservation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
African Development Foundation	73	0	0	0	0	0	0	0	0	0	0	0	0
Agency for International Development	3,983	0	0	0	0	0	0	0	0	0	0	0	0
American Battle Monuments Commission	76	0	0	0	0	1	1	0	0	0	0	0	0
Appalachian Regional Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Architectural and Transportation Barriers Compliance Board	28	0	0	0	0	0	0	0	0	0	0	0	0
Arctic Research Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Armed Forces Retirement Home	282	0	0	0	0	0	0	0	0	0	0	0	0
Barry Goldwater Scholarship and Excellence in Education Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Broadcasting Board of Governors	1,675	0	0	0	0	0	0	0	0	0	0	0	0
Central Intelligence Agency *	0	0	0	0	0	0	0	0	0	0	0	0	0
Chemical Safety and Hazard Investigation Board	46	1	1	0	0	1	1	0	0	0	0	0	0
Christopher Columbus Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission of Fine Arts	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission on Civil Rights	44	0	0	0	0	0	0	0	0	0	0	0	0
Committee for Purchase from People Who Are Blind or Severely Disabled	31	0	0	0	0	0	0	0	0	0	0	0	0
Commodity Futures Trading Commission	707	0	0	0	0	0	0	0	0	0	0	0	0
Consumer Financial Protection Bureau	970	0	0	0	0	0	0	0	0	0	0	0	0
Consumer Product Safety Commission	522	0	0	0	0	0	0	0	0	0	0	0	0
Corporation for National and Community Service	615	0	0	0	0	0	0	0	0	0	0	0	0
Court Services and Offender Supervision Agency for the District of Columbia	1,242	0	0	0	0	0	0	0	0	0	0	0	0
Defense Army and Air Force Exchange	34,273	0	0	0	0	0	0	0	0	0	0	0	0
Defense Commissary Agency	14,382	0	0	0	0	0	0	0	0	0	0	0	0
Defense Contract Audit Agency	5,181	0	0	0	0	0	0	0	0	0	0	0	0
Defense Contract Management Agency	10,452	0	0	0	0	0	0	0	0	0	0	0	0
Defense Finance and Accounting Service	11,982	0	0	0	0	0	0	0	0	0	0	0	0
Defense Human Resources Activity	1,176	0	0	0	0	2	2	0	0	0	0	0	0
Defense Information Systems Agency	6,304	0	0	0	0	0	0	0	0	0	0	0	0
Defense Intelligence Agency *	0	0	0	0	0	1	0	1	0	0	0	0	0
Defense Joint Task Force National Capital Region Medical	4,417	0	0	0	0	1	1	0	0	0	0	0	0
Defense Logistics Agency	25,229	0	0	0	0	0	0	0	0	0	0	0	0
Defense Media Activity	2,000	0	0	0	0	0	0	0	0	0	0	0	0
Defense Missile Defense Agency	2,326	0	0	0	0	0	0	0	0	0	0	0	0
Defense National Geospatial-Intelligence Agency *	0	0	0	0	0	0	0	0	0	0	0	0	0
Defense National Guard Bureau	57,511	0	0	0	0	0	0	0	0	0	0	0	0

Table B-27 FY 2012 Contractor New Staff Training													
	Total	Contract Counselors				Contract Investigators				Contract Counselors/Investigators			
	Work	New Staff Training				New Staff Training				New Staff Training			
Agency or Department	Force	Total	32 Hour	8 Hour	None	Total	32 Hour	8 Hour	None	Total	32 Hour	8 Hour	None
Defense National Security Agency *	0	0	0	0	0	0	0	0	0	0	0	0	0
Defense Nuclear Facilities Safety Board	116	0	0	0	0	0	0	0	0	0	0	0	0
Defense Office of the Inspector General	1,600	0	0	0	0	0	0	0	0	0	0	0	0
Defense Office of the Secretary - Wash. Hqtrs. Services	6,766	0	0	0	0	0	0	0	0	0	0	0	0
Defense Security Service	874	0	0	0	0	0	0	0	0	0	0	0	0
Defense Technical Information Center	204	0	0	0	0	0	0	0	0	0	0	0	0
Defense Threat Reduction Agency	1,299	0	0	0	0	0	0	0	0	0	0	0	0
Defense TRICARE Management Activity	842	0	0	0	0	1	1	0	0	0	0	0	0
Defense Uniformed Services University	794	0	0	0	0	0	0	0	0	0	0	0	0
Department of Agriculture	103,822	0	0	0	0	0	0	0	0	0	0	0	0
Department of Commerce	45,766	0	0	0	0	0	0	0	0	0	0	0	0
Department of Defense Education Activity	16,346	0	0	0	0	0	0	0	0	0	0	0	0
Department of Education	4,373	0	0	0	0	0	0	0	0	0	0	0	0
Department of Energy	15,680	0	0	0	0	0	0	0	0	2	2	0	0
Department of Health and Human Services	83,123	15	9	9	0	75	51	41	0	35	15	25	0
Department of Homeland Security	200,559	0	0	0	0	2	2	0	0	0	0	0	0
Department of Housing and Urban Development	9,061	0	0	0	0	0	0	0	0	0	0	0	0
Department of Justice	116,973	0	0	0	0	1	1	0	0	0	0	0	0
Department of Labor	16,819	0	0	0	0	0	0	0	0	0	0	0	0
Department of State	69,885	0	0	0	0	0	0	0	0	0	0	0	0
Department of the Air Force	173,807	0	0	0	0	0	0	0	0	0	0	0	0
Department of the Army	250,617	0	0	0	0	0	0	0	0	0	0	0	0
Department of the Interior	78,779	0	0	0	0	5	0	5	0	0	0	0	0
Department of the Navy	245,574	0	0	0	0	0	0	0	0	0	0	0	0
Department of the Treasury	115,292	0	0	0	0	0	0	0	0	0	0	0	0
Department of Transportation	57,187	0	0	0	0	0	0	0	0	0	0	0	0
Department of Veterans Affairs	323,154	4	4	0	0	6	5	1	0	4	4	0	0
Election Assistance Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Environmental Protection Agency	17,001	0	0	0	0	0	0	0	0	0	0	0	0
Equal Employment Opportunity Commission	2,291	0	0	0	0	0	0	0	0	0	0	0	0
Export-Import Bank of the US	408	0	0	0	0	0	0	0	0	0	0	0	0
Farm Credit Administration	302	0	0	0	0	0	0	0	0	0	0	0	0
Farm Credit System Insurance Corporation	12	0	0	0	0	0	0	0	0	0	0	0	0
Federal Communications Commission	1,788	0	0	0	0	0	0	0	0	0	0	0	0
Federal Deposit Insurance Corporation	7,846	0	0	0	0	0	0	0	0	0	0	0	0
Federal Election Commission	355	0	0	0	0	0	0	0	0	0	0	0	0
Federal Energy Regulatory Commission	1,483	0	0	0	0	0	0	0	0	0	0	0	0
Federal Financial Institutions Examination Council	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Housing Finance Agency	706	0	0	0	0	0	0	0	0	0	0	0	0

Table B-27 FY 2012 Contractor New Staff Training													
	Total	Contract Counselors				Contract Investigators				Contract Counselors/Investigators			
	Work	New Staff Training				New Staff Training				New Staff Training			
Agency or Department	Force	Total	32 Hour	8 Hour	None	Total	32 Hour	8 Hour	None	Total	32 Hour	8 Hour	None
Federal Labor Relations Authority	138	0	0	0	0	0	0	0	0	0	0	0	0
Federal Maritime Commission	124	0	0	0	0	0	0	0	0	0	0	0	0
Federal Mediation and Conciliation Service	243	0	0	0	0	0	0	0	0	0	0	0	0
Federal Mine Safety & Health Review Commission	78	0	0	0	0	0	0	0	0	0	0	0	0
Federal Reserve System--Board of Governors	2,412	0	0	0	0	0	0	0	0	0	0	0	0
Federal Retirement Thrift Investment Board	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Trade Commission	1,178	0	0	0	0	0	0	0	0	0	0	0	0
General Services Administration	12,416	0	0	0	0	0	0	0	0	0	0	0	0
Government Printing Office	1,879	0	0	0	0	0	0	0	0	0	0	0	0
Harry S. Truman Scholarship Foundation	5	0	0	0	0	0	0	0	0	0	0	0	0
Holocaust Memorial Museum U.S.	397	0	0	0	0	0	0	0	0	0	0	0	0
Institute of Museum and Library Services	88	0	0	0	0	0	0	0	0	0	0	0	0
Inter-American Foundation	43	0	0	0	0	0	0	0	0	0	0	0	0
International Boundary and Water Commission	258	0	0	0	0	0	0	0	0	0	0	0	0
International Joint Commission: US and Canada	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
International Trade Commission	397	0	0	0	0	0	0	0	0	0	0	0	0
James Madison Memorial Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Japan-United States Friendship Commission	4	0	0	0	0	0	0	0	0	0	0	0	0
John F. Kennedy Center for the Performing Arts	2,250	0	0	0	0	0	0	0	0	0	0	0	0
Marine Mammal Commission	14	0	0	0	0	0	0	0	0	0	0	0	0
Merit Systems Protection Board	208	0	0	0	0	0	0	0	0	0	0	0	0
Millennium Challenge Corporation	288	0	0	0	0	0	0	0	0	0	0	0	0
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Aeronautics and Space Administration	18,416	0	0	0	0	1	1	0	0	0	0	0	0
National Archives and Records Administration	3,381	0	0	0	0	0	0	0	0	0	0	0	0
National Capital Planning Commission	39	0	0	0	0	0	0	0	0	0	0	0	0
National Council on Disability	26	0	0	0	0	0	0	0	0	0	0	0	0
National Credit Union Administration	1,195	0	0	0	0	0	0	0	0	0	0	0	0
National Endowment for the Arts	174	0	0	0	0	0	0	0	0	0	0	0	0
National Endowment for the Humanities	199	0	0	0	0	0	0	0	0	0	0	0	0
National Foundation on the Arts &the Humanities	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Gallery of Art	834	0	0	0	0	0	0	0	0	0	0	0	0
National Indian Gaming Commission	97	0	0	0	0	0	0	0	0	0	0	0	0
National Labor Relations Board	1,702	0	0	0	0	0	0	0	0	0	0	0	0
National Mediation Board	50	0	0	0	0	0	0	0	0	0	0	0	0
National Reconnaissance Office *	0	0	0	0	0	0	0	0	0	0	0	0	0
National Science Foundation	1,663	0	0	0	0	0	0	0	0	0	0	0	0
National Transportation Safety Board	413	0	0	0	0	0	0	0	0	0	0	0	0
Navajo and Hopi Indian Relocation Commission	38	0	0	0	0	0	0	0	0	0	0	0	0

Table B-27 FY 2012 Contractor New Staff Training													
	Total	Contract Counselors				Contract Investigators				Contract Counselors/Investigators			
	Work	New Staff Training				New Staff Training				New Staff Training			
Agency or Department	Force	Total	32 Hour	8 Hour	None	Total	32 Hour	8 Hour	None	Total	32 Hour	8 Hour	None
Nuclear Regulatory Commission	3,775	0	0	0	0	0	0	0	0	0	0	0	0
Nuclear Waste Technical Review Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Occupational Safety & Health Review Commission	58	0	0	0	0	0	0	0	0	0	0	0	0
Office of Government Ethics	69	0	0	0	0	0	0	0	0	0	0	0	0
Office of Personnel Management	5,843	0	0	0	0	0	0	0	0	0	0	0	0
Office of Special Counsel	129	0	0	0	0	0	0	0	0	0	0	0	0
Office of the Director of National Intelligence *	0	0	0	0	0	0	0	0	0	0	0	0	0
Overseas Private Investment Corporation	241	0	0	0	0	0	0	0	0	0	0	0	0
Peace Corps	896	0	0	0	0	0	0	0	0	0	0	0	0
Pension Benefit Guaranty Corporation	971	0	0	0	0	0	0	0	0	0	0	0	0
Postal Regulatory Commission	73	0	0	0	0	0	0	0	0	0	0	0	0
Presidio Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Railroad Retirement Board	945	0	0	0	0	0	0	0	0	0	0	0	0
Securities and Exchange Commission	3,826	0	0	0	0	0	0	0	0	0	0	0	0
Selective Service System	121	0	0	0	0	0	0	0	0	0	0	0	0
Small Business Administration	5,228	0	0	0	0	0	0	0	0	0	0	0	0
Smithsonian Institution	6,057	0	0	0	0	0	0	0	0	0	0	0	0
Social Security Administration	65,474	0	0	0	0	0	0	0	0	0	0	0	0
Tennessee Valley Authority	12,762	0	0	0	0	0	0	0	0	0	0	0	0
Trade and Development Agency	46	0	0	0	0	0	0	0	0	0	0	0	0
U.S. Postal Service	625,701	0	0	0	0	56	56	0	0	0	0	0	0
Utah Reclamation Mitigation and Conservation Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Valles Caldera Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Cabinet Level Subtotal	2,740,130	19	13	9	0	150	119	48	0	41	21	25	0
Midsize Agencies Subtotal	152,013	0	0	0	0	1	1	0	0	0	0	0	0
Small Agencies Subtotal	46,564	0	0	0	0	0	0	0	0	0	0	0	0
Micro Agencies Subtotal	1,286	1	1	0	0	2	2	0	0	0	0	0	0
Government-wide	2,939,993	20	14	9	0	153	122	48	0	41	21	25	0

NRF = No Report Filed

* Total work force numbers do not include employees not reported for national security reasons.

Table B-28 FY 2012 Contractor Experienced Staff Training

Agency or Department	Total Work Force	Contract Counselors				Contract Investigators				Contract Counselors/Investigators			
		Experienced Staff Training				Experienced Staff Training				Experienced Staff Training			
		Total	8 Hour	32 Hour	None	Total	8 Hour	32 Hour	None	Total	8 Hour	32 Hour	None
Advisory Council on Historic Preservation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
African Development Foundation	73	1	1	0	0	1	1	0	0	0	0	0	0
Agency for International Development	3,983	0	0	0	0	9	9	0	0	0	0	0	0
American Battle Monuments Commission	76	0	0	0	0	14	14	0	0	3	2	0	1
Appalachian Regional Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Architectural and Transportation Barriers Compliance Board	28	0	0	0	0	0	0	0	0	0	0	0	0
Arctic Research Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Armed Forces Retirement Home	282	0	0	0	0	0	0	0	0	0	0	0	0
Barry Goldwater Scholarship and Excellence in Education Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Broadcasting Board of Governors	1,675	4	4	0	0	5	5	0	0	9	9	0	0
Central Intelligence Agency *	0	0	0	0	0	1	1	0	0	0	0	0	0
Chemical Safety and Hazard Investigation Board	46	0	0	0	0	0	0	0	0	0	0	0	0
Christopher Columbus Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission of Fine Arts	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Commission on Civil Rights	44	0	0	0	0	0	0	0	0	0	0	0	0
Committee for Purchase from People Who Are Blind or Severely Disabled	31	0	0	0	0	0	0	0	0	1	1	0	0
Commodity Futures Trading Commission	707	0	0	0	0	1	1	0	0	0	0	0	0
Consumer Financial Protection Bureau	970	0	0	0	0	0	0	0	0	0	0	0	0
Consumer Product Safety Commission	522	0	0	0	0	4	4	0	0	0	0	0	0
Corporation for National and Community Service	615	10	0	10	0	10	0	10	0	0	0	0	0
Court Services and Offender Supervision Agency for the District of Columbia	1,242	0	0	0	0	0	0	0	0	1	1	0	0
Defense Army and Air Force Exchange	34,273	0	0	0	0	0	0	0	0	0	0	0	0
Defense Commissary Agency	14,382	0	0	0	0	0	0	0	0	0	0	0	0
Defense Contract Audit Agency	5,181	6	6	0	0	6	6	0	0	0	0	0	0
Defense Contract Management Agency	10,452	0	0	0	0	0	0	0	0	0	0	0	0
Defense Finance and Accounting Service	11,982	0	0	0	0	0	0	0	0	0	0	0	0
Defense Human Resources Activity	1,176	0	0	0	0	0	0	0	0	0	0	0	0
Defense Information Systems Agency	6,304	2	2	0	0	0	0	0	0	0	0	0	0
Defense Intelligence Agency *	0	0	0	0	0	0	0	0	0	0	0	0	0
Defense Joint Task Force National Capital Region Medical	4,417	0	0	0	0	0	0	0	0	0	0	0	0
Defense Logistics Agency	25,229	3	3	0	0	0	0	0	0	0	0	0	0
Defense Media Activity	2,000	0	0	0	0	0	0	0	0	0	0	0	0
Defense Missile Defense Agency	2,326	0	0	0	0	0	0	0	0	0	0	0	0
Defense National Geospatial-Intelligence Agency *	0	0	0	0	0	0	0	0	0	0	0	0	0
Defense National Guard Bureau	57,511	2	2	0	0	0	0	0	0	0	0	0	0
Defense National Security Agency *	0	0	0	0	0	0	0	0	0	0	0	0	0
Defense Nuclear Facilities Safety Board	116	0	0	0	0	0	0	0	0	0	0	0	0
Defense Office of the Inspector General	1,600	0	0	0	0	0	0	0	0	0	0	0	0

Table B-28 FY 2012 Contractor Experienced Staff Training

Agency or Department	Total Work Force	Contract Counselors				Contract Investigators				Contract Counselors/Investigators			
		Experienced Staff Training				Experienced Staff Training				Experienced Staff Training			
		Total	8 Hour	32 Hour	None	Total	8 Hour	32 Hour	None	Total	8 Hour	32 Hour	None
Defense Office of the Secretary - Wash. Hqtrs. Services	6,766	2	2	0	0	0	0	0	0	0	0	0	0
Defense Security Service	874	0	0	0	0	5	5	0	0	0	0	0	0
Defense Technical Information Center	204	0	0	0	0	0	0	0	0	0	0	0	0
Defense Threat Reduction Agency	1,299	1	1	0	0	0	0	0	0	0	0	0	0
Defense TRICARE Management Activity	842	0	0	0	0	0	0	0	0	0	0	0	0
Defense Uniformed Services University	794	0	0	0	0	0	0	0	0	0	0	0	0
Department of Agriculture	103,822	12	10	2	0	149	130	19	0	51	51	0	0
Department of Commerce	45,766	0	0	0	0	34	34	0	0	0	0	0	0
Department of Defense Education Activity	16,346	2	2	0	0	14	14	0	0	2	2	0	0
Department of Education	4,373	0	0	0	0	8	8	0	0	0	0	0	0
Department of Energy	15,680	0	0	0	0	25	25	0	0	8	8	0	0
Department of Health and Human Services	83,123	88	51	37	0	348	153	195	0	102	54	48	0
Department of Homeland Security	200,559	44	44	0	0	214	214	0	0	8	8	0	0
Department of Housing and Urban Development	9,061	0	0	0	0	42	42	0	0	0	0	0	0
Department of Justice	116,973	0	0	0	0	108	108	0	0	0	0	0	0
Department of Labor	16,819	0	0	0	0	38	38	0	0	15	15	0	0
Department of State	69,885	0	0	0	0	25	25	0	0	0	0	0	0
Department of the Air Force	173,807	4	0	0	4	0	0	0	0	0	0	0	0
Department of the Army	250,617	2	0	2	0	0	0	0	0	0	0	0	0
Department of the Interior	78,779	0	0	0	0	50	21	20	9	4	4	0	0
Department of the Navy	245,574	0	0	0	0	0	0	0	0	0	0	0	0
Department of the Treasury	115,292	5	5	0	0	0	0	0	0	0	0	0	0
Department of Transportation	57,187	3	3	0	0	39	36	3	0	0	0	0	0
Department of Veterans Affairs	323,154	33	33	0	0	113	113	0	0	36	36	0	0
Election Assistance Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Environmental Protection Agency	17,001	0	0	0	0	12	12	0	0	0	0	0	0
Equal Employment Opportunity Commission	2,291	0	0	0	0	0	0	0	0	0	0	0	0
Export-Import Bank of the US	408	1	1	0	0	1	1	0	0	1	1	0	0
Farm Credit Administration	302	3	3	0	0	10	10	0	0	0	0	0	0
Farm Credit System Insurance Corporation	12	3	3	0	0	10	10	0	0	0	0	0	0
Federal Communications Commission	1,788	0	0	0	0	2	2	0	0	0	0	0	0
Federal Deposit Insurance Corporation	7,846	2	2	0	0	15	15	0	0	0	0	0	0
Federal Election Commission	355	0	0	0	0	0	0	0	0	0	0	0	0
Federal Energy Regulatory Commission	1,483	1	1	0	0	4	4	0	0	1	1	0	0
Federal Financial Institutions Examination Council	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Federal Housing Finance Agency	706	1	1	0	0	1	1	0	0	5	5	0	0
Federal Labor Relations Authority	138	0	0	0	0	1	1	0	0	0	0	0	0
Federal Maritime Commission	124	0	0	0	0	0	0	0	0	0	0	0	0
Federal Mediation and Conciliation Service	243	0	0	0	0	0	0	0	0	0	0	0	0
Federal Mine Safety & Health Review Commission	78	0	0	0	0	0	0	0	0	0	0	0	0
Federal Reserve System--Board of Governors	2,412	0	0	0	0	7	7	0	0	0	0	0	0
Federal Retirement Thrift Investment Board	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF

Table B-28 FY 2012 Contractor Experienced Staff Training

Agency or Department	Total Work Force	Contract Counselors				Contract Investigators				Contract Counselors/Investigators			
		Experienced Staff Training				Experienced Staff Training				Experienced Staff Training			
		Total	8 Hour	32 Hour	None	Total	8 Hour	32 Hour	None	Total	8 Hour	32 Hour	None
Federal Trade Commission	1,178	0	0	0	0	0	0	0	0	0	0	0	0
General Services Administration	12,416	12	12	0	0	69	63	6	0	0	0	0	0
Government Printing Office	1,879	0	0	0	0	5	5	0	0	0	0	0	0
Harry S. Truman Scholarship Foundation	5	0	0	0	0	0	0	0	0	0	0	0	0
Holocaust Memorial Museum U.S.	397	0	0	0	0	0	0	0	0	0	0	0	0
Institute of Museum and Library Services	88	0	0	0	0	0	0	0	0	0	0	0	0
Inter-American Foundation	43	0	0	0	0	0	0	0	0	0	0	0	0
International Boundary and Water Commission	258	0	0	0	0	0	0	0	0	0	0	0	0
International Joint Commission: US and Canada	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
International Trade Commission	397	2	2	0	0	2	2	0	0	0	0	0	0
James Madison Memorial Fellowship Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Japan-United States Friendship Commission	4	0	0	0	0	0	0	0	0	0	0	0	0
John F. Kennedy Center for the Performing Arts	2,250	2	2	0	0	1	1	0	0	0	0	0	0
Marine Mammal Commission	14	0	0	0	0	0	0	0	0	0	0	0	0
Merit Systems Protection Board	208	0	0	0	0	1	1	0	0	0	0	0	0
Millennium Challenge Corporation	288	0	0	0	0	0	0	0	0	0	0	0	0
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Aeronautics and Space Administration	18,416	6	6	0	0	17	17	0	0	1	0	1	0
National Archives and Records Administration	3,381	0	0	0	0	8	8	0	0	0	0	0	0
National Capital Planning Commission	39	1	1	0	0	0	0	0	0	0	0	0	0
National Council on Disability	26	0	0	0	0	0	0	0	0	0	0	0	0
National Credit Union Administration	1,195	1	1	0	0	4	4	0	0	1	1	0	0
National Endowment for the Arts	174	0	0	0	0	0	0	0	0	0	0	0	0
National Endowment for the Humanities	199	0	0	0	0	0	0	0	0	0	0	0	0
National Foundation on the Arts & the Humanities	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
National Gallery of Art	834	0	0	0	0	1	1	0	0	0	0	0	0
National Indian Gaming Commission	97	1	1	0	0	2	2	0	0	0	0	0	0
National Labor Relations Board	1,702	0	0	0	0	0	0	0	0	0	0	0	0
National Mediation Board	50	0	0	0	0	0	0	0	0	0	0	0	0
National Reconnaissance Office *	0	0	0	0	0	0	0	0	0	0	0	0	0
National Science Foundation	1,663	3	3	0	0	4	4	0	0	0	0	0	0
National Transportation Safety Board	413	3	3	0	0	7	7	0	0	0	0	0	0
Navajo and Hopi Indian Relocation Commission	38	1	1	0	0	0	0	0	0	0	0	0	0
Nuclear Regulatory Commission	3,775	0	0	0	0	6	6	0	0	0	0	0	0
Nuclear Waste Technical Review Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Occupational Safety & Health Review Commission	58	0	0	0	0	0	0	0	0	0	0	0	0
Office of Government Ethics	69	0	0	0	0	0	0	0	0	0	0	0	0
Office of Personnel Management	5,843	0	0	0	0	2	2	0	0	0	0	0	0
Office of Special Counsel	129	0	0	0	0	0	0	0	0	0	0	0	0
Office of the Director of National Intelligence *	0	0	0	0	0	1	1	0	0	0	0	0	0
Overseas Private Investment Corporation	241	0	0	0	0	0	0	0	0	0	0	0	0
Peace Corps	896	1	1	0	0	4	4	0	0	5	5	0	0

Table B-28 FY 2012 Contractor Experienced Staff Training													
Agency or Department	**Total**	**Contract Counselors**				**Contract Investigators**				**Contract Counselors/Investigators**			
	Work	**Experienced Staff Training**				**Experienced Staff Training**				**Experienced Staff Training**			
	Force	**Total**	**8 Hour**	**32 Hour**	**None**	**Total**	**8 Hour**	**32 Hour**	**None**	**Total**	**8 Hour**	**32 Hour**	**None**
Pension Benefit Guaranty Corporation	971	0	0	0	0	6	6	0	0	0	0	0	0
Postal Regulatory Commission	73	0	0	0	0	0	0	0	0	0	0	0	0
Presidio Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Railroad Retirement Board	945	0	0	0	0	4	4	0	0	0	0	0	0
Securities and Exchange Commission	3,826	2	2	0	0	10	10	0	0	0	0	0	0
Selective Service System	121	1	1	0	0	1	1	0	0	0	0	0	0
Small Business Administration	5,228	0	0	0	0	25	25	0	0	0	0	0	0
Smithsonian Institution	6,057	0	0	0	0	4	4	0	0	0	0	0	0
Social Security Administration	65,474	13	13	0	0	79	79	0	0	0	0	0	0
Tennessee Valley Authority	12,762	0	0	0	0	2	2	0	0	0	0	0	0
Trade and Development Agency	46	0	0	0	0	0	0	0	0	0	0	0	0
U.S. Postal Service	625,701	0	0	0	0	111	111	0	0	0	0	0	0
Utah Reclamation Mitigation and Conservation Commission	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Valles Caldera Trust	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF	NRF
Cabinet Level Subtotal	2,740,130	209	164	41	4	1,329	1,083	237	9	226	178	48	0
Midsize Agencies Subtotal	152,013	33	33	0	0	225	219	6	0	1	0	1	0
Small Agencies Subtotal	46,564	36	26	10	0	123	113	10	0	23	23	0	0
Micro Agencies Subtotal	1,286	6	6	0	0	25	25	0	0	4	3	0	1
Government-wide	2,939,993	284	229	51	4	1,702	1,440	253	9	254	204	49	1

NRF = No Report Filed

* Total work force numbers do not include employees not reported for national security reasons.

Table B-29 FY 2012 Appellate Receipts and Closures

Agency or Department	Total Work Force	Total Final Agency Actions	Number Appellate Receipts	% Appellate Receipts Per Total Final Agency Actions	Number Appellate Closures	% Appellate Closures Per Total Final Agency Actions	% Appellate Closures Per Total Work Force	Number Appellate Merit Closures	Number Appellate Findings of Discrimination (Disc.)	% Appellate Findings of Disc. Per Merit Closures	Number Appellate Procedural (Proc.) Closures	Number Appellate Reversals of Proc. Closures	% Appellate Reversals Per Proc. Closures
Agency for International Development	3,983	9	2	22.22%	5	55.56%	0.13%	2	0	0.00%	3	0	0.00%
American Battle Monuments Commission	76	0	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
Armed Forces Retirement Home	282	4	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
Central Intelligence Agency *	0	27	13	48.15%	7	25.93%	0.00%	1	0	0.00%	4	2	50.00%
Commodity Futures Trading Commission	707	2	1	50.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
Commission on Civil Rights	44	0	0	0.00%	1	0.00%	2.27%	1	0	0.00%	0	0	0.00%
Consumer Product Safety Commission	522	1	0	0.00%	3	300.00%	0.57%	2	0	0.00%	1	1	100.00%
Corporation for National and Community Service	615	3	2	66.67%	2	66.67%	0.33%	0	0	0.00%	2	0	0.00%
Court Services & Offender Supervision Agency for DC	1,242	9	7	77.78%	5	55.56%	0.40%	0	0	0.00%	4	0	0.00%
Defense Army and Air Force Exchange	34,273	47	12	25.53%	10	21.28%	0.03%	5	1	20.00%	5	3	60.00%
Defense Commissary Agency	14,382	67	24	35.82%	28	41.79%	0.19%	10	0	0.00%	15	5	33.33%
Defense Contract Audit Agency	5,181	14	6	42.86%	5	35.71%	0.10%	1	0	0.00%	3	0	0.00%
Defense Contract Management Agency	10,452	24	12	50.00%	6	25.00%	0.06%	1	0	0.00%	3	1	33.33%
Defense Finance and Accounting Service	11,982	23	12	52.17%	18	78.26%	0.15%	7	0	0.00%	9	3	33.33%
Defense Human Resource Activity	1,176	1	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
Defense Information Systems Agency	6,304	5	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
Defense Intelligence Agency *	0	25	6	24.00%	6	24.00%	N/A	2	0	0.00%	3	2	66.67%
Defense Logistics Agency	25,229	75	25	33.33%	18	24.00%	0.07%	12	0	0.00%	5	1	20.00%
Defense Media Activity	2,000	0	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
Defense Missile Defense Agency	2,326	0	1	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
Defense National Geospatial-Intelligence *	0	12	9	75.00%	8	66.67%	N/A	3	0	0.00%	4	0	0.00%
Defense National Guard Bureau	57,511	26	14	53.85%	6	23.08%	0.01%	2	1	50.00%	3	0	0.00%
Defense National Security Agency *	0	13	5	38.46%	10	76.92%	N/A	2	0	0.00%	5	3	60.00%
Defense Nuclear Facilities Safety Board	116	0	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
Defense Office of the Inspector General	1,600	1	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
Defense Office of the Secretary/Wash Hqtrs Service	6,766	26	11	42.31%	6	23.08%	0.09%	3	0	0.00%	2	2	100.00%
Defense Security Service	874	5	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
Defense Threat Reduction Agency	1,299	4	3	75.00%	4	100.00%	0.31%	2	0	0.00%	0	0	0.00%
Defense Uniformed Services University	794	0	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
Department of Agriculture	103,822	254	126	49.61%	136	53.54%	0.13%	71	14	19.72%	53	12	22.64%
Department of Commerce	45,766	346	104	30.06%	82	23.70%	0.18%	38	0	0.00%	39	6	15.38%
Defense Department of Education Activity	16,346	28	6	21.43%	8	28.57%	0.05%	5	0	0.00%	3	1	33.33%
Department of Education	4,373	31	14	45.16%	15	48.39%	0.34%	11	0	0.00%	2	0	0.00%
Department of Energy	15,680	27	22	81.48%	19	70.37%	0.12%	9	0	0.00%	8	0	0.00%
Department of Health and Human Services	83,123	225	87	38.67%	72	32.00%	0.09%	38	1	2.63%	29	13	44.83%
Department of Homeland Security	200,559	735	286	38.91%	269	36.60%	0.13%	116	5	4.31%	129	28	21.71%
Department of Housing and Urban Development	9,061	43	20	46.51%	20	46.51%	0.22%	12	1	8.33%	3	0	0.00%
Department of Justice	116,973	616	184	29.87%	127	20.62%	0.11%	63	11	17.46%	51	17	33.33%
Department of Labor	16,819	75	38	50.67%	36	48.00%	0.21%	21	2	9.52%	10	1	10.00%
Department of State	69,885	70	30	42.86%	27	38.57%	0.04%	16	2	12.50%	10	1	10.00%
Department of the Air Force	173,807	269	104	38.66%	95	35.32%	0.05%	38	5	13.16%	39	11	28.21%
Department of the Army	250,617	540	272	50.37%	257	47.59%	0.10%	92	4	4.35%	146	48	32.88%
Department of the Interior	78,779	177	70	39.55%	70	39.55%	0.09%	47	3	6.38%	20	3	15.00%
Department of the Navy	245,574	340	191	56.18%	204	60.00%	0.08%	68	3	4.41%	118	34	28.81%
Department of the Treasury	115,292	277	98	35.38%	107	38.63%	0.09%	62	4	6.45%	32	1	3.13%

Table B-29 FY 2012 Appellate Receipts and Closures

Agency or Department	Total Work Force	Total Final Agency Actions	Number Appellate Receipts	% Appellate Receipts Per Total Final Agency Actions	Number Appellate Closures	% Appellate Closures Per Total Final Agency Actions	% Appellate Closures Per Total Work Force	Number Appellate Merit Closures	Number Appellate Findings of Discrimination (Disc.)	% Appellate Findings of Disc. Per Merit Closures	Number Appellate Procedural (Proc.) Closures	Number Appellate Reversals of Proc. Closures	% Appellate Reversals Per Proc. Closures
Department of Transportation	57,187	229	124	54.15%	135	58.95%	0.24%	46	3	6.52%	82	25	30.49%
Department of Veterans Affairs	323,154	1,379	488	35.39%	453	32.85%	0.14%	201	8	3.98%	225	75	33.33%
Environmental Protection Agency	17,001	26	17	65.38%	23	88.46%	0.14%	15	1	6.67%	5	1	20.00%
Equal Employment Opportunity Commission	2,291	13	10	76.92%	7	53.85%	0.31%	4	0	0.00%	1	0	0.00%
Export-Import Bank of the US	408	1	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
Farm Credit Administration	302	0	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
Federal Communications Commission	1,788	2	1	50.00%	1	50.00%	0.06%	0	0	0.00%	1	1	100.00%
Federal Deposit Insurance Corporation	7,846	26	18	69.23%	14	53.85%	0.18%	1	1	100.00%	13	1	7.69%
Federal Election Commission	355	0	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
Federal Energy Regulatory Commission	1,483	8	4	50.00%	8	100.00%	0.54%	0	0	0.00%	8	4	50.00%
Federal Housing Finance Board	706	1	1	100.00%	1	100.00%	0.14%	0	0	0.00%	1	1	100.00%
Federal Labor Relations Authority	138	0	0	0.00%	1	N/A	0.72%	0	0	0.00%	1	0	0.00%
Federal Maritime Commission	124	0	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
Federal Mediation and Conciliation Service	243	0	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
Federal Reserve System- Board of Governors	2,412	1	1	100.00%	1	100.00%	0.04%	0	0	0.00%	0	0	0.00%
Federal Trade Commission	1,178	1	0	0.00%	1	100.00%	0.08%	1	0	0.00%	0	0	0.00%
General Services Administration	12,416	55	25	45.45%	25	45.45%	0.20%	10	0	0.00%	12	3	25.00%
Government Printing Office	1,879	18	4	22.22%	11	61.11%	0.59%	2	0	0.00%	9	7	77.78%
Holocaust Memorial Museum U.S.	397	0	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
International Boundary and Water Commission	258	0	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
International Broadcasting Bureau	1,675	8	3	37.50%	3	37.50%	0.18%	3	0	0.00%	0	0	0.00%
International Trade Commission	397	0	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
John F. Kennedy Center for the Performing Arts	2,250	0	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
Merit Systems Protection Board	208	0	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
Millennium Challenge Corporation	288	0	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
National Aeronautics and Space Administration	18,416	30	12	40.00%	5	16.67%	0.03%	3	0	0.00%	2	0	0.00%
National Archives and Records Administration	3,381	8	4	50.00%	2	25.00%	0.06%	0	0	0.00%	2	0	0.00%
National Credit Union Administration	1,195	1	1	100.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
National Endowment for the Arts	174	1	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
National Endowment for the Humanities	199	0	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
National Gallery of Art	834	4	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
National Indian Gaming Commission	97	0	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
National Labor Relations Board	1,702	4	1	25.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
National Mediation Board	50	0	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
National Reconnaissance Office *	0	6	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
National Science Foundation	1,663	0	3	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
National Transportation Safety Board	413	1	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
Nuclear Regulatory Commission	3,775	1	4	400.00%	4	400.00%	0.11%	2	0	0.00%	2	1	50.00%
Office of Personnel Management	5,843	19	12	63.16%	9	47.37%	0.15%	3	0	0.00%	6	2	33.33%
Office of Special Counsel	129	0	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
Office of the Director of National Intelligence *	0	2	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
Overseas Private Investment Corporation	241	0	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
Peace Corps	896	4	0	0.00%	1	25.00%	0.11%	1	0	0.00%	0	0	0.00%
Pension Benefit Guaranty Corporation	971	17	6	35.29%	3	17.65%	0.31%	0	0	0.00%	2	0	0.00%
Presidio Trust	NRF	NRF	0	N/A	1	N/A	N/A	0	0	0.00%	1	0	0.00%

Table B-29 FY 2012 Appellate Receipts and Closures

Agency or Department	Total Work Force	Total Final Agency Actions	Number Appellate Receipts	% Appellate Receipts Per Total Final Agency Actions	Number Appellate Closures	% Appellate Closures Per Total Final Agency Actions	% Appellate Closures Per Total Work Force	Number Appellate Merit Closures	Number Appellate Findings of Discrimination (Disc.)	% Appellate Findings of Disc. Per Merit Closures	Number Appellate Procedural (Proc.) Closures	Number Appellate Reversals of Proc. Closures	% Appellate Reversals Per Proc. Closures
Railroad Retirement Board	945	0	1	N/A	2	N/A	0.21%	0	0	0.00%	0	0	0.00%
Securities and Exchange Commission	3,826	4	4	100.00%	7	175.00%	0.18%	1	0	0.00%	6	0	0.00%
Selective Service System	121	0	0	0.00%	0	0.00%	0.00%	0	0	0.00%	0	0	0.00%
Small Business Administration	5,228	26	12	46.15%	10	38.46%	0.19%	3	0	0.00%	7	4	57.14%
Smithsonian Institution	6,057	12	1	8.33%	1	8.33%	0.02%	0	0	0.00%	1	1	100.00%
Social Security Administration	65,474	310	149	48.06%	145	46.77%	0.22%	89	5	5.62%	48	10	20.83%
Tennessee Valley Authority	12,762	39	22	56.41%	20	51.28%	0.16%	7	2	28.57%	12	3	25.00%
U.S. Postal Service	625,701	3,524	1,602	45.46%	1,678	47.62%	0.27%	572	32	5.59%	998	357	35.77%
Other Agencies*	6,195	11	0	0.00%	1	9.09%	0.02%	0	0	0.00%	1	0	0.00%
Government-Wide	2,939,893	10,273	4,350	42.34%	4,265	41.52%	0.15%	1,727	109	6.31%	2,209	695	31.46%

*** Other agencies include *Office of Trade Representative* which do not file Form 462.**

* Total work force numbers do not include employees not reported for national security reasons.

The U.S. Equal Employment Opportunity Commission

Instructions to Federal Agencies for EEO MD-715

Guidance for Completing the EEOC FORM 715-01 Workforce Data Tables

---

Introduction

The purpose of the MD 715 Workforce Data Tables is to assist agencies in identifying triggers to be explored. Agency attention should be devoted to what the compiled data reveals about the agency and its workforce. The process of barrier identification and elimination is more important than the mere completion of the workforce data tables.

The agency workforce is reviewed and generally compared to appropriate comparators to seek indications of possible triggers, which must then be investigated by the agency. All agencies are expected to investigate triggers indicating barriers for any group and report them in Form 715-01, PART I. Agencies with 1,000 or more employees are also required to describe in PART J their Special Program Plan for the Recruitment, Hiring, and Advancement of Individuals with Targeted Disabilities.

Permanent/Temporary

Tables A1, B1, A8 and B8 have separate sections for permanent and for temporary employees. Those agencies with temporary employees must file two sets of Tables A4, A5, A6, A7, B4, B5, B6, and B7, one for permanent employees, and one for temporary employees. Complete Tables A2, A3-1, A3-2, A9, A10, A11, A12, A13, A14, B2, B3-1, B3-2, B9, B10, B11, B12, B13, and B14 for permanent employees only.

Tenure codes 1 and 2 are considered permanent employee status. Any part time, intermittent, or seasonal employee with tenure code 1 or 2 is reported as permanent.

Calculating Ratios

All analysis of the data tables should be based on the ratios, not the numbers. The ratio for each group is computed by dividing the number of employees in the group by the total number of employees for that particular row. Generally, all ratios are computed **across** the row. Thus, the number of employees in the group is divided by the total number of employees in the row to get the ratio for the group.

However, in Tables A3-2, A4-2, A5-2, B3-2, B4-2 and B5-2, the distribution is computed as a ratio of the total workforce, down the Total column. The ratios for each group is computed **down** the column for that group and not across the rows.

For example, Table A4-1 depicts the total number of employees at a grade level and what percent of all employees at that grade level are represented by the particular group in the column above. Accordingly, the denominator for Table A4-1 is the total number of employees in that particular grade. Table A4-2, on the other hand, depicts what percentage of the particular group are in each grade. Thus, the denominator for Table A4-2 is the total number individuals within a particular group in the agency's workforce.

Specific Information for Each Table

The remainder of this document provides guidance for completing and analyzing each table. Employee numbers should be obtained from the agency workforce data and personnel action data. Applicant data is obtained through a separate tracking system. Ratios are calculated as described in the preceding paragraph.

Tables A1 and B1 allow agencies to examine workforce distribution for the current and prior year to determine whether the changes, including net changes, are relatively uniform or whether any group is not keeping pace with the others.

Table A1: Total Workforce - Distribution by Race/Ethnicity and Sex

Enter the current and prior year workforce numbers and percentages. Lines should total 100% **across** rows. Compute ratios by dividing the number in each group by the total for that line (in the "All" column). Numbers for Current FY Permanent, Temporary, and Non-Appropriated fund employees should total up to the numbers in the Total-Current FY row.

In the "Difference" row, enter the difference between the prior year employee numbers and the current year employee numbers. If the current year numbers are smaller, show the difference as a negative number. On the percentage line, show the difference between the ratios for the current year and the prior year.

Compute net change by dividing difference in employment numbers (current year vs prior year) by the number of employees in the prior year. If a group decreased, the net change is a negative; add a minus sign. For a detailed explanation of computing net change and examples, please see the Instructions to Federal Agencies for EEO MD 715 Section III, Page 14 of 15.

If a group has a net change lower than the net change for the total workforce, it is a trigger of the possible existence of a barrier. A current workforce ratio below the Civilian Labor Force (CLF) for any group is another trigger.

Table B1: Total Workforce - Distribution by Disability

Complete the tables and do the analysis in the same manner as for Table A1, except the ratio of employees with targeted disabilities is compared to the prior year's Federal high. (In FY 2003, the Federal high was 2.27%.) A ratio of employees with targeted disabilities below the Federal high is a trigger. A lower net change for targeted disabilities is also a trigger, indicating a possible barrier.

The purpose of **Tables A2 and B2** is to compare the permanent workforce distribution within each component with the availability rate (the Civilian Labor Force), to determine if possible hiring or retention barriers exist in specific components.

Please note that all agencies must report their components on Table 2, regardless of whether the components are included on the list of second level agencies that must report.

Table A2: Total Workforce by Component - Distribution by Race/Ethnicity and Sex

Enter total workforce distribution and distribution by component. For most agencies, components are the major agency segments. Depending on the agency, these are Regions, Bureaus, Operating Divisions, or Services, etc. Numbers for the components should total up to the Total for the agency. Ratios are computed

across rows. When one or more components has a lower ratio of a group than the other components, it is a trigger.

Table B2: Total Workforce by Component - Distribution by Disability

Complete the same way as A2. All agencies with a ratio of employees with targeted disabilities below the Federal high are expected to report barriers for this group. When one or more components has a lower ratio of employees with targeted disabilities than the other components, it is a trigger.

Tables A3 and B3 compare either: (-1) the total number of employees in an occupational category and what percentage of all employees in that occupational category are represented by the particular group; or (-2) the percentage of the particular group that are in each occupational category.

Tables A3-1 and A3-2: Occupational Categories - Distribution by Race/Ethnicity and Sex

Employees with supervisory or managerial status are reported in the first occupational category - supervisors and managers. The number and ratio of supervisors who are at GS 15 and above are listed in the first two lines. The number and ratio of supervisors in GS 13 and 14 are reported in the second two lines. The number and ratio of supervisors who are at GS 12 and below are reported in the third two lines. An agency may also choose to place employees who have significant policy-making responsibilities, but do not supervise other employees, in these three sub-categories.

The fourth sub-category, called "Other," contains employees in a number of different occupations which are primarily business, financial and administrative in nature, and do not have supervisory or significant policy responsibility. The number and ratio of employees in the "Other category (in occupational series that are in EEO category one but are not supervisors/policy makers) go in the next lines. The total for these four sub-categories is reported on the line "Officials and Managers TOTAL"

In **Table A3-1**, the ratios are computed **across** the rows, because it compares the total number of employees in an occupational category and what percentage of all employees in that occupational category are represented by the particular group. In **Table A3-2**, the ratios are computed **down** the columns because it compares the percentage of the particular group that are in each occupational category.

Tables B3-1 and B3-2: Occupational Categories - Distribution by Disability

These tables are completed in the same manner as A3-1 and A3-2, respectively. Ratios for employees with targeted disabilities are compared with ratios for employees with no disabilities. Lower ratios are triggers that must be investigated.

Tables A4 and B4 compare either: (-1) the total number of employees at a General Schedule (GS) grade level and what percentage of all employees at that GS grade level are represented by the particular group; or (-2) what percentage of the particular group are in each GS grade.

Tables A4-1 and A4-2: Participation Rates For General Schedule (GS) Grades by Race/Ethnicity and Sex

In **Table A4-1**, the ratios are computed **across** the rows, because it compares the total number of employees in a GS grade and what percentage of all employees in that grade are represented by the particular group. In **Table A4-2**, the ratios are computed **down** the columns because it compares the percentage of the particular group that are in each GS grade.

Agencies should analyze this data with an eye toward determining whether a "glass ceiling" exists for any group. In particular, low participation for a group in any of the senior grades (GS 13 and above) compared to the participation rate for the total work force in these grades is a trigger.

Tables B4-1 and B4-2: Participation Rates For General Schedule (GS) Grades by Disability

These tables are completed in the same manner as A3-1 and A3-2, respectively. Ratios for employees with targeted disabilities are compared with ratios for employees with no disabilities.

Agencies should analyze this data with an eye toward determining whether a "glass ceiling" exists for any group. In particular, low participation in any of the senior grades (GS 13 and above) compared to the participation rate for employees with no disabilities in these grades is a trigger.

Tables A5 and B5 compare either: (-1) the total number of employees at a Wage Grade level and what percentage of all employees at that Wage Grade level are represented by the particular group; or (-2) what percentage of the particular group are in each Wage Grade.

Tables A5-1 and A5-2: Participation Rates For Wage Grades by Race/Ethnicity and Sex

Complete and analyze these tables in the same manner as A4-1 and A4-2, respectively. However, if an agency has more than one wage grade system and the systems are not compatible, it will be necessary to complete additional A5-1 and A5-2 Tables for each such system.

Tables B5-1 and B5-2: Participation Rates For Wage Grades by Disability

Complete and analyze these tables in the same manner as B4-1 and B4-2, respectively.

In **Tables A6 and B6**, agencies examine the distribution of each group within major occupations.

Table A6: Participation Rates for Major Occupations - Distribution by Race/Ethnicity and Sex

Every agency has employees who are in occupations that are essential to the mission of the agency. For example, at the General Accounting Office (GAO) accountants and auditors are mission related occupations and, therefore the job series for accountants (510) and auditors (511) are "major occupations" for GAO. Select five to seven of the agency's major occupations with the largest number of employees.

In the far left column, enter the job series. For each job series, enter the employee distribution numbers and ratios, and the appropriate CLF ratios for the occupational series. (Ratios are calculated **across** each row.) If a group has a participation rate below the CLF, it is a trigger.

Table B6: Participation Rates for Major Occupations - Distribution by Disability

For the same major occupations reported on Table A6, show the distribution by disability category. Compare the distribution ratio for employees with targeted disabilities with the ratio for employees with no disabilities. Lower ratios for employees with targeted disabilities compared to employees with no disabilities are triggers.

Tables A7 and B7 provide a method for analyzing the effectiveness of current recruitment methods. It allows the agency to determine whether a sufficient number of applications are received from qualified individuals in each group. This Table focuses on the same makor occupations reported in Table 6.

Table A7: Applicants and Hires for Major Occupations by Race/Ethnicity and Sex

On the first line, enter the job series. Total the information for all job announcements for that occupation/job series. Enter the total number of applications received. On the next two lines, enter the number and ratio of applicants who voluntarily self identified their race/ethnicity and sex. (All ratios equal 100% **across** the rows.) On the next lines, enter the number and ratio of applicants who voluntarily identified and were found to be qualified.

Discrepancies between the ratios of those who self-identified and those who were qualified are triggers indicating the possibility that barriers may exist due to, for example, inadequate recruitment activity or a problem in the screening process. Next, enter the number and ratio of individuals who were selected. A discrepancy between the ratios of those qualified and those selected is a trigger indicating the possibility that a barrier exists due to, for example, a disconnect between recruitment and hiring efforts.

Table B7: Applicants and Hires by Disability

As part of a long-standing effort to encourage agencies to hire individuals with severe disabilities, the Federal government provides special hiring options, called Special Appointing Authorities. Schedule A is a Special Appointing Authority. These options are for temporary appointment, with potential for conversion to a permanent, career appointment. Individuals who do not have a visible disability must provide documentation to show that s/he has a severe disability. Thus, applicants for these temporary positions self-identify. Agencies are required to track this information and report it in Table B7. The second line (ratios) is based on the numbers in the first line - the ratios should equal 100% **across** the line. By comparing the number and ratio of applications to the number and ratio of hires, agencies can identify triggers.

Some individuals who apply competitively voluntarily identify themselves as an individual with a disability. Of this group, those with targeted disabilities should be reported here. The ratios should equal 100% **across** the row. A discrepancy between the ratio of those who applied and those hired is a trigger.

Tables A8 and B8 allow agencies to analyze the cumulative result of hiring decisions.

Table A8: New Hires by Type of Appointment - Distribution by Race/Ethnicity and Sex

When individuals are hired, each must be given a self-identification form to complete. If an individual declines to complete the form, the agency must complete it by visual identification or, if available, information the employee provided previously. Using information from this form, enter the number and ratio

of new hires for permanent, temporary, and non-appropriated fund positions. Ratios should total 100% **across** each line. Compare for each group the ratio on each line with their ratio in the CLF, noting any discrepancies as triggers.

Table B8: New Hires by Type of Appointment - Distribution by Disability

Complete this table the same as Table A8. Compare the ratio of individuals with targeted disabilities hired into each type of appointment with the ratios for individuals with no disabilities. Discrepancies indicate triggers.

Tables A9 and B9 allow analysis of the cumulative result of selections for internal promotion opportunities for the Major Occupations selected for Table 6.

Table A9: Selections for Internal Competitive Promotions for Major Occupations by Race/Ethnicity and Sex

For each of the job series, show the total number and distribution of applications received from existing employees for promotions in this job series. Then show the number and ratio of those who qualified and those who were selected. The last line is for the ratio of employees from each group who are eligible for the vacancies (the relevant applicant pool). All ratios should total 100 percent **across** the row.

Each set of ratios is useful. A discrepancy between the ratios in the relevant applicant pool and the ratios for applicants can indicate a trigger related to the methods used in publicizing the opportunity or perceptions that deterred employees from applying. A discrepancy between ratios of those who were qualified and those who applied is a trigger. It could indicate, for example, that some employees are not receiving commensurate levels of experience or that the selection criteria impacts some groups in an adverse manner. A variance between the ratios of those selected and those who are in the relevant applicant pool is also a trigger.

Table B9: Selections for Internal Competitive Promotions for Major Occupations by Disability

This Table should be completed and analyzed in the same manner as Table A9.

Tables A10 and B10 provide a method for determining whether all groups are receiving career ladder promotions in the same average amount of time.

Table A10: Non-Competitive Promotions - Time in Grade - Distribution by Race/Ethnicity and Sex

In the first two rows, enter the number and ratios of employees in the career ladder who are eligible for a non-competitive promotion (i.e., employees who have not reached the top grade of the career ladder).

The remaining rows are for recording information on the impact of delays in non-competitive promotions. An agency-wide policy to delay career ladder promotions is acceptable, but agencies must watch for situations that lead to delays for certain groups only. Ratios are computed **across** the rows.

To complete this table, the agency must determine its policy for career ladder promotions - what is the

minimum amount of time required in grade before a career ladder employee is eligible for a promotion? In the next two rows, enter the number and ratios of employees who have been in their pay grade for the minimum amount of time plus one to twelve months. Then enter the number and ratios of employees who have been in their pay grade for the minimum amount of time plus thirteen to 24 months. In the last two rows, enter the number and ratios of employees who have been in grade for the minimum amount of time plus 25 months or more.

Discrepancies between groups indicate a trigger.

Table B10: Non-Competitive Promotions - Time in Grade - Distribution by Disability

Complete Table B10 in the same manner as table A10. Any discrepancies between employees with targeted disabilities and employees with no disabilities are triggers.

Tables A11 and B11 allow agencies to determine the cumulative impace of selections for senior level positions.

Table A11: Internal Selections for Senior Level Positions (GS 13, GS 14, GS 15, and SES) by Race/Ethnicity and Sex

To complete this form, collect by pay grade the data on internal selections for positions at the GS 13, GS 14, GS 15, and SES levels. For each level, list the total number of applications, the distribution (ratio) of applications received, the number of applicants who were found to be qualified for the position, the ratio of those qualified, the number selected for the position, and the ratio of those selected. Ratio (percent) rows should equal 100% **across** the row. On the last line, show the ratios of the relevant pool. The relevant pool includes all employees in the next lower pay grade and in all series that qualify them for the position(s) announced.

A discrepancy between the ratios of the relevant pool and the distribution (ratios) of groups from whom applications were received, individuals were found to be qualified, or individuals were selected indicate a trigger.

Table B11: Internal Selections for Senior Level Positions (GS 13, GS14, GS 15, and SES) by Disability

Complete Table B11 in the same manner as Table A11.

Tables A12 and B12 allow examination of the distribution of opportunities to participate in Career Development programs.

Career Development programs are those that, upon completion, qualify a participant for a promotion. One-time training courses that are not part of such a program are not to be included on this form.

Table A12: Participation in Career Development by Race/Ethnicity and Sex

In the first space, enter the number of slots available for career development programs. On the next line,

enter the distribution ratios for employees in GS 5 to GS 12. (Ratios are computed **across** rows.) Then enter the number and ratios for those who applied and for those who were chosen to participate in the career development. Compare the ratios. Repeat the process for GS 13, GS 14, GS 15 and SES employees. Discrepancies between the relevant pool and those who applied or participated is a trigger.

Table B12: Participation in Career Development by Disability

Complete Table B12 in the same manner as Table A12.

Use **Tables A13 and B13** to examine the distribution of awards.

The purpose of Table 13 is to examine the distribution of awards. Time-Off awards are Nature of Action Codes (NOAC) 846 and 847. Cash awards are NOACs 840, 841, 842, 843, 844, 845, 848, 849 and 871.

Table A13: Employee Recognition and Awards - Distribution by Race/Ethnicity and Sex

The first four lines are for time-off awards of nine hours or less. Enter the number and ratio of employees who received time off awards of nine hours or less. Ratios should equal 100% **across** the rows. Then enter the total number of hours given to each group, and the average number of hours. To compute the average number of hours, for each group divide the total hours by the number of employees in the group (from the first full line). Compare the average number of hours. Discrepancies are a trigger.

Complete the rest of the form and analysis in the same manner.

Table B13: Employee Recognition and Awards - Distribution by Disability

Complete and analyze Table B13 in the same manner as Table A13.

Tables A14 and B14 differentiate between voluntary and involuntary separations to assist agencies in determining the impact of these actions on each group and on the agency.

Table A14: Separations by Type of Separation - Distribution by Race/Ethnicity and Sex

The purpose of Table 14 is to examine the distribution of separations from the permanent workforce. Enter the number and ratio of employees who separated voluntarily (transfer, retirement, etc.) The Nature of Action Codes (NOAC) for voluntary separations are 300, 301, 302, 303, 317. 350, 351, 352, 353, 355, and 390.

Enter the number and ratio of employees who separated involuntarily (disciplinary dismissal). NOACs for involuntary separations are: 304, 312, 330, 357, and 385. Ratios are computed **across** the rows, If the agency experienced a Reduction in Force (RIF) or similar downsizing activity (NOAC 356), add two lines to the Table to report separations due to RIFs separately from the terminations due to performance or disciplinary issues. Add the employee numbers columns to obtain the number of employees for the Total Separations line. Compute the distribution ratios for Total Separations.

From Table A1, obtain Permanent Current FY data and ratios, and enter in the Total Workforce lines at the bottom of Table A14. Compare the total work force ratio for each group with the group ratios for voluntary and involuntary separations. A separation ratio higher than the group's Total work force ratio is a trigger.

Table B14: Separations by Type of Separation - Distribution by Disability

Complete Table B14 in the same manner as Table A14. From Table B1, obtain the Permanent Current FY data and ratios, and enter in the Total Workforce lines at the bottom of Table B14. Separation ratios for employees with targeted disabilities that are higher than separation ratios for employees with no disabilities are a trigger.

This page was last modified on July 20, 2004.


Return to Home Page

The U.S. Equal Employment Opportunity Commission

Instructions to Federal Agencies for EEO MD-715

Section I
The Model EEO Program

The Model EEO Program

This section explains the basic elements necessary to create and maintain a model EEO program, as required under both Title VII of the Civil Rights Act of 1964 (Title VII), as amended, 42 U.S.C. § 2000e *et seq*., and Section 501 of the Rehabilitation Act of 1973 (Rehabilitation Act), as amended, 29 U.S.C. § 791 *et seq*. A model EEO program effectively considers and addresses concerns arising under both Title VII and Section 501 of the Rehabilitation Act.

When establishing a model EEO program, an agency should incorporate into the design a structure for effective management, accountability and self-analysis which will ensure program success and compliance with EEO MD-715. Agency personnel programs and policies should be evaluated regularly to ascertain whether such programs have any barriers that tend to limit or restrict equitable opportunities for open competition in the workplace.

EEO MD-715 divides the essential elements of model agency EEO programs into six broad categories, as listed below. An agency should review its EEO and personnel programs, policies and performance standards against all six elements to identify where their EEO program can become more effective.

The six essential elements for a model EEO program, as described in EEO-MD-715, at PART A, II. A-F, and PART B, III. A-F, are as follows:

- Demonstrated commitment from agency leadership;
- Integration of EEO into the agency's strategic mission;
- Management and program accountability;
- Proactive prevention of unlawful discrimination;
- Efficiency; and
- Responsiveness and legal compliance.

These six elements serve as the foundation upon which each agency shall build its program. The following describes each essential element and provides samples of the self-assessment inquiries that an agency should employ to determine whether its EEO program is properly established and compliant with the EEO MD-715 standards. Following the discussion of the Model EEO Program elements are instructions and a self-assessment checklist that all agencies will use to assess compliance with the elements of the model program.

Element One - Demonstrated Commitment

Start with an Effective EEO Program Policy Statement(s)[(1)]

- A committed agency/facility/installation head will, at the beginning of her/his tenure, and each year

thereafter, issue a signed policy statement declaring the agency's position against discrimination on any protected basis.

- This policy shall be prominently posted in all personnel offices, EEO offices, and on the agency's internal website.
- This statement shall affirm the principles of equal employment opportunity and assure that EEO program requirements will be enforced by the agency head and agency management.
- Some of the principles the policy statement must assure will be upheld include, but are not limited to:
  - Equal employment opportunity for all employees and applicants for employment, regardless of their race, religion, color, sex, national origin, age, or disability.
  - All employees will have the freedom to compete on a fair and level playing field with equal opportunity for competition.
  - Equal employment opportunity covers all personnel/employment programs, management practices and decisions including, but not limited to, recruitment/hiring, merit promotion, transfer, reassignments, training and career development, benefits, and separation.
  - Workplace harassment will not be tolerated, allegations of harassment will be immediately investigated, and, where allegations are substantiated, appropriate action will be taken. (Anti-harassment policy requirements are discussed under Element Four. Agencies may choose to include all issues under one policy or issue a separate anti-harassment policy, based on their needs.)
  - Reprisal against one who engaged in protected activity will not be tolerated, and the agency supports the rights of all employees to exercise their rights under the civil rights statutes.

Allocate Sufficient Resources

- An agency shall provide sufficient staffing and resources to operate the EEO program in an effective manner. For example, staff and resources should also be sufficient to enable accurate collection and analysis of data and other employment factors, including applicant information, to enable the efficient identification of barriers. This will necessarily require staff beyond the EEO office, particularly Information Management/Services.
- An agency must also provide sufficient staffing, funding, and authority to eliminate identified barriers. In order to determine whether it is providing sufficient resources an agency should examine a number of factors, including:
  - whether the agency employs personnel with the training and experience to conduct the analyses required by MD-715 and these instructions;
  - whether the agency's EEO staff has the knowledge, skills and ability to ensure that agency EEO programs and procedures are effectively implemented;
  - whether the agency has implemented adequate data collection and analysis systems that permit tracking of the information required by MD-715 and these instructions;
  - whether sufficient resources have been provided to conduct effective audits of field facilities' efforts to achieve a model EEO program and eliminate discrimination under Title VII an the Rehabilitation Act;
  - whether EEO training and education programs are made available to all managers and employees;
  - whether a central fund or other mechanisms have been established for providing disability accommodations;
  - whether there is a Disability Program Manager or other mechanisms in place to ensure coordination of disability accommodations in all major components of the agency; and

- whether there are such Special Emphasis Program Managers as may be necessary (29 C.F.R. § 1614.102(b)(4)).

Ensure All Employees are Informed

- An agency must ensure that EEO program information is distributed to all employees, using all media available, including the World Wide Web or Internet.
  - The agency must ensure that each employee is informed of the agency's annual EEO program policy statements, as well as the requirements and prohibitions of Title VII and the Rehabilitation Act, and the operation of the EEO complaint process and procedures.
  - Federal regulation requires that EEO posters and program information be prominently posted throughout the agency's facilities, and that complainants are advised, in writing, about the complaint process (29 C.F.R. § 1614.102(b)(5), (7)).
  - Distribute the agency's reasonable accommodation procedures to all managers, supervisors, and others responsible for processing requests for reasonable accommodation, and make the procedures readily available to all other employees.
  - Provide training to all employees and supervisors on the operation of the EEO process, protections afforded to employees, related policy statements, and reasonable accommodation procedures.
- Demonstrate the value of EEO to the agency and employees.
  - Seek input (*e.g.*, using employee surveys and focus groups, discussions with employee advisory groups, etc.) regarding the workplace environment.

Element Two - Making EEO an Integral Part of the Agency's Strategic Mission

Structure From The Top

- The success of an agency's EEO program ultimately depends on individual decisions made by individual agency managers. Therefore, agency managers constitute an integral part of the agency's EEO program. The EEO office serves as a resource to these managers by providing direction, guidance and monitoring of key activities to achieve a diverse workplace free of barriers to equal opportunity.
- The agency's EEO program should be organized and structured in such a manner as to maintain a work place that is free from discrimination in any of its management policies, practices or procedures and supports the agency's strategic mission.
- This necessarily includes an appropriate reporting structure, as previously mentioned. The agency's EEO Director shall have a regular and effective means of informing the agency head and other top management officials of the effectiveness, efficiency and legal compliance of the agency's EEO program.
- Such access includes, but is not limited to, the State of the Agency briefing to be given to the head of the agency by the principal EEO Director/Officer following the submission of the agency's EEOC FORM 715-01. The briefing should thoroughly cover all components of the agency's EEOC FORM 715-01, including an assessment of the performance of the agency in each of the six elements of the Model EEO Program, as well as a report on the progress of the agency in completing its barrier analysis including any barriers it identified and/or eliminated or reduced the impact of. Pertinent information from workplace data tables may be presented as well.
- Similarly, field level EEO Directors should have a regular and effective means of informing the field level agency head and other top field management officials of the effectiveness, efficiency and legal compliance of the field offices' EEO program. Again, such access includes, but is not limited to, the State of the Agency briefing to be given to the field level agency head by the principal EEO

Director/Officer following the submission of the field's EEOC FORM 715-01 (whether such submission is made directly to the EEOC or to the agency's headquarters for inclusion in the agency-wide report).

- The agency should maintain EEO program organizational charts and procedures which explain how sub-units/installations are to establish their own local programs and submit annual reports through the agency chain-of-command as described by this directive.

Strategic Commitment

- Ensure that EEO Officials are involved in critical workplace decisions, have regular access to senior staff, and participate in meetings where critical personnel decisions regarding management and the deployment of Human Resources are made.
- As previously mentioned, the allocation of sufficient resources to the EEO program cannot be over-emphasized. An agency must provide sufficient qualified staff and the resources to ensure quality customer service and a workplace free of discrimination to its employees. This includes the allocation of funding for mandatory EEO training of managers, supervisors and EEO staff.

Element Three - Ensuring Management and Program Accountability

Overall Accountability and EEO Programmatic Management

- Hire, develop, and retain supervisors and managers who have effective managerial, communication, and interpersonal skills in order to supervise most effectively in a workplace with diverse employees and avoid disputes arising from ineffective communications.
- Inform managers and supervisors that success and a positive evaluation will include an assessment of how that manager contributes to the agency's EEO program by emphasizing to managers and supervisors that equality of opportunity is essential to attracting, developing and retaining the most qualified workforce, with such a workforce being essential to ensuring the agency's achievement of its strategic mission.
    - For all managers and supervisors, make successful performance contingent, in part, on efforts to achieve a workplace free of discrimination. Agencies should develop their own standards to incorporate into the mission of the agency as a whole.
    - Where discrimination has been found by an adjudicatory body, the agency must ensure full and prompt compliance with orders accompanying such decisions. This includes orders from the agency itself, the EEOC, the Merit Systems Protection Board, labor arbitrators, the Federal Labor Relations Authority, the Department of Labor, and federal courts. Agencies must also comply with the terms of settlement agreements entered into by the agency.
    - The agency should review findings of discrimination, and the evidence collected in the investigatory record in other suitable cases, to determine the appropriateness of taking disciplinary action against agency employees, (including management officials, supervisors and/or co-workers), involved in the matter.
- Make clear that all managers and supervisors share responsibility with EEO program and human resources officials for the successful implementation of EEO programs.
    - Provide managers and supervisors with initial and regular refresher training to understand their responsibilities under civil rights laws, including ADR, and how those responsibilities figure into the success of the agency's EEO program and overall mission.
    - Conduct regular internal audits, on at least an annual basis, to assess the effectiveness and efficiency of the EEO program and to ascertain whether the agency has removed identified barriers to equality of opportunity in the workplace.

- Ensure that personnel policies and procedures, rules of conduct, promotion, evaluation and training systems are routinely reviewed to ensure that they are clearly defined, well-communicated, consistently applied and fairly implemented.
- Ensure there are procedures in place for effective coordination between the agency's EEO office and related agency human resource programs and other management programs, such as the Federal Equal Opportunity Recruitment Program (FEORP), ADR, Employee Relations, and others.

Element Four - Proactive Prevention

- As part of its ongoing obligation to prevent discrimination on the bases of race, color, national origin, religion, sex, age, reprisal and disability, and to eliminate barriers that impede free and open competition in the workplace, an agency must conduct a self-assessment on at least an annual basis to monitor progress, identify areas where barriers may operate to exclude certain groups, and develop strategic plans to eliminate identified barriers.
- As stated under Element One, an agency must develop and make known to all employees an effective anti-discrimination policy that explains what protections are afforded by the civil rights laws and how complaints may be raised, including the EEO process and other processes.
- In addition to the anti-discrimination policy mentioned above, agencies should develop a comprehensive anti-harassment policy to prevent harassment on all protected bases (including, but not limited to, sexual harassment) and retaliation in the workplace. The policy should:
  - Inform employees as to what type of behavior is prohibited, and the steps to take if faced with a harassment situation.
  - Provide for multiple avenues of redress, not just the EEO complaint process.
  - Provide that no acts of retaliation will be tolerated.
  - For further guidance, see *EEOC Enforcement Guidance: Vicarious Liability for Unlawful Harassment by Supervisors* (6/18/99); and *EEOC Enforcement Guidance on Harris v. Forklift Sys., Inc., 510 U.S. 17 (1993)* (3/8/94).
- Pursuant to Executive Order 13164, as of July 25, 2001, all federal agencies were required to have developed written procedures for acting on requests for reasonable accommodation under the Rehabilitation Act. Agencies that remain noncompliant with this Executive Order must develop such procedures immediately and submit them to the Commission, which will offer feedback. The policy should be regularly evaluated for compliance with current law and regulations.[(2)] An agency must ensure that all employees are informed of, and have access to, such procedures, including making the procedures available on the World Wide Web or Internet.
- An effective reasonable accommodation procedure must include the following:
  - An explanation as to how an employee or job applicant may initiate a request for reasonable accommodation.
  - An explanation of how the agency will process a request for reasonable accommodation and from whom the individual requesting accommodation will receive a final decision.
  - A designated time period during which reasonable accommodation requests will be granted or denied, absent extenuating circumstances.
  - An explanation of the responsibility of the employee or applicant requesting reasonable accommodation when the disability and/or need for accommodation is not obvious or already known to provide appropriate medical information, when requested, related to the functional impairment and the requested accommodation.
  - An explanation of the circumstances under which the agency may request supplemental medical information in support of an accommodation request.

- An explanation of the agency's right to have medical information reviewed by a medical expert of the agency's choosing at the agency's expense.
- An explanation of the circumstances in which reassignment will be required as a reasonable accommodation if the agency determines that no reasonable accommodation will permit the employee with a disability to perform the essential functions of his or her current position.
- A provision that denials of requests for reasonable accommodation will be in writing and specify the reasons for denial.
- A provision that the agency's systems of record-keeping track the processing of requests for reasonable accommodation and maintain the confidentiality of medical information received in accordance with applicable law and regulations.
- Encouragement of the use of informal dispute resolution processes to allow individuals with disabilities to obtain prompt reconsideration of denials of reasonable accommodation.
- Provisions for the effective dissemination of the written procedures and sufficient training.
- For further information, consult the *EEOC Policy Guidance on Executive Order 13164: Establishing Procedures to Facilitate the Provision of Reasonable Accommodation* (10/20/00).

Element Five - Efficiency

- The agency must evaluate its EEO complaint resolution process to ensure it is efficient, fair and impartial. Processing times should not exceed those provided for in 29 C.F.R. Part 1614.
  - The agency's complaint process must provide for neutral adjudication; consequently, the agency's EEO office must be kept separate from the legal defense arm of the agency (*i.e.*, the Office of General Counsel) or other agency offices having conflicting or competing interests.
  - Agencies must establish and make available an ADR program that facilitates an early, effective, neutral, efficient informal resolution of disputes. This enables disputants to potentially resolve disputes in a quick, amicable and cost effective manner.
  - The agency should have a system for identifying, monitoring and reporting significant trends reflected by complaint processing activity. Analysis of data relating to the nature and disposition of EEO complaints can provide useful insight into the extent to which an agency is meeting its obligations under Title VII and the Rehabilitation Act.
  - The agency should have a system for ensuring timely and complete compliance with EEOC orders, as well as the orders of other adjudicatory bodies, and implementation of the provisions of settlement/resolution agreements.
- The agency must have in place adequate and accurate information collection systems, which are integrated into the agency's information management infrastructure, that will provide the ability to conduct a wide array of periodic examinations of the agency's Title VII and Section 501 workforce profile(s). Such systems will be used to collect data, and monitor and evaluate its EEO programs. All gencies shall provide for the following:
  - A data collection system that allows the agency to identify and evaluate information related to management actions affecting employment status. The system should be capable of tracking applicant flow data for each selection made by the agency identified by race, national origin, sex, and, where known, disability, as well as disposition of each application. 29 C.F.R. § 1607.
  - A system capable of monitoring employment trends through review of personnel transactions and other historical data.
  - A system capable of tracking recruitment efforts to permit data analyses of these efforts.
- The system shall allow integration of comprehensive management, personnel, and budget planning with Title VII and Rehabilitation Act program planning.

- All agencies shall also provide for a complaint tracking and monitoring system that permits the agency to identify the location, status, and length of time elapsed at each stage of the EEO complaint process, the issues and the bases of the complaints, the aggrieved individuals, the involved management officials and other information necessary to analyze complaint activity to identify trends.
- All agencies must be mindful of the provisions of the Privacy Act of 1974, 5 U.S.C. § 552a, as amended, which regulate the collection, maintenance, use and dissemination of personal information by federal executive branch agencies. All agencies must balance the need to maintain information about individuals (such as aggrieved individuals and involved management officials) with the rights of such individuals to be protected against unwarranted invasions of their privacy stemming from federal agencies' collection, maintenance, use and disclosure of personal information about them. Accordingly, agency data collecting systems and complaint tracking and monitoring systems must be devised and implemented in a manner which complies with the Privacy Act. As always, agencies should guard against unwarranted disclosure of this information and ensure that appropriate protective measures exist to safeguard the information.
- Agencies are encouraged to consult with EEOC to learn which federal agencies have best practices that can be used as a model.

Element Six - Responsiveness and Legal Compliance

- The head of the agency or agency head designee shall certify to the EEOC that the agency is in full compliance with the EEO laws and EEOC regulations, policy guidance, and other written instructions. This annual certification will be provided on EEOC FORM 715-01 PART F.
- All agencies shall report their EEO program efforts and accomplishments to the EEOC and respond to EEOC directives and orders, including final orders contained in administrative decisions, in accordance with instructions, time frames and deadlines.
- All agencies shall similarly comply with orders and directives of other adjudicatory bodies with concurrent jurisdiction over the EEO laws.

The following instructions explain the purpose of and how to fill out the self-assessment checklist.

Agency Self-Assessment Checklist

Purpose of the Self-Assessment Checklist

The following Self-Assessment Checklist is designed to provide an efficient and effective means for each federal agency to determine whether its overall EEO program is properly established and compliant with the essential elements (standards) set forth in EEO MD-715.

The Self-Assessment Checklist is intended to guide an agency through each essential element and is aimed at promoting compliance, quality, and timeliness in all facets of the agency's overall EEO program. While not the only method of assessment, using this checklist will assist the agency in identifying trends and/or issues for making informed decisions on topics where the agency needs to provide more attention. Use of the checklist also permits certification that the agency has conducted the required annual self-assessment (see PART F of EEOC FORM 715-01).

The Self-Assessment Checklist also is included as PART G of EEOC FORM 715-01. Although submission of PART G of EEOC FORM 715-01 is optional, agencies must nevertheless perform the mandatory self-assessment by completing the Checklist. Agencies also are responsible for maintaining such supporting documentation and data relative to the establishment of a model EEO program, regardless of whether they opt to submit PART G of EEOC FORM 715-01. All agencies must retain the Checklist and supporting

documentation and make it available upon request by the EEOC. Such documentation should not be submitted with EEOC FORM 715-01 even if the agency opts to submit PART G.

Whether or not an agency chooses to submit PART G of FORM 715-01, every agency is still required to develop plans for addressing "no" responses from the checklist. Agencies required to submit PART H of FORM 715-01 (see the chart on page three of Section III) must submit a PART H for each problem (or cluster of problems) that the agency has identified for correction or improvement.

Finally, if an agency submits its Self-Assessment Checklist as PART G and highlights the best practices it utilizes, the Commission may share those practices with the EEO community as a whole.

Set-up of the Self-Assessment Checklist

For each essential element, the checklist provides a series of " indicator" statements which are followed by another series of questions (measures) that will assist the agency in determining whether its EEO program(s) are properly established.

To the right of the measures, there are three columns. The first two columns are provided for the agency to indicate "yes" or "no" as to whether the measure has or has not been met. The third column provides space for the agency to indicate any appropriate comments.

How to use the Self-Assessment Checklist

Where "no" responses to questions are noted, the agency should explore for identification of program weaknesses or deficiencies. The results of each such exploration are reported on the EEO Plan For Obtaining the Essential Elements of a Model EEO Program, EEOC FORM 715-01 PART H.

Not all identified potential problems will necessarily require development of an EEOC FORM 715-01 PART H.

For example, if an agency head was only recently installed (i.e., within the last 2 months), a "no" response to the compliance indicator - "EEO Policy statements are up-to-date" - the agency should use the space provided in the far right column of FORM 715-01 PART G, to report when the policy statement will be issued by the new agency head.

There may also be instances where an agency's "no" response actually is intended to indicate "not applicable." In such instances, the agency will check the "no" column but indicate "not applicable" in the comment column and provide a succinct explanation. For example, some of the smaller, volunteer-service agencies, such as The Peace Corps and The Corporation for National and Community Service, have over 75% of their workforces employed in temporary jobs. For these agencies, career development/training opportunities and competitive promotion programs are not provided to the extent that most other federal agencies provide such opportunities and programs. Similarly, for such agencies permanent appointments are almost non-existent, and thus the opportunity to convert an employee with a targeted disability from a "Schedule A" temporary appointment to a permanent appointment is very limited.

EEOC FORM
715-01
PART G

U.S. Equal Employment Opportunity Commission
FEDERAL AGENCY ANNUAL EEO PROGRAM STATUS REPORT
AGENCY SELF-ASSESSMENT CHECKLIST MEASURING ESSENTIAL ELEMENTS

Essential Element A: DEMONSTRATED COMMITMENT FROM AGENCY LEADERSHIP
Requires the agency head to issue written policy statements ensuring a workplace free of discriminatory harassment and a commitment to equal employment opportunity.

Compliance	**EEO policy statements are up-to-date.**	**Measure**	**For all unmet**

Indicator		has been met		measures, provide a brief explanation in the space below or complete and attach an EEOC FORM 715-01 PART H to the agency's status report
Measures		Yes	No	
The Agency Head was installed on _____. The EEO policy statement was issued on _____. Was the EEO policy Statement issued within 6 - 9 months of the installation of the Agency Head? If no, provide an explanation.				
During the current Agency Head's tenure, has the EEO policy Statement been re-issued annually? If no, provide an explanation.				
Are new employees provided a copy of the EEO policy statement during orientation?				
When an employee is promoted into the supervisory ranks, is s/he provided a copy of the EEO policy statement?				
Compliance Indicator	**EEO policy statements have been communicated to all employees.**	**Measure has been met**		**For all unmet measures, provide a brief explanation in the space below or complete and attach an EEOC FORM 715-01 PART H to the agency's status report**
Measures		**Yes**	**No**	
Have the heads of subordinate reporting components communicated support of all agency EEO policies through the ranks?				
Has the agency made written materials available to all employees and applicants, informing them of the variety of EEO programs and administrative and judicial remedial procedures available to them?				
Has the agency prominently posted such written materials in all personnel offices, EEO offices, and on the agency's internal website? **[see 29 CFR §1614.102(b)(5)]**				
Compliance Indicator	**Agency EEO policy is vigorously enforced by agency management.**	**Measure has been met**		**For all unmet measures, provide a brief explanation in the space below or complete and**

Measures	Yes	No	attach an EEOC FORM 715-01 PART H to the agency's status report
Are managers and supervisors evaluated on their commitment to agency EEO policies and principles, including their efforts to:			
resolve problems/disagreements and other conflicts in their respective work environments as they arise?			
address concerns, whether perceived or real, raised by employees and following-up with appropriate action to correct or eliminate tension in the workplace?			
support the agency's EEO program through allocation of mission personnel to participate in community out-reach and recruitment programs with private employers, public schools and universities?			
ensure full cooperation of employees under his/her supervision with EEO office officials such as EEO Counselors, EEO Investigators, etc.?			
ensure a workplace that is free from all forms of discrimination, harassment and retaliation?			
ensure that subordinate supervisors have effective managerial, communication and interpersonal skills in order to supervise most effectively in a workplace with diverse employees and avoid disputes arising from ineffective communications ?			
ensure the provision of requested religious accommodations when such accommodations do not cause an undue hardship?			
ensure the provision of requested disability accommodations to qualified individuals with disabilities when such accommodations do not cause an undue hardship?			
Have all employees been informed about what behaviors are inappropriate in the workplace and that this behavior may result in disciplinary actions?			
Describe what means were utilized by the agency to so inform its workforce about the penalties for unacceptable behavior.			
Have the procedures for reasonable accommodation for individuals with disabilities been made readily available/accessible to all employees by disseminating such procedures during orientation of new employees and by making such procedures available on the World Wide Web or Internet?			
Have managers and supervisor been trained on their responsibilities under the procedures for reasonable accommodation?			

Essential Element B: INTEGRATION OF EEO INTO THE AGENCY'S STRATEGIC MISSION
Requires that the agency's EEO programs be organized and structured to maintain a workplace that is free from discrimination in any of the agency's policies, procedures or practices and supports the agency's strategic mission.

Compliance Indicator / Measures	The reporting structure for the EEO Program provides the Principal EEO Official with appropriate authority and resources to effectively carry out a successful EEO Program.	Measure has been met: Yes	Measure has been met: No	For all unmet measures, provide a brief explanation in the space below or complete and attach an EEOC FORM 715-01 PART H to the agency's status report
Is the EEO Director under the direct supervision of the agency head? **[see 29 CFR §1614.102(b)(4)]** For subordinate level reporting components, is the EEO Director/Officer under the immediate supervision of the lower level component's head official? (For example, does the Regional EEO Officer report to the Regional Administrator?)				
Are the duties and responsibilities of EEO officials clearly defined?				
Do the EEO officials have the knowledge, skills, and abilities to carry out the duties and responsibilities of their positions?				
If the agency has 2nd level reporting components, are there organizational charts that clearly define the reporting structure for EEO programs?				
If the agency has 2nd level reporting components, does the agency-wide EEO Director have authority for the EEO programs within the subordinate reporting components?				
If not, please describe how EEO program authority is delegated to subordinate reporting components.				

Compliance Indicator	The EEO Director and other EEO professional staff responsible for EEO programs have regular and effective means of informing the agency head and senior management officials of the status of EEO programs and are involved in, and consulted on, management/personnel actions.	Measure has been met	For all unmet measures, provide a brief explanation in the space below or complete and

Measures		**Yes**	**No**	**attach an EEOC FORM 715-01 PART H to the agency's status report**
Does the EEO Director/Officer have a regular and effective means of informing the agency head and other top management officials of the effectiveness, efficiency and legal compliance of the agency's EEO program?				
Following the submission of the immediately preceding FORM 715-01, did the EEO Director/Officer present to the head of the agency and other senior officials the "State of the Agency" briefing covering all components of the EEO report, including an assessment of the performance of the agency in each of the six elements of the Model EEO Program and a report on the progress of the agency in completing its barrier analysis including any barriers it identified and/or eliminated or reduced the impact of?				
Are EEO program officials present during agency deliberations prior to decisions regarding recruitment strategies, vacancy projections, succession planning, selections for training/career development opportunities, and other workforce changes?				
Does the agency consider whether any group of employees or applicants might be negatively impacted prior to making human resource decisions such as re-organizations and re-alignments?				
Are management/personnel policies, procedures and practices examined at regular intervals to assess whether there are hidden impediments to the realization of equality of opportunity for any group(s) of employees or applicants? **[see 29 C.F.R. § 1614.102(b)(3)]**				
Is the EEO Director included in the agency's strategic planning, especially the agency's human capital plan, regarding succession planning, training, etc., to ensure that EEO concerns are integrated into the agency's strategic mission?				
Compliance Indicator	**The agency has committed sufficient human resources and budget allocations to its EEO programs to ensure successful operation.**	**Measure has been met**		**For all unmet measures, provide a brief explanation in the space below or complete and attach an EEOC FORM 715-01 PART H to the agency's status report**
Measures		**Yes**	**No**	
Does the EEO Director have the authority and funding to ensure implementation of agency EEO action plans to improve EEO program efficiency and/or eliminate identified barriers to the realization of				

equality of opportunity?			
Are sufficient personnel resources allocated to the EEO Program to ensure that agency self-assessments and self-analyses prescribed by EEO MD-715 are conducted annually and to maintain an effective complaint processing system?			
Are statutory/regulatory EEO related Special Emphasis Programs sufficiently staffed?			
Federal Women's Program - 5 U.S.C. 7201; 38 U.S.C. 4214; Title 5 CFR, Subpart B, 720.204			
Hispanic Employment Program - Title 5 CFR, Subpart B, 720.204			
People With Disabilities Program Manager; Selective Placement Program for Individuals With Disabilities - Section 501 of the Rehabilitation Act; Title 5 U.S.C. Subpart B, Chapter 31, Subchapter I-3102; 5 CFR 213.3102(t) and (u); 5 CFR 315.709			
Are other agency special emphasis programs monitored by the EEO Office for coordination and compliance with EEO guidelines and principles, such as FEORP - 5 CFR 720; Veterans Employment Programs; and Black/African American; American Indian/Alaska Native, Asian American/Pacific Islander programs?			

Compliance Indicator	**The agency has committed sufficient budget to support the success of its EEO Programs.**	**Measure has been met**		**For all unmet measures, provide a brief explanation in the space below or complete and attach an EEOC FORM 715-01 PART H to the agency's status report**
Measures		**Yes**	**No**	
Are there sufficient resources to enable the agency to conduct a thorough barrier analysis of its workforce, including the provision of adequate data collection and tracking systems				
Is there sufficient budget allocated to all employees to utilize, when desired, all EEO programs, including the complaint processing program and ADR, and to make a request for reasonable accommodation? (Including subordinate level reporting components?)				
Has funding been secured for publication and distribution of EEO materials (e.g. harassment policies, EEO posters, reasonable accommodations procedures, etc.)?				
Is there a central fund or other mechanism for funding supplies, equipment and services necessary to provide disability accommodations?				

Does the agency fund major renovation projects to ensure timely compliance with Uniform Federal Accessibility Standards?			
Is the EEO Program allocated sufficient resources to train all employees on EEO Programs, including administrative and judicial remedial procedures available to employees?			
Is there sufficient funding to ensure the prominent posting of written materials in all personnel and EEO offices? **[see 29 C.F.R. § 1614.102(b)(5)]**			
Is there sufficient funding to ensure that all employees have access to this training and information?			
Is there sufficient funding to provide all managers and supervisors with training and periodic up-dates on their EEO responsibilities:			
for ensuring a workplace that is free from all forms of discrimination, including harassment and retaliation?			
to provide religious accommodations?			
to provide disability accommodations in accordance with the agency's written procedures?			
in the EEO discrimination complaint process?			
to participate in ADR?			

Essential Element C: MANAGEMENT AND PROGRAM ACCOUNTABILITY
This element requires the Agency Head to hold all managers, supervisors, and EEO Officials responsible for the effective implementation of the agency's EEO Program and Plan.

Compliance Indicator / **Measures**	**EEO program officials advise and provide appropriate assistance to managers/supervisors about the status of EEO programs within each manager's or supervisor's area or responsibility.**	**Measure has been met**		**For all unmet measures, provide a brief explanation in the space below or complete and attach an EEOC FORM 715-01 PART H to the agency's status report**
		Yes	**No**	
Are regular (monthly/quarterly/semi-annually) EEO updates provided to management/supervisory officials by EEO program officials?				
Do EEO program officials coordinate the development and implementation of EEO Plans with all appropriate agency managers to include Agency Counsel, Human Resource Officials, Finance, and the Chief information Officer?				
Compliance Indicator	**The Human Resources Director and the EEO Director meet regularly to assess whether**	**Measure has been**		**For all unmet measures,**

Measures	**personnel programs, policies, and procedures are in conformity with instructions contained in EEOC management directives. [see 29 CFR § 1614.102(b)(3)]**	**met**		**provide a brief explanation in the space below or complete and attach an EEOC FORM 715-01 PART H to the agency's status report**
		Yes	**No**	
Have time-tables or schedules been established for the agency to review its Merit Promotion Program Policy and Procedures for systemic barriers that may be impeding full participation in promotion opportunities by all groups?				
Have time-tables or schedules been established for the agency to review its Employee Recognition Awards Program and Procedures for systemic barriers that may be impeding full participation in the program by all groups?				
Have time-tables or schedules been established for the agency to review its Employee Development/Training Programs for systemic barriers that may be impeding full participation in training opportunities by all groups?				
Compliance Indicator	**When findings of discrimination are made, the agency explores whether or not disciplinary actions should be taken.**	**Measure has been met**		**For all unmet measures, provide a brief explanation in the space below or complete and attach an EEOC FORM 715-01 PART H to the agency's status report**
Measures		**Yes**	**No**	
Does the agency have a disciplinary policy and/or a table of penalties that covers employees found to have committed discrimination?				
Have all employees, supervisors, and managers been informed as to the penalties for being found to perpetrate discriminatory behavior or for taking personnel actions based upon a prohibited basis?				
Has the agency, when appropriate, disciplined or sanctioned managers/supervisors or employees found to have discriminated over the past two years?				
If so, cite number found to have discriminated and list penalty /disciplinary action for each type of violation.				
Does the agency promptly (within the established time frame) comply with EEOC, Merit Systems Protection Board, Federal Labor Relations Authority, labor arbitrators, and District Court orders?				

Does the agency review disability accommodation decisions/actions to ensure compliance with its written procedures and analyze the information tracked for trends, problems, etc.?			

Essential Element D: PROACTIVE PREVENTION

Requires that the agency head makes early efforts to prevent discriminatory actions and eliminate barriers to equal employment opportunity in the workplace.

Compliance Indicator / **Measures**	**Analyses to identify and remove unnecessary barriers to employment are conducted throughout the year.**	**Measure has been met**		**For all unmet measures, provide a brief explanation in the space below or complete and attach an EEOC FORM 715-01 PART H to the agency's status report**
		Yes	**No**	
Do senior managers meet with and assist the EEO Director and/or other EEO Program Officials in the identification of barriers that may be impeding the realization of equal employment opportunity?				
When barriers are identified, do senior managers develop and implement, with the assistance of the agency EEO office, agency EEO Action Plans to eliminate said barriers?				
Do senior managers successfully implement EEO Action Plans and incorporate the EEO Action Plan Objectives into agency strategic plans?				
Are trend analyses of workforce profiles conducted by race, national origin, sex and disability?				
Are trend analyses of the workforce's major occupations conducted by race, national origin, sex and disability?				
Are trends analyses of the workforce's grade level distribution conducted by race, national origin, sex and disability?				
Are trend analyses of the workforce's compensation and reward system conducted by race, national origin, sex and disability?				
Are trend analyses of the effects of management/personnel policies, procedures and practices conducted by race, national origin, sex and disability?				

Compliance Indicator	**The use of Alternative Dispute Resolution (ADR) is encouraged by senior management.**	**Measure has been met**	**For all unmet measures, provide a brief explanation in the space below or complete and**

Measures		Yes	No	attach an EEOC FORM 715-01 PART H to the agency's status report
Are all employees encouraged to use ADR?				
Is the participation of supervisors and managers in the ADR process required?				

Essential Element E: EFFICIENCY
Requires that the agency head ensure that there are effective systems in place for evaluating the impact and effectiveness of the agency's EEO Programs as well as an efficient and fair dispute resolution process.

Compliance Indicator / Measures	The agency has sufficient staffing, funding, and authority to achieve the elimination of identified barriers.	Measure has been met: Yes	Measure has been met: No	For all unmet measures, provide a brief explanation in the space below or complete and attach an EEOC FORM 715-01 PART H to the agency's status report
Does the EEO Office employ personnel with adequate training and experience to conduct the analyses required by MD-715 and these instructions?				
Has the agency implemented an adequate data collection and analysis systems that permit tracking of the information required by MD-715 and these instructions?				
Have sufficient resources been provided to conduct effective audits of field facilities' efforts to achieve a model EEO program and eliminate discrimination under Title VII and the Rehabilitation Act?				
Is there a designated agency official or other mechanism in place to coordinate or assist with processing requests for disability accommodations in all major components of the agency?				
Are 90% of accommodation requests processed within the time frame set forth in the agency procedures for reasonable accommodation?				

Compliance Indicator / Measures	The agency has an effective complaint tracking and monitoring system in place to increase the effectiveness of the agency's EEO Programs.	Measure has been met: Yes	Measure has been met: No	For all unmet measures, provide a brief explanation in the space below or complete and attach an EEOC FORM 715-01 PART H to the agency's status

			report
Does the agency use a complaint tracking and monitoring system that allows identification of the location, and status of complaints and length of time elapsed at each stage of the agency's complaint resolution process?			
Does the agency's tracking system identify the issues and bases of the complaints, the aggrieved individuals/complainants, the involved management officials and other information to analyze complaint activity and trends?			
Does the agency hold contractors accountable for delay in counseling and investigation processing times?			
If yes, briefly describe how:			
Does the agency monitor and ensure that new investigators, counselors, including contract and collateral duty investigators, receive the 32 hours of training required in accordance with EEO Management Directive MD-110?			
Does the agency monitor and ensure that experienced counselors, investigators, including contract and collateral duty investigators, receive the 8 hours of refresher training required on an annual basis in accordance with EEO Management Directive MD-110?			
Compliance Indicator	**The agency has sufficient staffing, funding and authority to comply with the time frames in accordance with the EEOC (29 C.F.R. Part 1614) regulations for processing EEO complaints of employment discrimination.**	**Measure has been met**	**For all unmet measures, provide a brief explanation in the space below or complete and attach an EEOC FORM 715-01 PART H to the agency's status report**
Measures		**Yes** / **No**	
Are benchmarks in place that compare the agency's discrimination complaint processes with 29 C.F.R. Part 1614?			
Does the agency provide timely EEO counseling within 30 days of the initial request or within an agreed upon extension in writing, up to 60 days?			
Does the agency provide an aggrieved person with written notification of his/her rights and responsibilities in the EEO process in a timely fashion?			
Does the agency complete the investigations within the applicable prescribed time frame?			

When a complainant requests a final agency decision, does the agency issue the decision within 60 days of the request?			
When a complainant requests a hearing, does the agency immediately upon receipt of the request from the EEOC AJ forward the investigative file to the EEOC Hearing Office?			
When a settlement agreement is entered into, does the agency timely complete any obligations provided for in such agreements?			
Does the agency ensure timely compliance with EEOC AJ decisions which are not the subject of an appeal by the agency?			

Compliance Indicator	**There is an efficient and fair dispute resolution process and effective systems for evaluating the impact and effectiveness of the agency's EEO complaint processing program.**	**Measure has been met**		**For all unmet measures, provide a brief explanation in the space below or complete and attach an EEOC FORM 715-01 PART H to the agency's status report**
Measures		**Yes**	**No**	
In accordance with 29 C.F.R. §1614.102(b), has the agency established an ADR Program during the pre-complaint and formal complaint stages of the EEO process?				
Does the agency require all managers and supervisors to receive ADR training in accordance with EEOC (29 C.F.R. Part 1614) regulations, with emphasis on the federal government's interest in encouraging mutual resolution of disputes and the benefits associated with utilizing ADR?				
After the agency has offered ADR and the complainant has elected to participate in ADR, are the managers required to participate?				
Does the responsible management official directly involved in the dispute have settlement authority?				

Compliance Indicator	**The agency has effective systems in place for maintaining and evaluating the impact and effectiveness of its EEO programs.**	**Measure has been met**		**For all unmet measures, provide a brief explanation in the space below or complete and attach an EEOC FORM 715-01 PART H to the agency's status report**
Measures		**Yes**	**No**	
Does the agency have a system of management controls in place to ensure the timely, accurate, complete and consistent reporting of EEO complaint data to the EEOC?				

Does the agency provide reasonable resources for the EEO complaint process to ensure efficient and successful operation in accordance with 29 C.F.R. § 1614.102(a)(1)?			
Does the agency EEO office have management controls in place to monitor and ensure that the data received from Human Resources is accurate, timely received, and contains all the required data elements for submitting annual reports to the EEOC?			
Do the agency's EEO programs address all of the laws enforced by the EEOC?			
Does the agency identify and monitor significant trends in complaint processing to determine whether the agency is meeting its obligations under Title VII and the Rehabilitation Act?			
Does the agency track recruitment efforts and analyze efforts to identify potential barriers in accordance with MD-715 standards?			
Does the agency consult with other agencies of similar size on the effectiveness of their EEO programs to identify best practices and share ideas?			

Compliance Indicator	**The agency ensures that the investigation and adjudication function of its complaint resolution process are separate from its legal defense arm of agency or other offices with conflicting or competing interests.**	**Measure has been met**		**For all unmet measures, provide a brief explanation in the space below or complete and attach an EEOC FORM 715-01 PART H to the agency's status report**
Measures		**Yes**	**No**	
Are legal sufficiency reviews of EEO matters handled by a functional unit that is separate and apart from the unit which handles agency representation in EEO complaints?				
Does the agency discrimination complaint process ensure a neutral adjudication function?				
If applicable, are processing time frames incorporated for the legal counsel's sufficiency review for timely processing of complaints?				

Essential Element F: RESPONSIVENESS AND LEGAL COMPLIANCE
This element requires that federal agencies are in full compliance with EEO statutes and EEOC regulations, policy guidance, and other written instructions.

Compliance Indicator	**Agency personnel are accountable for timely compliance with orders issued by EEOC Administrative Judges.**	**Measure has been met**	**For all unmet measures, provide a brief explanation in the space below or complete and**

Measures		Yes	No	attach an EEOC FORM 715-01 PART H to the agency's status report
	Does the agency have a system of management control to ensure that agency officials timely comply with any orders or directives issued by EEOC Administrative Judges?			
Compliance Indicator	**The agency's system of management controls ensures that the agency timely completes all ordered corrective action and submits its compliance report to EEOC within 30 days of such completion.**	Measure has been met		For all unmet measures, provide a brief explanation in the space below or complete and attach an EEOC FORM 715-01 PART H to the agency's status report
Measures		Yes	No	
Does the agency have control over the payroll processing function of the agency? If Yes, answer the two questions below.				
Are there steps in place to guarantee responsive, timely, and predictable processing of ordered monetary relief?				
Are procedures in place to promptly process other forms of ordered relief?				
Compliance Indicator	**Agency personnel are accountable for the timely completion of actions required to comply with orders of EEOC.**	Measure has been met		For all unmet measures, provide a brief explanation in the space below or complete and attach an EEOC FORM 715-01 PART H to the agency's status report
Measures		Yes	No	
Is compliance with EEOC orders encompassed in the performance standards of any agency employees?				
If so, please identify the employees by title in the comments section, and state how performance is measured.				
Is the unit charged with the responsibility for compliance with EEOC orders located in the EEO office?				
If not, please identify the unit in which it is located, the number of employees in the unit, and their grade levels in the comments section.				

Have the involved employees received any formal training in EEO compliance?			
Does the agency promptly provide to the EEOC the following documentation for completing compliance:			
Attorney Fees: Copy of check issued for attorney fees and /or a narrative statement by an appropriate agency official, or agency payment order dating the dollar amount of attorney fees paid?			
Awards: A narrative statement by an appropriate agency official stating the dollar amount and the criteria used to calculate the award?			
Back Pay and Interest: Computer print-outs or payroll documents outlining gross back pay and interest, copy of any checks issued, narrative statement by an appropriate agency official of total monies paid?			
Compensatory Damages: The final agency decision and evidence of payment, if made?			
Training: Attendance roster at training session(s) or a narrative statement by an appropriate agency official confirming that specific persons or groups of persons attended training on a date certain?			
Personnel Actions (e.g., Reinstatement, Promotion, Hiring, Reassignment): Copies of SF-50s			
Posting of Notice of Violation: Original signed and dated notice reflecting the dates that the notice was posted. A copy of the notice will suffice if the original is not available.			
Supplemental Investigation: 1. Copy of letter to complainant acknowledging receipt from EEOC of remanded case. 2. Copy of letter to complainant transmitting the Report of Investigation (not the ROI itself unless specified). 3. Copy of request for a hearing (complainant's request or agency's transmittal letter).			
Final Agency Decision (FAD): FAD or copy of the complainant's request for a hearing.			
Restoration of Leave: Print-out or statement identifying the amount of leave restored, if applicable. If not, an explanation or statement.			
Civil Actions: A complete copy of the civil action complaint demonstrating same issues raised as in compliance matter.			
Settlement Agreements: Signed and dated agreement with specific dollar amounts, if applicable. Also, appropriate documentation of relief is provided.			

Footnotes:

1. *See* 29 C.F.R. § 1614.102.

2. When an agency makes modifications to its procedures, the procedures must be resubmitted to the Commission. *See EEOC Policy Guidance on Executive Order 13164: Establishing Procedures to Facilitate the Provision of Reasonable Accommodation* (10/20/00), Question 28.

This page was last modified on July 20, 2004.


Return to Home Page

Equal Employment Opportunity (EEO) Terminology

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Administrative Judge (AJ): An official assigned by the Equal Employment Opportunity Commission (EEOC) to hold hearings on formal complaints of discrimination and to otherwise process individual or class complaints for the EEOC.

Affirmative Action: Positive steps taken by an employer which contribute toward greater employment opportunities for minorities, females, the elderly, and the disabled. In federal employment, extra effort must be made to include qualified women, minorities, employees over 40, and the disabled at grade levels and in job categories where they are under represented.

Affirmative Action Plans/Affirmative Employment Plan: Written plans for programs required by Executive Order 11478 and other laws and regulations. AAP's may contain studies which show how the work force at the activity has been used, and may include goals and timetables for increasing the representation of protected class members in those areas where they have been under represented.

Age Discrimination: A claim of discrimination based on age by an individual who is at least 40 years of age at the time of the alleged discriminatory act.

Aggrieved Person: A person who believes that he/she has been discriminated against in some way and makes his/her concerns known.

Allegation of Reprisal: A claim of restraint, interference, coercion, discrimination, or retaliation in connection with presenting or processing a complaint or because of any opposition to an employment practice made unlawful under Title 29 CFR part 1614.

Complainant: An employee, a former employee, or an applicant for employment who files a formal complaint of discrimination based on his/her race, color, religion, sex, national origin, age (40), physical or mental disability and/or reprisal.

Discrimination: Any act or failure to act, impermissibly based in whole or in part on a person's race, color, religion, sex, national origin, age, physical or mental handicap, and/or reprisal, that adversely affects privileges, benefits, working conditions, results in disparate treatment, or had a disparate impact on employees or applicants.

Disparate Impact: Under EEO law, less favorable effect for one group than for another. Disparate impact results when rules applied to all employees have a different and more inhibiting effect on women and minority groups than on the majority. For example, nonessential educational requirements for certain jobs can have a disparate impact on minority groups looking for work, as they often have been limited in their access to educational opportunities.

Disparate Treatment: Inconsistent application of rules and policies to one group of people over another. Discrimination may result when rules and policies are applied differently to members of protected classes. Disciplining Hispanic and Afro-American employees for tardiness, while ignoring tardiness among other employees, is an example of disparate treatment. Such inconsistent application of rules often leads to complaints.

EEO Counselor: An employee of the EEO Office, working under the direction of the EEO Manager, who makes informal inquiries and seeks resolution of informal complaints.

Equal Employment Opportunity: The goal of laws which make some types of discrimination in employment illegal. Equal employment opportunity will become a reality when each U.S. citizen has an equal chance to enjoy the benefits of employment. EEO is not a guarantee of employment for anyone. Under EEO law, only job related factors can be used to determine if an individual is qualified for a particular job. Ideally, EEO laws and Affirmative Action programs combine to achieve equal employment opportunities. See EEO law, Affirmative Action, and Affirmative Action Plan/Affirmative Employment Plan.

Equal Employment Opportunity Commission (EEOC): The Federal agency with overall responsibility for federal sector complaints. The EEOC issues policy and regulations on the discrimination complaint system, holds hearings and makes findings and recommendations on

discrimination complaints; and, makes final decisions on discrimination complaints that have been appealed. It also reviews, upon request, decisions of negotiated grievances and Merit Systems Protection Board (MSPB) appeals if they include issues of discrimination.

Equal Employment Opportunity Laws: Five laws which prohibit discrimination on the basis of race, color, religion, sex, national origin, physical handicap and mental handicap in any terms, conditions, or privileges of employment. The five EEO laws are:

- The Equal Pay Act of 1963, as amended.
- Title VII of the Civil Rights Act of 1964, as amended by the Equal Employment Opportunity Act of 1972 and the Pregnancy Disability Act of 1978.
- The Rehabilitation Act of 1973, as amended.
- The Age Discrimination in Employment Act of 1967, as amended.
- The Civil Rights Act of 1991.

Ethnic Group: A group of people who share a common religion, color, or national origin. Irish-Americans, Mexican-Americans, German-Americans, Italian-Americans, Hindus, Moslems, and Jews are examples of ethnic groups. Some members of ethnic groups participate in the customs and practices of their groups, while others do not. Discrimination based on these customs and practices may be illegal under EEO law. See Minority.

Formal Complaint: A written complaint, DLA Form 1808, filed under 29 CFR 1614, alleging that a specific act of discrimination or reprisal has/have taken place that is personal to the individual.

Hearing: The presentation of such oral and written evidence concerning a complaint of discrimination presented before the EEOC.

Informal Complaint: A matter of alleged discrimination which an aggrieved person brings to the attention of the EEO Counselor before a formal discrimination complaint is filed.

Investigative Report: The report of investigation (ROI) prepared by an investigator after a formal discrimination complaint is filed, accepted for processing, and is investigated.

Job Related: Essential to job performance. The knowledge, skills, abilities, and experience necessary to perform a particular job. Tests are job related if they test whether an applicant or employee can perform the job in question. A rule or practice is job related if it is necessary for the safe and efficient performance of a particular job. For example, a rule prohibiting employees from wearing loose, flowing clothing around high speed rotating equipment is job related. However, the same rule applied in an office with no rotating equipment is not job related, and may have a disparate impact on some ethnic minorities.

Merit Principles: The rules established by the Office of Personnel Management that the federal government follows in hiring, promoting, and all terms and conditions of employment. One of those rules states that the selection and advancement shall be made on the basis of an applicant's or employee's ability, knowledge, and skills in fair and open competition.

Merit Systems Protection Board (MSPB): The federal agency responsible for deciding appealable personnel actions and mixed case appeals.

Minority: The smaller part of a group. A group within a country or state that differs in race, religion or national origin from the dominant group. According to EEOC guidelines, minority is used to mean four particular groups who share a race, color or national origin.

These groups are:

- American Indian or Alaskan Native. A person having origins in any of the original peoples of North America, and who maintain their culture through a tribe or community.
- Asian or Pacific Islander. A person having origins in any of the original people of the Far East, Southeast Asia, India, or the Pacific Islands. These areas include, for example, China, India, Korea, the Philippine Islands, and Samoa.
- Black (except Hispanic). A person having origins in any of the black racial groups of Africa.
- Hispanic. A person of Mexican, Puerto Rican, Cuban, Central or South American, or other Spanish culture or origin, regardless of race.

- The many peoples with origins in Europe, North Africa, or the Middle East make up the dominant white population. Of course, many more minority groups can be identified in the American population. However, they are not classified separately as minorities under EEO law. It should be noted that women are not classified as a minority. However, they have experienced the same kind of systematic exclusion from the economy as the various minorities. Thus, they are considered as having "minority status" as far as the law is concerned.

Mixed Case Appeal: An appeal filed with the MSPB which alleges that an adverse personnel action resulted, in whole or in part, because of discrimination on the basis of race, color, religion, sex, national origin, age (40), physical or mental handicap, and/or reprisal, or alleges that such action resulted in sex-based wage discrimination.

Mixed Case Complaint: A complaint involving an action appealable to MSPB which alleges that the action was taken because of discrimination. Actions appealable to the MSPB include but are not limited to removals, demotions, suspensions for more than 14 days, reductions-in-force, and furloughs for less than 30 days.

Negotiated Settlement Agreement: A written settlement agreement voluntarily signed by the complainant or agent and the agency, during the precomplaint or formal complaint process, which resolves a discrimination complaint. The terms of the agreement are binding on both parties.

Numerical Goal: A target number of qualified women and minorities hired and advanced within a given period of time through an Affirmative Action Program. A numerical goal is not a quota, as it may not be reached within the time frame. It does not permit the hiring or advancement of **unqualified** employees. Numerical goals provide a standard which allows an activity to measure the effectiveness of its Affirmative Action Program. When numerical goals are reached, the percent of women and minority group members working at appropriate grade levels and classifications will be closer to their percentage in the labor market.

Official Time: Under 29 CFR Section 1614.605, complainants have a right to a "reasonable" about of official time, if otherwise on duty, to prepare a complaint filed under this regulation. The ? is not obligated to change work schedules, incur overtime, or pay travel. However, when the an EEOC administrative judge requests the complainant's presence in connection with a complaint, the complainant will be granted official time for the duration of such meeting or hearing regardless of the tour of duty. Employees must arrange in advance with their supervisors to use this duty time. Disagreements as to what is "reasonable" time are resolved by the activity Commander or his/her designee. "Reasonable duty time" includes all time actually spent in meetings and hearings required by an EEOC official, plus a reasonable amount of preparation time. Reasonable time is generally defined in terms of hours rather than days, weeks, or months.

Office of Federal Operations (OFO): The EEOC component that handles all administrative appeals to the EEOC.

Prima Facie: This Latin term translates as "on first view", or "at first appearance". In EEO cases, complainants present evidence and arguments to support a claim of discrimination. If those arguments cannot be rebutted with additional evidence, the claim will be supported by the court within further argument. Thus, a prima facie case is established. In the EEO area, statistics of under utilization have been sufficient to make a prima facie case for discrimination.

Protected Class: The groups protected from the employment discrimination by law. These groups include men and women on the basis of sex; any group which shares a common race, religion, color, or national origin; people over 40; and people with physical or mental handicaps. Every U.S. citizen is a member of some protected class, and is entitled to the benefits of EEO law. However, the EEO laws were passed to correct a history of unfavorable treatment of women and minority group members.

Quota: Fixed hiring and promotion rates based on race, sex, or other protected class standards which must be met at all costs. In extreme cases, the courts have assigned quotas to some employers who have continued to practice illegal discrimination. The agency or any other employer cannot use quotas to meet their affirmative action goals unless a court orders it. Quotas are considered discriminatory against males and other non minority people.

Reasonable Accommodation: Any change in the work environment, in the way things are customarily done, or in the application process that enables a person with a disability to enjoy equal employment opportunities. The three general categories of reasonable accommodation are changes

to: (1) job application process to permit people with disabilities to be considered for jobs; (2) enable people with disabilities to perform the essential functions of a job; and (3) give people with disabilities equal access to the benefits and privileges of employment.

Representative: A person selected and designated in writing by a complainant or the class agent. The representative may accompany, represent, and advise in the complaint process.

Reprisal: Unlawful restraint, coercion or discrimination against complainants, their representatives, witnesses, EEO Counselors, investigators, and other agency officials with responsibility for processing EEO complaints.

Settlement: An adjustment arrived at during the precomplaint or formal complaint process, which resolves issues raised to the satisfaction of the complainant. The terms of the adjustment must be set out in a negotiated settlement agreement.

Sexual Harassment: Unwelcome sexual advances, requests for sexual favors, and/or other verbal or physical conduct of a sexual nature based on one or more of the following conditions a) Submission to such conduct is made either explicitly or implicitly a term or condition of an individual's employment b) Submission to or rejection of such conduct by an individual is used as the basis for employment decisions affecting such individual c) Such conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile, or offensive work environment.

Under Represented: Inadequately represented in the work force of a particular activity. This term is used to describe the extent to which women and minorities are represented in particular grade levels and job categories. The percentage of women and minorities in the labor market is used as a standard to determine under representation. For example, suppose there are 100 GS-12's at an agency; three of them or 3% are black. However, the black labor market for GS-12 positions at that particular activity is 15%. In this case, blacks are under represented at the GS -12 level.

Under Utilized: To use less than fully; below potential use. This term is often applied to categories of employees who are working at jobs that do not make use of their skills and abilities, although they may have been hired for those skills and abilities. When an employee is consistently assigned to "dead end" jobs, he or she may be under utilized because they are often seen as able to perform only limited tasks.

§ 4119. Training for employees under the Office of the Architect of the Capitol and the Botanic Garden

(a) The Architect of the Capitol may, by regulation, make applicable such provisions of this chapter as the Architect determines necessary to provide for training of (1) individuals employed under the Office of the Architect of the Capitol and the Botanic Garden and (2) other congressional employees who are subject to the administrative control of the Architect. The regulations shall provide for training which, in the determination of the Architect, is consistent with the training provided by agencies under the preceding sections of this chapter.

(b) The Office of Personnel Management shall provide the Architect of the Capitol with such advice and assistance as the Architect may request in order to enable the Architect to carry out the purposes of this section.

(Added Pub. L. 97–346, § 1(a), Oct. 15, 1982, 96 Stat. 1647.)

§ 4120. Training for employees of the Capitol Police

(a) The Chief of the Capitol Police may, by regulation, make applicable such provisions of this chapter as the Chief determines necessary to provide for training of employees of the Capitol Police. The regulations shall provide for training which, in the determination of the Chief, is consistent with the training provided by agencies under the preceding sections of this chapter.

(b) The Office of Personnel Management shall provide the Chief of the Capitol Police with such advice and assistance as the Chief may request in order to enable the Chief to carry out the purposes of this section.

(Added Pub. L. 108–7, div. H, title I, § 1010(a), Feb. 20, 2003, 117 Stat. 360.)

§ 4121. Specific training programs

In consultation with the Office of Personnel Management, the head of each agency shall establish—

(1) a comprehensive management succession program to provide training to employees to develop managers for the agency; and

(2) a program to provide training to managers on actions, options, and strategies a manager may use in—

(A) relating to employees with unacceptable performance;

(B) mentoring employees and improving employee performance and productivity; and

(C) conducting employee performance appraisals.

(Added Pub. L. 108–411, title II, § 201(b)(1), Oct. 30, 2004, 118 Stat. 2311.)

CHAPTER 43—PERFORMANCE APPRAISAL

SUBCHAPTER I—GENERAL PROVISIONS

SUBCHAPTER II—PERFORMANCE APPRAISAL IN THE SENIOR EXECUTIVE SERVICE

AMENDMENTS

1993—Pub. L. 103–89, § 3(b)(1)(B)(ii), Sept. 30, 1993, 107 Stat. 981, struck out item 4302a ''Establishment of performance appraisal systems for performance management and recognition system employees''.

1984—Pub. L. 98–615, title II, § 202(b), Nov. 8, 1984, 98 Stat. 3216, added item 4302a.

1978—Pub. L. 95–454, title II, § 203(a), title IV, § 405(b), Oct. 13, 1978, 92 Stat. 1131, 1170, in chapter heading substituted ''APPRAISAL'' for ''RATING'', added heading for subchapter I, in item 4302 substituted ''Establishment of performance appraisal systems'' for ''Performance-rating plans; establishment of'', in item 4303 substituted ''Actions based on unacceptable performance'' for ''Performance-rating plans; requirements for'', in item 4304 substituted ''Responsibilities of Office of Personnel Management'' for ''Ratings for performance'', in item 4305 substituted ''Regulations'' for ''Review of ratings'', struck out items 4306 to 4308 ''Performance-rating plans; inspection of'', ''Other rating procedures prohibited'', and ''Regulations'', respectively, and added item for subchapter II and items 4311 to 4315.

SUBCHAPTER I—GENERAL PROVISIONS

AMENDMENTS

1979—Pub. L. 96–54, § 2(a)(20), Aug. 14, 1979, 93 Stat. 382, added heading for subchapter I.

§ 4301. Definitions

For the purpose of this subchapter—

(1) ''agency'' means—

(A) an Executive agency; and

(B) the Government Printing Office;

but does not include—

(i) a Government corporation;

(ii) the Central Intelligence Agency, the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the National Security Agency, or any Executive agency or unit thereof which is designated by the President and the principal function of which is the conduct of foreign intelligence or counterintelligence activities; or

(iii) the Government Accountability Office;

(2) ''employee'' means an individual employed in or under an agency, but does not include—

(A) an employee outside the United States who is paid in accordance with local native prevailing wage rates for the area in which employed;

(B) an individual in the Foreign Service of the United States;

(C) a physician, dentist, nurse, or other employee in the Veterans Health Adminis-

[1] So in original. Does not conform to section catchline.

tration of the Department of Veterans Affairs whose pay is fixed under chapter 73 of title 38;

(D) an administrative law judge appointed under section 3105 of this title;

(E) an individual in the Senior Executive Service or the Federal Bureau of Investigation and Drug Enforcement Administration Senior Executive Service;

(F) an individual appointed by the President;

(G) an individual occupying a position not in the competitive service excluded from coverage of this subchapter by regulations of the Office of Personnel Management; or

(H) an individual who (i) is serving in a position under a temporary appointment for less than one year, (ii) agrees to serve without a performance evaluation, and (iii) will not be considered for a reappointment or for an increase in pay based in whole or in part on performance; and

(3) ''unacceptable performance'' means performance of an employee which fails to meet established performance standards in one or more critical elements of such employee's position.

(Pub. L. 89–554, Sept. 6, 1966, 80 Stat. 440; Pub. L. 91–375, §6(c)(8), Aug. 12, 1970, 84 Stat. 776; Pub. L. 95–251, §2(a)(1), Mar. 27, 1978, 92 Stat. 183; Pub. L. 95–454, title II, §203(a), Oct. 13, 1978, 92 Stat. 1131; Pub. L. 100–325, §2(f), May 30, 1988, 102 Stat. 581; Pub. L. 101–474, §5(e), Oct. 30, 1990, 104 Stat. 1100; Pub. L. 101–510, div. A, title XII, §1206(e), Nov. 5, 1990, 104 Stat. 1661; Pub. L. 102–54, §13(b)(2), June 13, 1991, 105 Stat. 274; Pub. L. 103–359, title V, §501(e), Oct. 14, 1994, 108 Stat. 3429; Pub. L. 104–201, div. A, title XI, §1122(a)(1), Sept. 23, 1996, 110 Stat. 2687; Pub. L. 108–271, §8(b), July 7, 2004, 118 Stat. 814; Pub. L. 110–417, [div. A], title IX, §931(a)(1), Oct. 14, 2008, 122 Stat. 4575.)

HISTORICAL AND REVISION NOTES

Derivation	*U.S. Code*	*Revised Statutes and Statutes at Large*
.....	5 U.S.C. 2001.	Sept. 30, 1950, ch. 1123, §2, 64 Stat. 1098. Sept. 1, 1954, ch. 1208, §601(a), 68 Stat. 1115. June 17, 1957, Pub. L. 85–56, §2201(21), 71 Stat. 159. July 11, 1957, Pub. L. 85–101, 71 Stat. 293. Sept. 2, 1958, Pub. L. 85–857, §13(p), 72 Stat. 1266. Mar. 26, 1964, Pub. L. 88–290, ''Sec. 306(b)'', 78 Stat. 170.

In paragraph (1), the term ''Executive agency'' is substituted for the reference to ''executive departments, the independent establishments and agencies in the executive branch, including corporations wholly owned by the United States'' and ''the General Accounting Office''. The exception of ''a Government controlled corporation'' is added in subparagraph (vii) to preserve the application of this chapter to ''corporations wholly owned by the United States''. The exceptions for Production credit corporations and Federal intermediate credit banks in former section 2001(b)(5), (6) are omitted as they are no longer ''corporations wholly owned by the United States''. Under the Farm Credit Act of 1956, 70 Stat. 659, the production credit corporations were merged in the Federal intermediate credit banks, and pursuant to that Act the Federal intermediate credit banks have ceased to be corporations owned by the United States. The exceptions for Federal land banks and banks for cooperatives in former section 2001(b)(7), (8) are omitted as included within the exception of ''a Government controlled corporation'' in subparagraph (vii).

Paragraph (2) is supplied because the definition of ''employee'' in section 2105 does not encompass individuals employed by the government of the District of Columbia. The definition in paragraph (2) does not encompass members of the uniformed services as they are not ''employed'' in or under an agency.

Paragraph (2)(E) is based on the third and fifth sentences, respectively, of former sections 1010 and 1011, which are carried into sections 5362 and 559, respectively, and section 1106(a) of the Act of Oct. 28, 1949, ch. 782, 63 Stat. 972.

Standard changes are made to conform with the definitions applicable and the style of this title as outlined in the preface to the report.

AMENDMENTS

2008—Par. (1)(ii) Pub. L. 110–417 substituted ''National Geospatial-Intelligence Agency'' for ''National Imagery and Mapping Agency''.

2004—Par. (1)(iii). Pub. L. 108–271 substituted ''Government Accountability Office'' for ''General Accounting Office''.

1996—Par. (1)(ii). Pub. L. 104–201 substituted ''National Imagery and Mapping Agency'' for ''Central Imagery Office''.

1994—Par. (1)(ii). Pub. L. 103–359 inserted ''the Central Imagery Office,'' after ''Defense Intelligence Agency,''.

1991—Par. (2)(C). Pub. L. 102–54 substituted ''Veterans Health Administration of the Department of Veterans Affairs'' for ''Department of Medicine and Surgery, Veterans' Administration''.

1990—Par. (1). Pub. L. 101–474 redesignated subpar. (C) as (B) and struck out former subpar. (B) which included Administrative Office of United States Courts within definition of ''agency''.

Par. (2)(H). Pub. L. 101–510 added subpar. (H).

1988—Par. (2)(E). Pub. L. 100–325 inserted reference to Federal Bureau of Investigation and Drug Enforcement Administration Senior Executive Service.

1978—Pub. L. 95–454 substituted provisions defining ''agency'', ''employee'', and ''unacceptable performance'' for provisions defining ''agency'' and ''employee''.

Par. (2)(E). Pub. L. 95–251 substituted ''administrative law judge'' for ''hearing examiner''.

1970—Par. (1)(ii). Pub. L. 91–375 repealed cl. (ii) which excluded postal field service from definition of ''agency''.

EFFECTIVE DATE OF 1996 AMENDMENT

Amendment by Pub. L. 104–201 effective Oct. 1, 1996, see section 1124 of Pub. L. 104–201, set out as a note under section 193 of Title 10, Armed Forces.

EFFECTIVE DATE OF 1978 AMENDMENT

Amendment by Pub. L. 95–454 effective 90 days after Oct. 13, 1978, see section 907 of Pub. L. 95–454, set out as a note under section 1101 of this title.

EFFECTIVE DATE OF 1970 AMENDMENT

Amendment by Pub. L. 91–375 effective within 1 year after Aug. 12, 1970, on date established therefor by Board of Governors of United States Postal Service and published by it in Federal Register, see section 15(a) of Pub. L. 91–375, set out as an Effective Date note preceding section 101 of Title 39, Postal Service.

§ 4302. Establishment of performance appraisal systems

(a) Each agency shall develop one or more performance appraisal systems which—

(1) provide for periodic appraisals of job performance of employees;

(2) encourage employee participation in establishing performance standards; and

(3) use the results of performance appraisals as a basis for training, rewarding, reassigning, promoting, reducing in grade, retaining, and removing employees.

(b) Under regulations which the Office of Personnel Management shall prescribe, each performance appraisal system shall provide for—

(1) establishing performance standards which will, to the maximum extent feasible, permit the accurate evaluation of job performance on the basis of objective criteria (which may include the extent of courtesy demonstrated to the public) related to the job in question for each employee or position under the system;

(2) as soon as practicable, but not later than October 1, 1981, with respect to initial appraisal periods, and thereafter at the beginning of each following appraisal period, communicating to each employee the performance standards and the critical elements of the employee's position;

(3) evaluating each employee during the appraisal period on such standards;

(4) recognizing and rewarding employees whose performance so warrants;

(5) assisting employees in improving unacceptable performance; and

(6) reassigning, reducing in grade, or removing employees who continue to have unacceptable performance but only after an opportunity to demonstrate acceptable performance.

(c) In accordance with regulations which the Office shall prescribe, the head of an agency may administer and maintain a performance appraisal system electronically.

(Pub. L. 89–554, Sept. 6, 1966, 80 Stat. 440; Pub. L. 95–454, title II, § 203(a), Oct. 13, 1978, 92 Stat. 1132; Pub. L. 102–378, § 2(18), Oct. 2, 1992, 106 Stat. 1347; Pub. L. 106–398, § 1 [[div. A], title XI, § 1104], Oct. 30, 2000, 114 Stat. 1654, 1654A–311.)

HISTORICAL AND REVISION NOTES

Derivation	*U.S. Code*	*Revised Statutes and Statutes at Large*
.....	5 U.S.C. 2002.	Sept. 30, 1950, ch. 1123, § 3, 64 Stat. 1098.

Standard changes are made to conform with the definitions applicable and the style of this title as outlined in the preface to the report.

AMENDMENTS

2000—Subsec. (c). Pub. L. 106–398 added subsec. (c).

1992—Subsec. (a)(3). Pub. L. 102–378 substituted a period for semicolon at end.

1978—Pub. L. 95–454 substituted ''Establishment of performance appraisal systems'' for ''Performance-rating plans; establishment of'' in section catchline and in text substituted provisions relating to the establishment of a performance appraisal system, for provisions relating to the establishment of performance-rating plans.

EFFECTIVE DATE OF 1978 AMENDMENT

Amendment by Pub. L. 95–454 effective 90 days after Oct. 13, 1978, see section 907 of Pub. L. 95–454, set out as a note under section 1101 of this title.

[§ 4302a. Repealed. Pub. L. 103–89, § 3(b)(1)(B)(i), Sept. 30, 1993, 107 Stat. 981]

Section, added Pub. L. 98–615, title II, § 202(a), Nov. 8, 1984, 98 Stat. 3214; amended Pub. L. 101–103, § 5(a), Sept. 30, 1989, 103 Stat. 671; Pub. L. 102–22, § 2(a), Mar. 28, 1991, 105 Stat. 71, related to the establishment of performance appraisal systems for performance management and recognition system employees.

EFFECTIVE DATE OF REPEAL

Repeal effective Nov. 1, 1993, see section 3(c) of Pub. L. 103–89, set out as an Effective Date of 1993 Amendment note under section 3372 of this title.

§ 4303. Actions based on unacceptable performance

(a) Subject to the provisions of this section, an agency may reduce in grade or remove an employee for unacceptable performance.

(b)(1) An employee whose reduction in grade or removal is proposed under this section is entitled to—

(A) 30 days' advance written notice of the proposed action which identifies—

(i) specific instances of unacceptable performance by the employee on which the proposed action is based; and

(ii) the critical elements of the employee's position involved in each instance of unacceptable performance;

(B) be represented by an attorney or other representative;

(C) a reasonable time to answer orally and in writing; and

(D) a written decision which—

(i) in the case of a reduction in grade or removal under this section, specifies the instances of unacceptable performance by the employee on which the reduction in grade or removal is based, and

(ii) unless proposed by the head of the agency, has been concurred in by an employee who is in a higher position than the employee who proposed the action.

(2) An agency may, under regulations prescribed by the head of such agency, extend the notice period under subsection (b)(1)(A) of this section for not more than 30 days. An agency may extend the notice period for more than 30 days only in accordance with regulations issued by the Office of Personnel Management.

(c) The decision to retain, reduce in grade, or remove an employee—

(1) shall be made within 30 days after the date of expiration of the notice period, and

(2) in the case of a reduction in grade or removal, may be based only on those instances of unacceptable performance by the employee—

(A) which occurred during the 1-year period ending on the date of the notice under subsection (b)(1)(A) of this section in connection with the decision; and

(B) for which the notice and other requirements of this section are complied with.

(d) If, because of performance improvement by the employee during the notice period, the employee is not reduced in grade or removed, and the employee's performance continues to be acceptable for 1 year from the date of the advance

written notice provided under subsection (b)(1)(A) of this section, any entry or other notation of the unacceptable performance for which the action was proposed under this section shall be removed from any agency record relating to the employee.

(e) Any employee who is—

(1) a preference eligible;

(2) in the competitive service; or

(3) in the excepted service and covered by subchapter II of chapter 75,

and who has been reduced in grade or removed under this section is entitled to appeal the action to the Merit Systems Protection Board under section 7701.

(f) This section does not apply to—

(1) the reduction to the grade previously held of a supervisor or manager who has not completed the probationary period under section 3321(a)(2) of this title,

(2) the reduction in grade or removal of an employee in the competitive service who is serving a probationary or trial period under an initial appointment or who has not completed 1 year of current continuous employment under other than a temporary appointment limited to 1 year or less, or

(3) the reduction in grade or removal of an employee in the excepted service who has not completed 1 year of current continuous employment in the same or similar positions.

(Pub. L. 89–554, Sept. 6, 1966, 80 Stat. 440; Pub. L. 95–454, title II, § 203(a), Oct. 13, 1978, 92 Stat. 1133; Pub. L. 101–376, § 2(b), Aug. 17, 1990, 104 Stat. 462.)

HISTORICAL AND REVISION NOTES

Derivation	*U.S. Code*	*Revised Statutes and Statutes at Large*
.....	5 U.S.C. 2004.	Sept. 30, 1950, ch. 1123, § 5, 64 Stat. 1098.

The words ''required by this chapter'' are omitted as unnecessary.

Standard changes are made to conform with the definitions applicable and the style of this title as outlined in the preface to the report.

AMENDMENTS

1990—Subsec. (e). Pub. L. 101–376 amended subsec. (e) generally. Prior to amendment, subsec. (e) read as follows: ''Any employee who is a preference eligible or is in the competitive service and who has been reduced in grade or removed under this section is entitled to appeal the action to the Merit Systems Protection Board under section 7701 of this title.''

1978—Pub. L. 95–454 substituted ''Actions based on unacceptable performance'' for ''Performance-rating plans; requirements for'' in section catchline and in text substituted provisions relating to actions based on unacceptable performance, for provisions relating to requirements for performance-rating plans.

EFFECTIVE DATE OF 1990 AMENDMENT

Section 2(c) of Pub. L. 101–376 provided that: ''The amendments made by this section [amending this section and section 7511 of this title] shall apply with respect to any personnel action taking effect on or after the effective date of this Act [see below].''

Section 4 of Pub. L. 101–376 provided that: ''This Act and the amendments made by this Act [amending this section, sections 7511 and 7701 of this title, and enacting provisions set out as notes under this section and section 7501 of this title] shall become effective on the date of the enactment of this Act [Aug. 17, 1990], and, except as provided in section 2(c) [set out above], shall apply with respect to any appeal or other proceeding brought on or after such date.''

EFFECTIVE DATE OF 1978 AMENDMENT

Amendment by Pub. L. 95–454 effective 90 days after Oct. 13, 1978, see section 907 of Pub. L. 95–454, set out as a note under section 1101 of this title.

§ 4304. Responsibilities of the Office of Personnel Management

(a) The Office of Personnel Management shall make technical assistance available to agencies in the development of performance appraisal systems.

(b)(1) The Office shall review each performance appraisal system developed by any agency under this section and determine whether the performance appraisal system meets the requirements of this subchapter.

(2) The Comptroller General shall from time to time review on a selected basis performance appraisal systems established under this subchapter to determine the extent to which any such system meets the requirements of this subchapter and shall periodically report its findings to the Office and to the Congress.

(3) If the Office determines that a system does not meet the requirements of this subchapter (including regulations prescribed under section 4305), the Office shall direct the agency to implement an appropriate system or to correct operations under the system, and any such agency shall take any action so required.

(Pub. L. 89–554, Sept. 6, 1966, 80 Stat. 440; Pub. L. 95–454, title II, § 203(a), Oct. 13, 1978, 92 Stat. 1134.)

HISTORICAL AND REVISION NOTES

Derivation	*U.S. Code*	*Revised Statutes and Statutes at Large*
.....	5 U.S.C. 2005.	Sept. 30, 1950, ch. 1123, § 6, 64 Stat. 1099.

In subsection (a)(1), the words ''corresponding to an efficiency rating of 'good' under the Veterans' Preference Act of 1944, as amended, and under laws superseded by this chapter'' in clause (1) of former section 2005 are omitted, but are carried into section 3502.

Standard changes are made to conform with the definitions applicable and the style of this title as outlined in the preface to the report.

AMENDMENTS

1978—Pub. L. 95–454 substituted ''Responsibilities of the Office of Personnel Management'' for ''Ratings for performance'' in section catchline and in text substituted provisions relating to the responsibilities of the Office of Personnel Management under this subchapter, for provisions relating to ratings for performance.

EFFECTIVE DATE OF 1978 AMENDMENT

Amendment by Pub. L. 95–454 effective 90 days after Oct. 13, 1978, see section 907 of Pub. L. 95–454, set out as a note under section 1101 of this title.

§ 4305. Regulations

The Office of Personnel Management may prescribe regulations to carry out the purpose of this subchapter.

(Pub. L. 89–554, Sept. 6, 1966, 80 Stat. 441; Pub. L. 95–454, title II, § 203(a), Oct. 13, 1978, 92 Stat. 1134.)

HISTORICAL AND REVISION NOTES

Derivation	*U.S. Code*	*Revised Statutes and Statutes at Large*
.....	5 U.S.C. 2006.	Sept. 30, 1950, ch. 1123, § 7, 64 Stat. 1099.

In subsection (c), the words ''as a matter of right'' are omitted as unnecessary.

In subsection (d), the words ''are entitled'' are substituted for ''shall be afforded an opportunity''. The word ''considers'' is substituted for ''deems to be''.

Standard changes are made to conform with the definitions applicable and the style of this title as outlined in the preface to the report.

AMENDMENTS

1978—Pub. L. 95–454 substituted ''Regulations'' for ''Review of ratings'' in section catchline and in text substituted provisions relating to regulations to carry out this subchapter, for provisions relating to review of ratings.

EFFECTIVE DATE OF 1978 AMENDMENT

Amendment by Pub. L. 95–454 effective 90 days after Oct. 13, 1978, see section 907 of Pub. L. 95–454, set out as a note under section 1101 of this title.

[§§ 4306 to 4308. Omitted]

CODIFICATION

Sections 4306 to 4308, Pub. L. 89–554, Sept. 6, 1966, 80 Stat. 441, 442, were omitted in the general revision of this chapter by the Civil Service Reform Act of 1978, Pub. L. 95–454, § 203(a), Oct. 13, 1978, 92 Stat. 1131.

Section 4306 related to inspection of performance-rating plans.

Section 4307 related to prohibition of other rating procedures.

Section 4308 related to regulations for administration of the chapter, and is covered by revised section 4305.

SUBCHAPTER II—PERFORMANCE APPRAISAL IN THE SENIOR EXECUTIVE SERVICE

§ 4311. Definitions

For the purpose of this subchapter, ''agency'', ''senior executive'', and ''career appointee'' have the meanings set forth in section 3132(a) of this title.

(Added Pub. L. 95–454, title IV, § 405(a), Oct. 13, 1978, 92 Stat. 1167.)

EFFECTIVE DATE

Subchapter effective 9 months after Oct. 13, 1978, and congressional review of provisions of sections 401 through 412 of Pub. L. 95–454, see section 415(a)(1), (b), of Pub. L. 95–454, set out as a note under section 3131 of this title.

§ 4312. Senior Executive Service performance appraisal systems

(a) Each agency shall, in accordance with standards established by the Office of Personnel Management, develop one or more performance appraisal systems designed to—

(1) permit the accurate evaluation of performance in any position on the basis of criteria which are related to the position and which specify the critical elements of the position;

(2) provide for systematic appraisals of performance of senior executives;

(3) encourage excellence in performance by senior executives; and

(4) provide a basis for making eligibility determinations for retention in the Senior Executive Service and for Senior Executive Service performance awards.

(b) Each performance appraisal system established by an agency under subsection (a) of this section shall provide—

(1) that, on or before the beginning of each rating period, performance requirements for each senior executive in the agency are established in consultation with the senior executive and communicated to the senior executive;

(2) that written appraisals of performance are based on the individual and organizational performance requirements established for the rating period involved; and

(3) that each senior executive in the agency is provided a copy of the appraisal and rating under section 4314 of this title and is given an opportunity to respond in writing and have the rating reviewed by an employee, or (with the consent of the senior executive) a commissioned officer in the uniformed services serving on active duty, in a higher level in the agency before the rating becomes final.

(c)(1) The Office shall review each agency's performance appraisal system under this section, and determine whether the agency performance appraisal system meets the requirements of this subchapter.

(2) The Comptroller General shall from time to time review performance appraisal systems under this section to determine the extent to which any such system meets the requirements under this subchapter and shall periodically report its findings to the Office and to each House of the Congress.

(3) If the Office determines that an agency performance appraisal system does not meet the requirements under this subchapter (including regulations prescribed under section 4315), the agency shall take such corrective action as may be required by the Office.

(d) A senior executive may not appeal any appraisal and rating under any performance appraisal system under this section.

(Added Pub. L. 95–454, title IV, § 405(a), Oct. 13, 1978, 92 Stat. 1167; amended Pub. L. 98–615, title III, § 306(b)(2), Nov. 8, 1984, 98 Stat. 3220.)

AMENDMENTS

1984—Subsec. (b)(3). Pub. L. 98–615 inserted '', or (with the consent of the senior executive) a commissioned officer in the uniformed services serving on active duty,'' and directed that ''executive'' be struck out which was executed by striking ''executive'' only where it appeared before ''level in the agency''.

EFFECTIVE DATE OF 1984 AMENDMENT

Amendment by Pub. L. 98–615 effective following expiration of 90-day period beginning on Nov. 8, 1984, see section 307 of Pub. L. 98–615, set out as a note under section 3393 of this title.

§ 4313. Criteria for performance appraisals

Appraisals of performance in the Senior Executive Service shall be based on both individual

and organizational performance, taking into account such factors as—

(1) improvements in efficiency, productivity, and quality of work or service, including any significant reduction in paperwork;

(2) cost efficiency;

(3) timeliness of performance;

(4) other indications of the effectiveness, productivity, and performance quality of the employees for whom the senior executive is responsible; and

(5) meeting affirmative action goals, achievement of equal employment opportunity requirements, and compliance with the merit systems principles set forth under section 2301 of this title.

(Added Pub. L. 95–454, title IV, § 405(a), Oct. 13, 1978, 92 Stat. 1168; amended Pub. L. 103–424, § 6, Oct. 29, 1994, 108 Stat. 4364.)

AMENDMENTS

1994—Par. (5). Pub. L. 103–424 amended par. (5) generally. Prior to amendment, par. (5) read as follows: ''meeting affirmative action goals and achievement of equal employment opportunity requirements.''

§ 4314. Ratings for performance appraisals

(a) Each performance appraisal system shall provide for annual summary ratings of levels of performance as follows:

(1) one or more fully successful levels,

(2) a minimally satisfactory level, and

(3) an unsatisfactory level.

(b) Each performance appraisal system shall provide that—

(1) any appraisal and any rating under such system—

(A) are made only after review and evaluation by a performance review board established under subsection (c) of this section;

(B) are conducted at least annually, subject to the limitation of subsection (c)(3) of this section;

(C) in the case of a career appointee, may not be made within 120 days after the beginning of a new Presidential administration; and

(D) are based on performance during a performance appraisal period the duration of which shall be determined under guidelines established by the Office of Personnel Management, but which may be terminated in any case in which the agency making an appraisal determines that an adequate basis exists on which to appraise and rate the senior executive's performance;

(2) any career appointee receiving a rating at any of the fully successful levels under subsection (a)(1) of this section may be given a performance award under section 5384 of this title;

(3) any senior executive receiving an unsatisfactory rating under subsection (a)(3) of this section shall be reassigned or transferred within the Senior Executive Service, or removed from the Senior Executive Service, but any senior executive who receives 2 unsatisfactory ratings in any period of 5 consecutive years shall be removed from the Senior Executive Service; and

(4) any senior executive who twice in any period of 3 consecutive years receives less than fully successful ratings shall be removed from the Senior Executive Service.

(c)(1) Each agency shall establish, in accordance with regulations prescribed by the Office, one or more performance review boards, as appropriate. It is the function of the boards to make recommendations to the appropriate appointing authority of the agency relating to the performance of senior executives in the agency.

(2) The supervising official of the senior executive shall provide to the performance review board, an initial appraisal of the senior executive's performance. Before making any recommendation with respect to the senior executive, the board shall review any response by the senior executive to the initial appraisal and conduct such further review as the board finds necessary.

(3) Performance appraisals under this subchapter with respect to any senior executive shall be made by the appointing authority only after considering the recommendations by the performance review board with respect to such senior executive under paragraph (1) of this subsection.

(4) Members of performance review boards shall be appointed in such a manner as to assure consistency, stability, and objectivity in performance appraisal. Notice of the appointment of an individual to serve as a member shall be published in the Federal Register.

(5) In the case of an appraisal of a career appointee, more than one-half of the members of the performance review board shall consist of career appointees. The requirement of the preceding sentence shall not apply in any case in which the Office determines that there exists an insufficient number of career appointees available to comply with the requirement.

(Added Pub. L. 95–454, title IV, § 405(a), Oct. 13, 1978, 92 Stat. 1169; amended Pub. L. 104–66, title II, § 2181(b), Dec. 21, 1995, 109 Stat. 732.)

AMENDMENTS

1995—Subsec. (d). Pub. L. 104–66 struck out subsec. (d) which related to reports to Congress.

§ 4315. Regulations

The Office of Personnel Management shall prescribe regulations to carry out the purpose of this subchapter.

(Added Pub. L. 95–454, title IV, § 405(a), Oct. 13, 1978, 92 Stat. 1170.)

CHAPTER 45—INCENTIVE AWARDS

SUBCHAPTER I—AWARDS FOR SUPERIOR ACCOMPLISHMENTS

[1] So in original. Probably should not be capitalized.

the performance of the functions of the Board.'' after first sentence, inserted ''or buildings'' after ''building'' wherever appearing in third and fourth sentences, and substituted ''constructed on any site'' for ''constructed on the site'' in third sentence.

1934—Act June 19, 1934, inserted provisions after ''the preceding half year'' in first sentence and inserted second and third sentences.

CHANGE OF NAME

Section 203(a) of act Aug. 23, 1935, changed name of Federal Reserve Board to Board of Governors of the Federal Reserve System.

§ 244. Principal offices of Board; chairman of Board; obligations and expenses; qualifications of members; vacancies

The principal offices of the Board shall be in the District of Columbia. At meetings of the Board the chairman shall preside, and, in his absence, the vice chairman shall preside. In the absence of the chairman and the vice chairman, the Board shall elect a member to act as chairman pro tempore. The Board shall determine and prescribe the manner in which its obligations shall be incurred and its disbursements and expenses allowed and paid, and may leave on deposit in the Federal Reserve banks the proceeds of assessments levied upon them to defray its estimated expenses and the salaries of its members and employees, whose employment, compensation, leave, and expenses shall be governed solely by the provisions of this chapter and rules and regulations of the Board not inconsistent therewith; and funds derived from such assessments shall not be construed to be Government funds or appropriated moneys. No member of the Board of Governors of the Federal Reserve System shall be an officer or director of any bank, banking institution, trust company, or Federal Reserve bank or hold stock in any bank, banking institution, or trust company; and before entering upon his duties as a member of the Board of Governors of the Federal Reserve System he shall certify under oath that he has complied with this requirement, and such certification shall be filed with the secretary of the Board. Whenever a vacancy shall occur, other than by expiration of term, among the seven members of the Board of Governors of the Federal Reserve System appointed by the President as above provided, a successor shall be appointed by the President, by and with the advice and consent of the Senate, to fill such vacancy, and when appointed he shall hold office for the unexpired term of his predecessor.

(Dec. 23, 1913, ch. 6, § 10 (par.), 38 Stat. 261; June 3, 1922, ch. 205, 42 Stat. 621; June 16, 1933, ch. 89, § 6(b), 48 Stat. 167; Aug. 23, 1935, ch. 614, title II, § 203(a)–(c), 49 Stat. 704, 705.)

REFERENCES IN TEXT

This chapter, referred to in text, was in the original ''this Act, specific amendments thereof'', meaning act Dec. 23, 1913, ch. 6, 38 Stat. 251, as amended, known as the Federal Reserve Act. For complete classification of this Act to the Code, see References in Text note set out under section 226 of this title and Tables.

CODIFICATION

Section is comprised of fourth par. of section 10 of act Dec. 23, 1913. For classification to this title of other pars. of section 10, see Codification note set out under section 241 of this title.

Word ''seven'' was substituted for ''six'' in last sentence on authority of section 203(b) of act Aug. 23, 1935, which increased membership of the Board of Governors.

AMENDMENTS

1935—Act Aug. 23, 1935, § 203(c), substituted second and third sentences for former related provisions.

1933—Act June 16, 1933, fixed the principal offices of the Board, made the Secretary of the Treasury chairman, provided for chairman pro tempore, and referred to disbursements, obligations, salaries and leaves.

CHANGE OF NAME

Section 203(a) of act Aug. 23, 1935, changed name of Federal Reserve Board to Board of Governors of the Federal Reserve System.

§ 245. Vacancies during recess of Senate

The President shall have power to fill all vacancies that may happen on the Board of Governors of the Federal Reserve System during the recess of the Senate by granting commissions which shall expire with the next session of the Senate.

(Dec. 23, 1913, ch. 6, § 10 (par.), 38 Stat. 260; June 3, 1922, ch. 205, 42 Stat. 620; Aug. 23, 1935, ch. 614, title II, § 203(a), 49, Stat. 704.)

CODIFICATION

Section is comprised of fifth par. of section 10 of act Dec. 23, 1913. For classification to this title of other pars. of section 10, see Codification note set out under section 241 of this title.

CHANGE OF NAME

Section 203(a) of act Aug. 23, 1935, changed name of Federal Reserve Board to Board of Governors of the Federal Reserve System.

§ 246. Powers of Secretary of the Treasury as affected by chapter

Nothing in this chapter contained shall be construed as taking away any powers heretofore vested by law in the Secretary of the Treasury which relate to the supervision, management, and control of the Treasury Department and bureaus under such department, and wherever any power vested by this chapter in the Board of Governors of the Federal Reserve System or the Federal reserve agent appears to conflict with the powers of the Secretary of the Treasury, such powers shall be exercised subject to the supervision and control of the Secretary.

(Dec. 23, 1913, ch. 6, § 10 (par.), 38 Stat. 261; June 3, 1922, ch. 205, 42 Stat. 621; Aug. 23, 1935, ch. 614, title II, § 203(a), 49 Stat. 704.)

REFERENCES IN TEXT

This chapter, referred to in text, was in the original ''this Act'', meaning act Dec. 23, 1913, ch. 6, 38 Stat. 251, as amended, known as the Federal Reserve Act. For complete classification of this Act to the Code, see References in Text note set out under section 226 of this title and Tables.

CODIFICATION

Section is comprised of sixth par. of section 10 of act Dec. 23, 1913. For classification to this title of other pars. of section 10, see Codification note set out under section 241 of this title.

12 U.S. Code § 248 - Enumerated powers

Current through Pub. L. 113-121. (See Public Laws for the current Congress.)

US Code Notes Updates Authorities (CFR)

The Board of Governors of the Federal Reserve System shall be authorized and empowered:

(a) Examination of accounts and affairs of banks; publication of weekly statements; reports of liabilities and assets of depository institutions; covered institutions

(1)To examine at its discretion the accounts, books, and affairs of each Federal reserve bank and of each member bank and to require such statements and reports as it may deem necessary. The said board shall publish once each week a statement showing the condition of each Federal reserve bank and a consolidated statement for all Federal reserve banks. Such statements shall show in detail the assets and liabilities of the Federal reserve banks, single and combined, and shall furnish full information regarding the character of the money held as reserve and the amount, nature, and maturities of the paper and other investments owned or held by Federal reserve banks.

(2)To require any depository institution specified in this paragraph to make, at such intervals as the Board may prescribe, such reports of its liabilities and assets as the Board may determine to be necessary or desirable to enable the Board to discharge its responsibility to monitor and control monetary and credit aggregates. Such reports shall be made

(A) directly to the Board in the case of member banks and in the case of other depository institutions whose reserve requirements under sections 461, 463, 464, 465, and 466 of this title exceed zero, and

(B) for all other reports to the Board through the

(i) Federal Deposit Insurance Corporation in the case of insured State savings associations that are insured depository institutions (as defined in section 1813 of this title), State nonmember banks, savings banks, and mutual savings banks,

(ii) National Credit Union Administration Board in the case of insured credit unions,

(iii) the Comptroller of the Currency in the case of any Federal savings association which is an insured depository institution (as defined in section 1813 of this title) or which is a member as defined in section 1422 of this title, and

(iv) such State officer or agency as the Board may designate in the case of any other type of bank, savings association, or credit union. The Board shall endeavor to avoid the imposition of unnecessary burdens on reporting institutions and the duplication of other reporting requirements. Except as otherwise required by law, any data provided to any department, agency, or instrumentality of the United States pursuant to other reporting requirements shall be made available to the Board. The Board may classify depository institutions for the purposes of this paragraph and may impose different requirements on each such class.

(b) Permitting or requiring rediscounting of paper at specified rate

All lawyers

To permit, or, on the affirmative vote of at least five members of the Board of Governors, to require Federal reserve banks to rediscount the discounted paper of other Federal reserve banks at rates of interest to be fixed by the Board.

(c) Suspending reserve requirements

To suspend for a period not exceeding thirty days, and from time to time to renew such suspension for periods not exceeding fifteen days, any reserve requirements specified in this chapter.

(d) Supervising and regulating issue and retirement of notes

To supervise and regulate through the Secretary of the Treasury the issue and retirement of Federal Reserve notes, except for the cancellation and destruction, and accounting with respect to such cancellation and destruction, of notes unfit for circulation, and to prescribe rules and regulations under which such notes may be delivered by the Secretary of the Treasury to the Federal Reserve agents applying therefor.

(e) Adding to or reclassifying reserve cities

To add to the number of cities classified as reserve cities under existing law in which national banking associations are subject to the reserve requirements set forth in section 20 of this Act, or to reclassify existing reserve cities or to terminate their designation as such.

(f) Suspending or removing officers or directors of reserve banks

To suspend or remove any officer or director of any Federal reserve bank, the cause of such removal to be forthwith communicated in writing by the Board of Governors of the Federal Reserve System to the removed officer or director and to said bank.

(g) Requiring writing off of doubtful or worthless assets of banks

To require the writing off of doubtful or worthless assets upon the books and balance sheets of Federal reserve banks.

(h) Suspending operations of or liquidating or reorganizing banks

To suspend, for the violation of any of the provisions of this chapter, the operations of any Federal reserve bank, to take possession thereof, administer the same during the period of suspension, and, when deemed advisable, to liquidate or reorganize such bank.

(i) Requiring bonds of agents; safeguarding property in hands of agents

To require bonds of Federal reserve agents, to make regulations for the safeguarding of all collateral, bonds, Federal reserve notes, money, or property of any kind deposited in the hands of such agents, and said board shall perform the duties, functions, or services specified in this chapter, and make all rules and regulations necessary to enable said board effectively to perform the same.

(j) Exercising supervision over reserve banks

To exercise general supervision over said Federal reserve banks.

(k) Delegation of certain functions; power to delegate; review of delegated activities

To delegate, by published order or rule and subject to subchapter II of chapter 5, and chapter 7, of title 5, any of its functions, other than those relating to rulemaking or pertaining principally to monetary and credit policies, to one or more administrative law judges, members or employees of the Board, or Federal Reserve banks. The assignment of responsibility for the performance of any function that the Board determines to delegate shall be a function of the Chairman. The Board shall, upon the vote of one member, review action taken at a delegated level within such time and in such manner as the Board shall by rule prescribe. The Board of Governors may not delegate to a Federal reserve bank its functions for the establishment of policies for the supervision and regulation of depository institution holding companies and other financial firms supervised by the Board of Governors.

(l) Employing attorneys, experts, assistants, and clerks; salaries and fees

To employ such attorneys, experts, assistants, clerks, or other employees as may be deemed necessary to conduct the business of the board. All salaries and fees shall be

fixed in advance by said board and shall be paid in the same manner as the salaries of the members of said board. All such attorneys, experts, assistants, clerks, and other employees shall be appointed without regard to the provisions of the Act of January sixteenth, eighteen hundred and eighty-three (volume twenty-two, United States Statutes at Large, page four hundred and three), and amendments thereto, or any rule or regulation made in pursuance thereof: Provided, That nothing herein shall prevent the President from placing said employees in the classified service.

(m) [Repealed]

(n) Board's authority to examine depository institutions and affiliates

To examine, at the Board's discretion, any depository institution, and any affiliate of such depository institution, in connection with any advance to, any discount of any instrument for, or any request for any such advance or discount by, such depository institution under this chapter.

(o) Authority to appoint conservator or receiver

The Board may appoint the Federal Deposit Insurance Corporation as conservator or receiver for a State member bank under section 1821(c)(9) of this title.

(p) Authority

The Board may act in its own name and through its own attorneys in enforcing any provision of this title,[1] regulations promulgated hereunder, or any other law or regulation, or in any action, suit, or proceeding to which the Board is a party and which involves the Board's regulation or supervision of any bank, bank holding company (as defined in section 1841 of this title), or other entity, or the administration of its operations.

(q) Uniform protection authority for Federal reserve facilities

(1)Notwithstanding any other provision of law, to authorize personnel to act as law enforcement officers to protect and safeguard the premises, grounds, property, personnel, including members of the Board, of the Board, or any Federal reserve bank, and operations conducted by or on behalf of the Board or a reserve bank.

(2)The Board may, subject to the regulations prescribed under paragraph (5), delegate authority to a Federal reserve bank to authorize personnel to act as law enforcement officers to protect and safeguard the bank's premises, grounds, property, personnel, and operations conducted by or on behalf of the bank.

(3)Law enforcement officers designated or authorized by the Board or a reserve bank under paragraph (1) or (2) are authorized while on duty to carry firearms and make arrests without warrants for any offense against the United States committed in their presence, or for any felony cognizable under the laws of the United States committed or being committed within the buildings and grounds of the Board or a reserve bank if they have reasonable grounds to believe that the person to be arrested has committed or is committing such a felony. Such officers shall have access to law enforcement information that may be necessary for the protection of the property or personnel of the Board or a reserve bank.

(4)For purposes of this subsection, the term "law enforcement officers" means personnel who have successfully completed law enforcement training and are authorized to carry firearms and make arrests pursuant to this subsection.

(5)The law enforcement authorities provided for in this subsection may be exercised only pursuant to regulations prescribed by the Board and approved by the Attorney General.

(r) Voting; documentation of determinations

(1)Any action that this chapter provides may be taken only upon the affirmative vote of 5 members of the Board may be taken upon the unanimous vote of all members then in office if there are fewer than 5 members in office at the time of the action.

(2)

(A)Any action that the Board is otherwise authorized to take under section 343(3) of this title may be taken upon the unanimous vote of all available members then in office, if—

(i)at least 2 members are available and all available members participate in the action;

(ii)the available members unanimously determine that—

(I)unusual and exigent circumstances exist and the borrower is unable to secure adequate credit accommodations from other sources;

(II)action on the matter is necessary to prevent, correct, or mitigate serious harm to the economy or the stability of the financial system of the United States;

(III)despite the use of all means available (including all available telephonic, telegraphic, and other electronic means), the other members of the Board have not been able to be contacted on the matter; and

(IV)action on the matter is required before the number of Board members otherwise required to vote on the matter can be contacted through any available means (including all available telephonic, telegraphic, and other electronic means); and

(iii)any credit extended by a Federal reserve bank pursuant to such action is payable upon demand of the Board.

(B)The available members of the Board shall document in writing the determinations required by subparagraph (A)(ii), and such written findings shall be included in the record of the action and in the official minutes of the Board, and copies of such record shall be provided as soon as practicable to the members of the Board who were not available to participate in the action and to the Chairman of the Committee on Banking, Housing, and Urban Affairs of the Senate and to the Chairman of the Committee on Financial Services of the House of Representatives.

(s) 2 Federal Reserve transparency and release of information

(1) In general

In order to ensure the disclosure in a timely manner consistent with the purposes of this chapter of information concerning the borrowers and counterparties participating in emergency credit facilities, discount window lending programs, and open market operations authorized or conducted by the Board or a Federal reserve bank, the Board of Governors shall disclose, as provided in paragraph (2)—

(A)the names and identifying details of each borrower, participant, or counterparty in any credit facility or covered transaction;

(B)the amount borrowed by or transferred by or to a specific borrower, participant, or counterparty in any credit facility or covered transaction;

(C)the interest rate or discount paid by each borrower, participant, or counterparty in any credit facility or covered transaction; and

(D)information identifying the types and amounts of collateral pledged or assets transferred in connection with participation in any credit facility or covered transaction.

(2) Mandatory release date

In the case of—

(A)a credit facility, the Board shall disclose the information described in paragraph (1) on the date that is 1 year after the effective date of the termination by the Board of the authorization of the credit facility; and

(B)a covered transaction, the Board shall disclose the information described in paragraph (1) on the last day of the eighth calendar quarter following the calendar quarter in which the covered transaction was conducted.

(3) Earlier release date authorized

The Chairman of the Board may publicly release the information described in paragraph (1) before the relevant date specified in paragraph (2), if the Chairman determines that such disclosure would be in the public interest and would not harm the effectiveness of the relevant credit facility or the purpose or conduct of covered transactions.

(4) Definitions

For purposes of this subsection, the following definitions shall apply:

(A) Credit facility

The term "credit facility" has the same meaning as in section 714(f)(1)(A) of title 31.

(B) Covered transaction

The term "covered transaction" means—

(i)any open market transaction with a nongovernmental third party conducted under section 353 of this title or section 354, 355, or 356 of this title, after July 21, 2010; and

(ii)any advance made under section 347b of this title after July 21, 2010.

(5) Termination of credit facility by operation of law

A credit facility shall be deemed to have terminated as of the end of the 24-month period beginning on the date on which the credit facility ceases to make extensions of credit and loans, unless the credit facility is otherwise terminated by the Board before such date.

(6) Consistent treatment of information

Except as provided in this subsection or section 343(3)(D) of this title, or in section 714(f)(3)(C) of title 31, the information described in paragraph (1) and information concerning the transactions described in section 714(f) of such title, shall be confidential, including for purposes of section 552(b)(3) of title 5, until the relevant mandatory release date described in paragraph (2), unless the Chairman of the Board determines that earlier disclosure of such information would be in the public interest and would not harm the effectiveness of the relevant credit facility or the purpose of conduct of the relevant transactions.

(7) Protection of personal privacy

This subsection and section 343(3)(C) of this title, section 714(f)(3)(C) of title 31, and subsection (a) or (c) ofsection 1109 of the Dodd-Frank Wall Street Reform and Consumer Protection Act shall not be construed as requiring any disclosure of nonpublic personal information (as defined for purposes of section 6802 of title 15) concerning any individual who is referenced in collateral pledged or assets transferred in connection with a credit facility or covered transaction, unless the person is a borrower, participant, or counterparty under the credit facility or covered transaction.

(8) Study of FOIA exemption impact

(A) Study

The Inspector General of the Board of Governors of the Federal Reserve System shall—

(i)conduct a study on the impact that the exemption from section 552(b)(3) of title 5 (known as the Freedom of Information Act) established under paragraph (6) has had on the ability of the public to access information about the administration by the Board of Governors of emergency credit facilities, discount window lending programs, and open market operations; and

(ii)make any recommendations on whether the exemption described in clause (i) should remain in effect.

(B) Report

Not later than 30 months after July 21, 2010, the Inspector General of the Board of Governors of the Federal Reserve System shall submit a report on the findings of the study required under subparagraph (A) to the Committee on Banking, Housing, and Urban Affairs of the Senate and the Committee on Financial Services of the House of Representatives, and publish the report on the website of the Board.

(9) Rule of construction

Nothing in this section is meant to affect any pending litigation or lawsuit filed under section 552 of title 5 (popularly known as the Freedom of Information Act) on or before July 21, 2010.

(s) 2 Assessments, fees, and other charges for certain companies

(1) In general

The Board shall collect a total amount of assessments, fees, or other charges from the companies described in paragraph (2) that is equal to the total expenses the Board estimates are necessary or appropriate to carry out the supervisory and regulatory responsibilities of the Board with respect to such companies.

(2) Companies

The companies described in this paragraph are—

(A)all bank holding companies having total consolidated assets of $50,000,000,000 or more;

(B)all savings and loan holding companies having total consolidated assets of $50,000,000,000 or more; and

(C)all nonbank financial companies supervised by the Board under section 5323 of this title.

---

[1] See References in Text note below.

[2] So in original. Two subsecs. (s) have been enacted.

12 U.S. Code § 244 - Principal offices of Board; chairman of Board; obligations and expenses; qualifications of members; vacancies

Current through Pub. L. 113-121. (See Public Laws for the current Congress.)

US Code Notes Updates Authorities (CFR)

The principal offices of the Board shall be in the District of Columbia. At meetings of the Board the chairman shall preside, and, in his absence, the vice chairman shall preside. In the absence of the chairman and the vice chairman, the Board shall elect a member to act as chairman pro tempore. The Board shall determine and prescribe the manner in which its obligations shall be incurred and its disbursements and expenses allowed and paid, and may leave on deposit in the Federal Reserve banks the proceeds of assessments levied upon them to defray its estimated expenses and the salaries of its members and employees, whose employment, compensation, leave, and expenses shall be governed solely by the provisions of this chapter and rules and regulations of the Board not inconsistent therewith; and funds derived from such assessments shall not be construed to be Government funds or appropriated moneys. No member of the Board of Governors of the Federal Reserve System shall be an officer or director of any bank, banking institution, trust company, or Federal Reserve bank or hold stock in any bank, banking institution, or trust company; and before entering upon his duties as a member of the Board of Governors of the Federal Reserve System he shall certify under oath that he has complied with this requirement, and such certification shall be filed with the secretary of the Board. Whenever a vacancy shall occur, other than by expiration of term, among the seven members of the Board of Governors of the Federal Reserve System appointed by the President as above provided, a successor shall be appointed by the President, by and with the advice and consent of the Senate, to fill such vacancy, and when appointed he shall hold office for the unexpired term of his predecessor.

CHANGE OF NAME

Section 203(a) of act Aug. 23, 1935, changed name of Federal Reserve Board to Board of Governors of the Federal Reserve System.

§ 247. Reports to Congress

The Board of Governors of the Federal Reserve System shall annually make a full report of its operations to the Speaker of the House of Representatives, who shall cause the same to be printed for the information of the Congress. The report required under this paragraph shall include the reports required under section 1691f of title 15, section 57a(f)(7)[1] of title 15, section 1613 of title 15, and section 247a of this title.

(Dec. 23, 1913, ch. 6, §10 (par.), 38 Stat. 261; June 3, 1922, ch. 205, 42 Stat. 621; Aug. 23, 1935, ch. 614, title II, §203(a), 49 Stat. 704; Pub. L. 106–569, title XI, §1103(b), Dec. 27, 2000, 114 Stat. 3030.)

REFERENCES IN TEXT

Section 57a(f)(7) of title 15, referred to in text, was repealed by Pub. L. 111–203, title X, §1092(3), July 21, 2010, 124 Stat. 2095.

CODIFICATION

Section is comprised of seventh par. of section 10 of act Dec. 23, 1913. For classification to this title of other pars. of section 10, see Codification note set out under section 241 of this title.

AMENDMENTS

2000—Pub. L. 106–569 inserted at end ''The report required under this paragraph shall include the reports required under section 1691f of title 15, section 57a(f)(7) of title 15, section 1613 of title 15, and section 247a of this title.''

CHANGE OF NAME

Section 203(a) of act Aug. 23, 1935, changed name of Federal Reserve Board to Board of Governors of the Federal Reserve System.

MEMBERSHIP OF INTERNATIONAL BANKS IN FEDERAL RESERVE SYSTEM; REPORT TO CONGRESS

Pub. L. 95–369, §3(g), Sept. 17, 1978, 92 Stat. 610, provided that the Board report to Congress not later than 270 days after Sept. 17, 1978 recommendations with respect to permitting corporations organized or operating under section 25 or 25(a) of the Federal Reserve Act to become members of Federal Reserve Banks.

EFFECT OF INTERNATIONAL BANKING ACT OF 1978 ON INTERNATIONAL BANKS; REPORT TO CONGRESS

Pub. L. 95–369, §3(h), Sept. 17, 1978, 92 Stat. 610, provided that: ''As part of its annual report pursuant to section 10 of the Federal Reserve Act [this section], the Board shall include its assessment of the effects of the amendments made by this Act [see Short Title note set out under section 3101 of this title] on the capitalization and activities of corporations organized or operating under section 25 or 25(a) of the Federal Reserve Act [sections 601 to 604 and 611 to 631 of this title], and on commercial banks and the banking system.''

§ 247a. Records of action on policy relating to open-market operation and policies determined generally; inclusion in report to Congress

The Board of Governors of the Federal Reserve System shall keep a complete record of the action taken by the Board and by the Federal Open Market Committee upon all questions of policy relating to open-market operations and shall record therein the votes taken in connection with the determination of open-market policies and the reasons underlying the action of the Board and the Committee in each instance. The Board shall keep a similar record with respect to all questions of policy determined by the Board, and shall include in its annual report to the Congress a full account of the action so taken during the preceding year with respect to open-market policies and operations and with respect to the policies determined by it and shall include in such report a copy of the records required to be kept under the provisions of this section.

(Dec. 23, 1913, ch. 6, §10 (par.), as added Aug. 23, 1935, ch. 614, title II, §203(d), 49 Stat. 705.)

CODIFICATION

Section is comprised of tenth par. of section 10 of act Dec. 23, 1913, as added Aug. 23, 1935. For classification to this title of other pars. of section 10, see Codification note set out under section 241 of this title.

§ 247b. Appearances before Congress

The Vice Chairman for Supervision shall appear before the Committee on Banking, Housing, and Urban Affairs of the Senate and the Committee on Financial Services of the House of Representatives and at semi-annual hearings regarding the efforts, activities, objectives, and plans of the Board with respect to the conduct of supervision and regulation of depository institution holding companies and other financial firms supervised by the Board.

(Dec. 23, 1913, ch. 6, §10(12), as added Pub. L. 111–203, title XI, §1108(b), July 21, 2010, 124 Stat. 2126.)

CODIFICATION

Section is comprised of par. (12) of section 10 of act Dec. 23, 1913. No par. between pars. (10) and (12) has been enacted. For classification to this title of other pars. of section 10, see Codification note set out under section 241 of this title.

EFFECTIVE DATE

Section effective 1 day after July 21, 2010, except as otherwise provided, see section 4 of Pub. L. 111–203, set out as a note under section 5301 of this title.

§ 248. Enumerated powers

The Board of Governors of the Federal Reserve System shall be authorized and empowered:

(a) Examination of accounts and affairs of banks; publication of weekly statements; reports of liabilities and assets of depository institutions; covered institutions

(1) To examine at its discretion the accounts, books, and affairs of each Federal reserve bank and of each member bank and to require such statements and reports as it may deem necessary. The said board shall publish once each week a statement showing the condition of each Federal reserve bank and a consolidated statement for all Federal reserve banks. Such statements shall show in detail the assets and liabilities of the Federal reserve banks, single and

[1] See References in Text note below.

combined, and shall furnish full information regarding the character of the money held as reserve and the amount, nature, and maturities of the paper and other investments owned or held by Federal reserve banks.

(2) To require any depository institution specified in this paragraph to make, at such intervals as the Board may prescribe, such reports of its liabilities and assets as the Board may determine to be necessary or desirable to enable the Board to discharge its responsibility to monitor and control monetary and credit aggregates. Such reports shall be made (A) directly to the Board in the case of member banks and in the case of other depository institutions whose reserve requirements under sections 461, 463, 464, 465, and 466 of this title exceed zero, and (B) for all other reports to the Board through the (i) Federal Deposit Insurance Corporation in the case of insured State savings associations that are insured depository institutions (as defined in section 1813 of this title), State nonmember banks, savings banks, and mutual savings banks, (ii) National Credit Union Administration Board in the case of insured credit unions, (iii) the Comptroller of the Currency in the case of any Federal savings association which is an insured depository institution (as defined in section 1813 of this title) or which is a member as defined in section 1422 of this title, and (iv) such State officer or agency as the Board may designate in the case of any other type of bank, savings association, or credit union. The Board shall endeavor to avoid the imposition of unnecessary burdens on reporting institutions and the duplication of other reporting requirements. Except as otherwise required by law, any data provided to any department, agency, or instrumentality of the United States pursuant to other reporting requirements shall be made available to the Board. The Board may classify depository institutions for the purposes of this paragraph and may impose different requirements on each such class.

(b) Permitting or requiring rediscounting of paper at specified rate

To permit, or, on the affirmative vote of at least five members of the Board of Governors, to require Federal reserve banks to rediscount the discounted paper of other Federal reserve banks at rates of interest to be fixed by the Board.

(c) Suspending reserve requirements

To suspend for a period not exceeding thirty days, and from time to time to renew such suspension for periods not exceeding fifteen days, any reserve requirements specified in this chapter.

(d) Supervising and regulating issue and retirement of notes

To supervise and regulate through the Secretary of the Treasury the issue and retirement of Federal Reserve notes, except for the cancellation and destruction, and accounting with respect to such cancellation and destruction, of notes unfit for circulation, and to prescribe rules and regulations under which such notes may be delivered by the Secretary of the Treasury to the Federal Reserve agents applying therefor.

(e) Adding to or reclassifying reserve cities

To add to the number of cities classified as reserve cities under existing law in which national banking associations are subject to the reserve requirements set forth in section 20 of this Act, or to reclassify existing reserve cities or to terminate their designation as such.

(f) Suspending or removing officers or directors of reserve banks

To suspend or remove any officer or director of any Federal reserve bank, the cause of such removal to be forthwith communicated in writing by the Board of Governors of the Federal Reserve System to the removed officer or director and to said bank.

(g) Requiring writing off of doubtful or worthless assets of banks

To require the writing off of doubtful or worthless assets upon the books and balance sheets of Federal reserve banks.

(h) Suspending operations of or liquidating or reorganizing banks

To suspend, for the violation of any of the provisions of this chapter, the operations of any Federal reserve bank, to take possession thereof, administer the same during the period of suspension, and, when deemed advisable, to liquidate or reorganize such bank.

(i) Requiring bonds of agents; safeguarding property in hands of agents

To require bonds of Federal reserve agents, to make regulations for the safeguarding of all collateral, bonds, Federal reserve notes, money, or property of any kind deposited in the hands of such agents, and said board shall perform the duties, functions, or services specified in this chapter, and make all rules and regulations necessary to enable said board effectively to perform the same.

(j) Exercising supervision over reserve banks

To exercise general supervision over said Federal reserve banks.

(k) Delegation of certain functions; power to delegate; review of delegated activities

To delegate, by published order or rule and subject to subchapter II of chapter 5, and chapter 7, of title 5, any of its functions, other than those relating to rulemaking or pertaining principally to monetary and credit policies, to one or more administrative law judges, members or employees of the Board, or Federal Reserve banks. The assignment of responsibility for the performance of any function that the Board determines to delegate shall be a function of the Chairman. The Board shall, upon the vote of one member, review action taken at a delegated level within such time and in such manner as the Board shall by rule prescribe. The Board of Governors may not delegate to a Federal reserve bank its functions for the establishment of policies for the supervision and regulation of depository institution holding companies and other financial firms supervised by the Board of Governors.

(*l*) Employing attorneys, experts, assistants, and clerks; salaries and fees

To employ such attorneys, experts, assistants, clerks, or other employees as may be deemed

necessary to conduct the business of the board. All salaries and fees shall be fixed in advance by said board and shall be paid in the same manner as the salaries of the members of said board. All such attorneys, experts, assistants, clerks, and other employees shall be appointed without regard to the provisions of the Act of January sixteenth, eighteen hundred and eighty-three (volume twenty-two, United States Statutes at Large, page four hundred and three), and amendments thereto, or any rule or regulation made in pursuance thereof: *Provided*, That nothing herein shall prevent the President from placing said employees in the classified service.

(m) [Repealed]

(n) Board's authority to examine depository institutions and affiliates

To examine, at the Board's discretion, any depository institution, and any affiliate of such depository institution, in connection with any advance to, any discount of any instrument for, or any request for any such advance or discount by, such depository institution under this chapter.

(*o*) Authority to appoint conservator or receiver

The Board may appoint the Federal Deposit Insurance Corporation as conservator or receiver for a State member bank under section 1821(c)(9) of this title.

(p) Authority

The Board may act in its own name and through its own attorneys in enforcing any provision of this title,[1] regulations promulgated hereunder, or any other law or regulation, or in any action, suit, or proceeding to which the Board is a party and which involves the Board's regulation or supervision of any bank, bank holding company (as defined in section 1841 of this title), or other entity, or the administration of its operations.

(q) Uniform protection authority for Federal reserve facilities

(1) Notwithstanding any other provision of law, to authorize personnel to act as law enforcement officers to protect and safeguard the premises, grounds, property, personnel, including members of the Board, of the Board, or any Federal reserve bank, and operations conducted by or on behalf of the Board or a reserve bank.

(2) The Board may, subject to the regulations prescribed under paragraph (5), delegate authority to a Federal reserve bank to authorize personnel to act as law enforcement officers to protect and safeguard the bank's premises, grounds, property, personnel, and operations conducted by or on behalf of the bank.

(3) Law enforcement officers designated or authorized by the Board or a reserve bank under paragraph (1) or (2) are authorized while on duty to carry firearms and make arrests without warrants for any offense against the United States committed in their presence, or for any felony cognizable under the laws of the United States committed or being committed within the buildings and grounds of the Board or a reserve bank if they have reasonable grounds to believe that the person to be arrested has committed or is committing such a felony. Such officers shall have access to law enforcement information that may be necessary for the protection of the property or personnel of the Board or a reserve bank.

(4) For purposes of this subsection, the term ''law enforcement officers'' means personnel who have successfully completed law enforcement training and are authorized to carry firearms and make arrests pursuant to this subsection.

(5) The law enforcement authorities provided for in this subsection may be exercised only pursuant to regulations prescribed by the Board and approved by the Attorney General.

(r) Voting; documentation of determinations

(1) Any action that this chapter provides may be taken only upon the affirmative vote of 5 members of the Board may be taken upon the unanimous vote of all members then in office if there are fewer than 5 members in office at the time of the action.

(2)(A) Any action that the Board is otherwise authorized to take under section 343(3) of this title may be taken upon the unanimous vote of all available members then in office, if—

(i) at least 2 members are available and all available members participate in the action;

(ii) the available members unanimously determine that—

(I) unusual and exigent circumstances exist and the borrower is unable to secure adequate credit accommodations from other sources;

(II) action on the matter is necessary to prevent, correct, or mitigate serious harm to the economy or the stability of the financial system of the United States;

(III) despite the use of all means available (including all available telephonic, telegraphic, and other electronic means), the other members of the Board have not been able to be contacted on the matter; and

(IV) action on the matter is required before the number of Board members otherwise required to vote on the matter can be contacted through any available means (including all available telephonic, telegraphic, and other electronic means); and

(iii) any credit extended by a Federal reserve bank pursuant to such action is payable upon demand of the Board.

(B) The available members of the Board shall document in writing the determinations required by subparagraph (A)(ii), and such written findings shall be included in the record of the action and in the official minutes of the Board, and copies of such record shall be provided as soon as practicable to the members of the Board who were not available to participate in the action and to the Chairman of the Committee on Banking, Housing, and Urban Affairs of the Senate and to the Chairman of the Committee on Financial Services of the House of Representatives.

[1] See References in Text note below.

(s)[2] Federal Reserve transparency and release of information

(1) In general

In order to ensure the disclosure in a timely manner consistent with the purposes of this chapter of information concerning the borrowers and counterparties participating in emergency credit facilities, discount window lending programs, and open market operations authorized or conducted by the Board or a Federal reserve bank, the Board of Governors shall disclose, as provided in paragraph (2)—

(A) the names and identifying details of each borrower, participant, or counterparty in any credit facility or covered transaction;

(B) the amount borrowed by or transferred by or to a specific borrower, participant, or counterparty in any credit facility or covered transaction;

(C) the interest rate or discount paid by each borrower, participant, or counterparty in any credit facility or covered transaction; and

(D) information identifying the types and amounts of collateral pledged or assets transferred in connection with participation in any credit facility or covered transaction.

(2) Mandatory release date

In the case of—

(A) a credit facility, the Board shall disclose the information described in paragraph (1) on the date that is 1 year after the effective date of the termination by the Board of the authorization of the credit facility; and

(B) a covered transaction, the Board shall disclose the information described in paragraph (1) on the last day of the eighth calendar quarter following the calendar quarter in which the covered transaction was conducted.

(3) Earlier release date authorized

The Chairman of the Board may publicly release the information described in paragraph (1) before the relevant date specified in paragraph (2), if the Chairman determines that such disclosure would be in the public interest and would not harm the effectiveness of the relevant credit facility or the purpose or conduct of covered transactions.

(4) Definitions

For purposes of this subsection, the following definitions shall apply:

(A) Credit facility

The term ''credit facility'' has the same meaning as in section 714(f)(1)(A) of title 31.

(B) Covered transaction

The term ''covered transaction'' means—

(i) any open market transaction with a nongovernmental third party conducted under section 353 of this title or section 354, 355, or 356 of this title, after July 21, 2010; and

(ii) any advance made under section 347b of this title after July 21, 2010.

(5) Termination of credit facility by operation of law

A credit facility shall be deemed to have terminated as of the end of the 24-month period beginning on the date on which the credit facility ceases to make extensions of credit and loans, unless the credit facility is otherwise terminated by the Board before such date.

(6) Consistent treatment of information

Except as provided in this subsection or section 343(3)(D) of this title, or in section 714(f)(3)(C) of title 31, the information described in paragraph (1) and information concerning the transactions described in section 714(f) of such title, shall be confidential, including for purposes of section 552(b)(3) of title 5, until the relevant mandatory release date described in paragraph (2), unless the Chairman of the Board determines that earlier disclosure of such information would be in the public interest and would not harm the effectiveness of the relevant credit facility or the purpose of conduct of the relevant transactions.

(7) Protection of personal privacy

This subsection and section 343(3)(C) of this title, section 714(f)(3)(C) of title 31, and subsection (a) or (c) of section 1109 of the Dodd-Frank Wall Street Reform and Consumer Protection Act shall not be construed as requiring any disclosure of nonpublic personal information (as defined for purposes of section 6802 of title 15) concerning any individual who is referenced in collateral pledged or assets transferred in connection with a credit facility or covered transaction, unless the person is a borrower, participant, or counterparty under the credit facility or covered transaction.

(8) Study of FOIA exemption impact

(A) Study

The Inspector General of the Board of Governors of the Federal Reserve System shall—

(i) conduct a study on the impact that the exemption from section 552(b)(3) of title 5 (known as the Freedom of Information Act) established under paragraph (6) has had on the ability of the public to access information about the administration by the Board of Governors of emergency credit facilities, discount window lending programs, and open market operations; and

(ii) make any recommendations on whether the exemption described in clause (i) should remain in effect.

(B) Report

Not later than 30 months after July 21, 2010, the Inspector General of the Board of Governors of the Federal Reserve System shall submit a report on the findings of the study required under subparagraph (A) to the Committee on Banking, Housing, and Urban Affairs of the Senate and the Committee on Financial Services of the House of Representatives, and publish the report on the website of the Board.

(9) Rule of construction

Nothing in this section is meant to affect any pending litigation or lawsuit filed under

[2] So in original. Two subsecs. (s) have been enacted.

section 552 of title 5 (popularly known as the Freedom of Information Act) on or before July 21, 2010.

(s)[2] Assessments, fees, and other charges for certain companies

(1) In general

The Board shall collect a total amount of assessments, fees, or other charges from the companies described in paragraph (2) that is equal to the total expenses the Board estimates are necessary or appropriate to carry out the supervisory and regulatory responsibilities of the Board with respect to such companies.

(2) Companies

The companies described in this paragraph are—

(A) all bank holding companies having total consolidated assets of $50,000,000,000 or more;

(B) all savings and loan holding companies having total consolidated assets of $50,000,000,000 or more; and

(C) all nonbank financial companies supervised by the Board under section 5323 of this title.

(Dec. 23, 1913, ch. 6, §11, 38 Stat. 261; Sept. 7, 1916, ch. 461, 39 Stat. 752; Sept. 26, 1918, ch. 177, §2, 40 Stat. 968; Mar. 3, 1919, ch. 101, §3, 40 Stat. 1315; Feb. 27, 1921, ch. 75, 41 Stat. 1146; June 26, 1930, ch. 612, 46 Stat. 814; Mar. 9, 1933, ch. 1, title I, §3, 48 Stat. 2; June 16, 1933, ch. 89, §7, 48 Stat. 167; Aug. 23, 1935, ch. 614, title II, §203(a), title III, §§321(a), 342, 49 Stat. 704, 713, 722; June 12, 1945, ch. 186, §1(c), 59 Stat. 237; Pub. L. 86–114, §3(b)(6), July 28, 1959, 73 Stat. 264; Pub. L. 86–251, §3(c), Sept. 9, 1959, 73 Stat. 488; Pub. L. 87–722, §3, Sept. 28, 1962, 76 Stat. 670; Pub. L. 89–427, §2, May 20, 1966, 80 Stat. 161; Pub. L. 89–765, Nov. 5, 1966, 80 Stat. 1314; Pub. L. 90–269, §1, Mar. 18, 1968, 82 Stat. 50; Pub. L. 95–251, §2(a)(3), Mar. 27, 1978, 92 Stat. 183; Pub. L. 96–221, title I, §102, Mar. 31, 1980, 94 Stat. 132; Pub. L. 97–258, §5(b), Sept. 13, 1982, 96 Stat. 1068; Pub. L. 97–457, §17(b), Jan. 12, 1983, 96 Stat. 2509; Pub. L. 101–73, title VII, §744(i)(1), Aug. 9, 1989, 103 Stat. 439; Pub. L. 102–242, title I, §§133(f), 142(c), Dec. 19, 1991, 105 Stat. 2273, 2281; Pub. L. 102–550, title XVI, §1603(d)(9), Oct. 28, 1992, 106 Stat. 4080; Pub. L. 103–325, title III, §§322(d), 331(d), title VI, §602(g)(2), Sept. 23, 1994, 108 Stat. 2227, 2232, 2293; Pub. L. 106–102, title VII, §735, Nov. 12, 1999, 113 Stat. 1479; Pub. L. 107–56, title III, §364, Oct. 26, 2001, 115 Stat. 333; Pub. L. 107–297, title III, §301, Nov. 26, 2002, 116 Stat. 2340; Pub. L. 111–203, title III, §§318(c), 366(1), title XI, §§1103(b), 1108(c), July 21, 2010, 124 Stat. 1527, 1556, 2118, 2126.)

REFERENCES IN TEXT

Sections 461, 463, 464, 465, and 466 of this title, referred to in subsec. (a)(2), was in the original ''section 19 of the Federal Reserve Act''. Provisions of section 19 relating to reserve requirements are classified to the cited sections. For complete classification of section 19 to the Code, see References in Text note set out under section 461 of this title.

This chapter, referred to in subsecs. (c), (h), (i), (n), (r)(1), and (s)(1), was in the original ''this Act'', meaning act Dec. 23, 1913, ch. 6, 38 Stat. 251, known as the Federal Reserve Act. For complete classification of this Act to the Code, see References in Text note set out under section 226 of this title and Tables.

Reference in subsec. (e) to ''section 20 of this Act'' means section 20 of the Federal Reserve Act which is not classified to the Code. Since section 20 does not set forth any reserve requirements, section 19 of the Federal Reserve Act might have been intended. For provisions of section 19 relating to reserve requirements, see note above.

The Act of January sixteenth, eighteen hundred and eighty-three, referred to in subsec. (*l*), is act Jan. 16, 1883, ch. 27, 22 Stat. 403, as amended, which enacted section 42 of former Title 40, Public Buildings, Property, and Works, and sections 632, 633, 635, 637, 638, and 640 to 642a of former Title 5, Executive Departments and Government Officers and Employees. For complete classification of this Act to the Code, see Tables. Section 42 of former Title 40 was repealed and reenacted as section 8165 of Title 40, Public Buildings, Property, and Works, by Pub. L. 107–217, §§1, 6(b), Aug. 21, 2002, 116 Stat. 1062, 1304. The sections that were classified to former Title 5 were repealed by Pub. L. 89–554, §8(a), Sept. 6, 1966, 80 Stat. 632, the first section of which enacted Title 5, Government Organization and Employees. For distribution of former sections of Title 5 into the revised Title 5, see table at the beginning of Title 5.

This title, referred to in subsec. (p), probably should read ''this Act'', meaning act Dec. 23, 1913, ch. 6, 38 Stat. 251, as amended, known as the Federal Reserve Act, which does not contain titles. For complete classification of this Act to the Code, see References in Text note set out under section 226 of this title and Tables.

Subsection (a) or (c) of section 1109 of the Dodd-Frank Wall Street Reform and Consumer Protection Act, referred to in subsec. (s)(7), is subsec. (a) or (c) of section 1109 of Pub. L. 111–203, title XI, 124 Stat. 2127, 2128, which is not classified to the Code.

July 21, 2010, referred to in subsec. (s)(8)(B), was in the original ''the date of enactment of this section'', which was translated as meaning the date of enactment of Pub. L. 111–203 which added subsec. (s), to reflect the probable intent of Congress.

CODIFICATION

In subsec. (k), ''subchapter II of chapter 5, and chapter 7, of title 5'' was substituted for ''the Administrative Procedure Act'' on authority of section 7(b) of Pub. L. 89–554, Sept. 6, 1966, 80 Stat. 631, the first section of which enacted Title 5, Government Organization and Employees.

Section is comprised of section 11 of act Dec. 23, 1913. The fourteenth par. of section 16 of act Dec. 23, 1913, which formerly constituted subsec. (*o*) of this section, is now classified to section 248–1 of this title.

AMENDMENTS

2010—Subsec. (a)(2). Pub. L. 111–203, §366(1)(A), which directed insertion of ''State savings associations that are insured depository institutions (as defined in section 1813 of this title),'' after ''case of insured'', was executed by making the insertion after ''case of insured'' in subpar. (B)(i), to reflect the probable intent of Congress.

Subsec. (a)(2)(B)(iii). Pub. L. 111–203, §366(1)(B), (C), substituted ''Comptroller of the Currency'' for ''Director of the Office of Thrift Supervision'' and inserted ''Federal'' before ''savings association which''.

Subsec. (a)(2)(B)(iv). Pub. L. 111–203, §366(1)(D), substituted ''savings association'' for ''savings and loan association''.

Subsec. (k). Pub. L. 111–203, §1108(c), inserted at end ''The Board of Governors may not delegate to a Federal reserve bank its functions for the establishment of policies for the supervision and regulation of depository institution holding companies and other financial firms supervised by the Board of Governors.''

Subsec. (s). Pub. L. 111–203, §1103(b), added subsec. (s) relating to Federal Reserve transparency and release of information.

Pub. L. 111–203, § 318(c), added subsec. (s) relating to assessments, fees, and other charges for certain companies.

2002—Subsec. (r). Pub. L. 107–297 added subsec. (r).

2001—Subsec. (q). Pub. L. 107–56 added subsec. (q).

1999—Subsec. (m). Pub. L. 106–102 substituted ''[Repealed]'' for text of subsec. (m) which related to percentage of capital and surplus represented by loans to be determined by the Federal Reserve Board.

1994—Subsec. (d). Pub. L. 103–325, § 602(g)(2), substituted ''Secretary of the Treasury'' for ''bureau under the charge of the Comptroller of the Currency'' before ''the issue and retirement'' and for ''Comptroller'' before ''to the Federal Reserve agents''.

Subsec. (m). Pub. L. 103–325, § 322(d), which directed substitution of ''15 percent'' for ''10 percentum'' wherever appearing, was executed by substituting ''15 percent'' for ''10 per centum'' in two places to reflect the probable intent of Congress.

Subsec. (p). Pub. L. 103–325, § 331(d), added subsec. (p).

1992—Subsecs. (*o*), (p). Pub. L. 102–550 redesignated subsec. (p) as (*o*).

1991—Subsec. (n). Pub. L. 102–242, § 142(c), which directed addition of subsec. (n) at end of section, was executed by adding subsec. (n) after subsec. (m). See Construction of 1991 Amendment note below.

Subsec. (p). Pub. L. 102–242, § 133(f), added subsec. (p).

1989—Subsec. (a)(2)(iii). Pub. L. 101–73 substituted ''the Director of the Office of Thrift Supervision in the case of any savings association which is an insured depository institution (as defined in section 1813 of this title)'' for ''Federal Home Loan Bank Board in the case of any institution insured by the Federal Savings and Loan Insurance Corporation''.

1983—Subsec. (m). Pub. L. 97–457 substituted ''under section 84(c)(4) of this title'' for ''under paragraph (8) of section 84 of this title'' after ''in the case of national banks''.

1982—Subsec. (n). Pub. L. 97–258 struck out subsec. (n) which provided that, whenever in the judgment of the Secretary of the Treasury such action was necessary to protect the currency system of the United States, the Secretary of the Treasury, in his discretion, could require any or all individuals, partnerships, associations, and corporations to pay and deliver to the Treasurer of the United States any or all gold coin, gold bullion, and gold certificates owned by such individuals, partnerships, associations, and corporations and that, upon receipt of such gold coin, gold bullion or gold certificates, the Secretary of the Treasury would pay therefor an equivalent amount of any other form of coin or currency coined or issued under the laws of the United States.

1980—Subsec. (a). Pub. L. 96–221 designated existing provisions as par. (1) and added par. (2).

1978—Subsec. (k). Pub. L. 95–251 substituted ''administrative law judges'' for ''hearing examiners''.

1968—Subsec. (c). Pub. L. 90–269 struck out requirements for establishment by the Board of Governors of the Federal Reserve System of a graduated tax on the deficiency in the gold reserve whenever the reserve held against Federal Reserve notes fell below 25 percent and for an automatic increase in the rates of interest or discount fixed by the Board in an amount equal to the graduated tax imposed.

1966—Subsec. (d). Pub. L. 89–427 excepted the cancellation and destruction, and the accounting with respect to the cancellation and destruction, of notes unfit for circulation from the area of responsibility exercised by the Board of Governors of the Federal Reserve System through the Bureau of the Comptroller of the Currency over the issue and retirement of Federal Reserve notes.

Subsec. (k). Pub. L. 89–765 added subsec. (k). A former subsec. (k) was repealed by Pub. L. 87–722, § 3, Sept. 28, 1962, 76 Stat. 670.

1962—Subsec. (k). Pub. L. 87–722 repealed subsec. (k) which related to the authority of the Board of Governors of the Federal Reserve System to permit national banks to act as trustees, etc., and is now covered by section 92a of this title.

1959—Subsec. (e). Pub. L. 86–114 substituted ''reserve cities'' for ''reserve and central reserve cities'' in two places.

Subsec. (m). Pub. L. 86–251 struck out ''in the form of notes'' after ''represented by obligations'' in proviso.

1945—Subsec. (c). Act June 12, 1945, substituted ''25 per centum'' for ''40 per centum'', and ''20 per centum'' for ''32½ per centum'' wherever appearing.

1935—Subsec. (k). Act Aug. 23, 1935, § 342, amended last sentence of third par.

Subsec. (m). Act Aug. 23, 1935, § 321(a), inserted proviso at end of first sentence.

1933—Subsec. (m). Act June 16, 1933, amended provisions generally.

Subsec. (n). Act Mar. 9, 1933, added subsec. (n).

1930—Subsec. (k). Act June 26, 1930, added last par.

Change of Name

Section 203(a) of act Aug. 23, 1935, changed name of Federal Reserve Board to Board of Governors of the Federal Reserve System.

Effective Date of 2010 Amendment

Amendment by section 318(c) of Pub. L. 111–203 effective on the transfer date, see section 318(e) of Pub. L. 111–203, set out as an Effective Date note under section 16 of this title.

Amendment by section 366(1) of Pub. L. 111–203 effective on the transfer date, see section 351 of Pub. L. 111–203, set out as a note under section 906 of Title 2, The Congress.

Amendment by sections 1103(b) and 1108(c) of Pub. L. 111–203 effective 1 day after July 21, 2010, except as otherwise provided, see section 4 of Pub. L. 111–203, set out as an Effective Date note under section 5301 of this title.

Effective Date of 1992 Amendment

Amendment by Pub. L. 102–550 effective as if included in the Federal Deposit Insurance Corporation Improvement Act of 1991, Pub. L. 102–242, as of Dec. 19, 1991, except that where amendment is to any provision of law added or amended by Pub. L. 102–242 effective after Dec. 19, 1992, then amendment by Pub. L. 102–550 effective on effective date of amendment by Pub. L. 102–242, see section 1609 of Pub. L. 102–550, set out as a note under section 191 of this title.

Effective Date of 1991 Amendment

Amendment by section 133(f) of Pub. L. 102–242 effective 1 year after Dec. 19, 1991, see section 133(g) of Pub. L. 102–242, set out as a note under section 191 of this title.

Effective Date of 1980 Amendment

Section 108 of title I of Pub. L. 96–221 provided that: ''This title [enacting section 248a of this title, amending this section and sections 342, 347b, 355, 360, 412, 461, 463, 505, and 1425a of this title, and enacting provisions set out as notes under sections 226 and 355 of this title] shall take effect on the first day of the sixth month which begins after the date of the enactment of this title [Mar. 31, 1980], except that the amendments regarding sections 19(b)(7) and 19(b)(8)(D) of the Federal Reserve Act [section 461(b)(7) and (b)(8)(D) of this title] shall take effect on the date of enactment of this title.''

Effective Date of 1959 Amendment

Amendment by Pub. L. 86–114 effective three years after July 28, 1959, see section 3(b) of Pub. L. 86–114, set out as a Central Reserve and Reserve Cities note under former section 141 of this title.

Construction of 1991 Amendment

Section 1603(e)(2) of Pub. L. 102–550 provided that: ''The amendment made by section 142(c) of the Federal Deposit Insurance Corporation Improvement Act of 1991

[Pub. L. 102–242] (adding a paragraph at the end of section 11 of the Federal Reserve Act [this section]) shall be considered to have been executed before the amendment made by section 133(f) of the Federal Deposit Insurance Corporation Improvement Act of 1991 [amending this section].''

EXECUTIVE ORDER NO. 6359

Ex. Ord. No. 6359, Oct. 25, 1933, as amended by Ex. Ord. No. 11825, Dec. 31, 1974, 40 F.R. 1003, which provided for receipt on consignment of gold by the United States mints and assay offices, was revoked by Ex. Ord. No. 12553, Feb. 25, 1986, 51 F.R. 7237.

EX. ORD. NO. 10547. INSPECTION OF STATISTICAL TRANSCRIPT CARDS

Ex. Ord. No. 10547, July 27, 1954, 19 F.R. 4661, required statistical transcript cards submitted with, or prepared by the Internal Revenue Service from, corporation income tax returns for the taxable years ending after June 30, 1951, and before July 1, 1952, to be open to inspection by the Board of Governors of the Federal Reserve System as an aid in executing the powers conferred upon such Board by this section, such inspection to be in accordance and upon compliance with the rules and regulations prescribed by the Secretary of the Treasury in T.D. 6081, 19 F.R. 4666.

§ 248–1. Rules and regulations for transfer of funds and charges therefor among banks; clearing houses

The Board of Governors of the Federal Reserve System shall make and promulgate from time to time regulations governing the transfer of funds and charges therefor among Federal reserve banks and their branches, and may at its discretion exercise the functions of a clearing house for such Federal reserve banks, or may designate a Federal reserve bank to exercise such functions, and may also require each such bank to exercise the functions of a clearing house for depository institutions.

(Dec. 23, 1913, ch. 6, § 16 (par.), 38 Stat. 268; Aug. 23, 1935, ch. 614, § 203(a), 49 Stat. 704; Pub. L. 96–221, title I, § 105(d), Mar. 31, 1980, 94 Stat. 140.)

CODIFICATION

Section is comprised of the thirteenth par. (formerly the fourteenth par.) of section 16 of act Dec. 23, 1913, which was formerly classified to section 248(*o*) of this title. For classification to this title of other pars. of section 16, see Codification note set out under section 411 of this title.

AMENDMENTS

1980—Pub. L. 96–221, which directed amendment of ''[t]he fourteenth paragraph of section 16 of the Federal Reserve Act (12 U.S.C. 248(*o*))'' by substituting ''depository institutions'' for ''its member banks'', was executed by making the substitution in this section to reflect the probable intent of Congress.

CHANGE OF NAME

Section 203(a) of act Aug. 23, 1935, changed the name of the Federal Reserve Board to Board of Governors of the Federal Reserve System.

EFFECTIVE DATE OF 1980 AMENDMENT

Amendment by Pub. L. 96–221 effective on first day of sixth month which begins after Mar. 31, 1980, see section 108 of Pub. L. 96–221, set out as a note under section 248 of this title.

§ 248a. Pricing of services

(a) Publication of pricing principles and proposed schedule of fees; effective date of schedule of fees

Not later than the first day of the sixth month after March 31, 1980, the Board shall publish for public comment a set of pricing principles in accordance with this section and a proposed schedule of fees based upon those principles for Federal Reserve bank services to depository institutions, and not later than the first day of the eighteenth month after March 31, 1980, the Board shall begin to put into effect a schedule of fees for such services which is based on those principles.

(b) Covered services

The services which shall be covered by the schedule of fees under subsection (a) of this section are—

(1) currency and coin services;
(2) check clearing and collection services;
(3) wire transfer services;
(4) automated clearinghouse services;
(5) settlement services;
(6) securities safekeeping services;
(7) Federal Reserve float; and
(8) any new services which the Federal Reserve System offers, including but not limited to payment services to effectuate the electronic transfer of funds.

(c) Criteria applicable

The schedule of fees prescribed pursuant to this section shall be based on the following principles:

(1) All Federal Reserve bank services covered by the fee schedule shall be priced explicitly.

(2) All Federal Reserve bank services covered by the fee schedule shall be available to nonmember depository institutions and such services shall be priced at the same fee schedule applicable to member banks, except that nonmembers shall be subject to any other terms, including a requirement of balances sufficient for clearing purposes, that the Board may determine are applicable to member banks.

(3) Over the long run, fees shall be established on the basis of all direct and indirect costs actually incurred in providing the Federal Reserve services priced, including interest on items credited prior to actual collection, overhead, and an allocation of imputed costs which takes into account the taxes that would have been paid and the return on capital that would have been provided had the services been furnished by a private business firm, except that the pricing principles shall give due regard to competitive factors and the provision of an adequate level of such services nationwide.

(4) Interest on items credited prior to collection shall be charged at the current rate applicable in the market for Federal funds.

(d) Budgetary consequences of decline in volume of services

The Board shall require reductions in the operating budgets of the Federal Reserve banks

Rules and Regulations

Federal Register
Vol. 68, No. 72
Tuesday, April 15, 2003

FEDERAL RESERVE SYSTEM

12 CFR Part 268

[Docket No. R–1096]

Rules Regarding Equal Opportunity

AGENCY: Board of Governors of the Federal Reserve System.

ACTION: Final rule.

SUMMARY: The Board of Governors of the Federal Reserve System (the Board) has adopted a final rule that amends its "Rules Regarding Equal Opportunity," which establishes programs and procedures to promote equal opportunity for Board employees. This rule was published on January 25, 2001, in the **Federal Register** as an immediately effective interim rule with opportunity for public comment. The Board received one public comment on this rule. The Board is now adopting the interim rule as a final rule with substantive changes to sections in the rule that address the Rehabilitation Act. These substantive changes are being made because after the Board adopted its interim rule, the Equal Employment Opportunity Commission (Commission), after public comment, adopted changes to the provisions in its parallel regulation entitled "Federal Sector Equal Employment Opportunity," 29 CFR part 1614, that address the Rehabilitation Act. The substantive changes to the Board's final rule, which incorporates changes to the Commission's regulation on the Rehabilitation Act, also respond to the comment that the Board received on its rule.

DATES: This final rule is effective immediately and applies to all Board equal employment opportunity (EEO) complaints pending at any stage of the administrative process as of April 15, 2003.

FOR FURTHER INFORMATION CONTACT: Stephen L. Siciliano, Assistant General Counsel (202–452–3920), or Alicia S. Foster, Counsel (202–452–5289), Legal Division, Board of Governors of the Federal Reserve System, 20th Street and Constitution Avenue NW., Washington, DC 20551. For users of Telecommunications Device for the Deaf ("TDD") only, contact 202/263–4869.

SUPPLEMENTARY INFORMATION: On January 2, 2001, the Board approved the revision of the Board's "Rules Regarding Equal Opportunity" as an immediately effective interim rule with opportunity for comment. The rule was published in the **Federal Register** on January 25, 2001 (66 FR 7703). The interim rule revised the Board's existing regulation entitled "Rules on Equal Opportunity," 12 CFR part 268, to incorporate the November 1999 changes made by the Equal Employment Opportunity Commission (Commission) to its parallel regulation entitled "Federal Sector Equal Employment Opportunity," 29 CFR part 1614, governing equal employment opportunity in the federal government generally. As explained in the preamble to the interim rule, this amendment is consistent with the Board's past practice as the Board's rule is modeled after and, in most respects, is identical to the Commission's regulation. The interim rule also made additional changes to the Board's regulation to bring it into closer conformance with the Commission's regulation. In a few instances, the interim rule continued distinctions between the Board's rule and the Commission's rule that reflect the Board's statutorily mandated independence.

One comment was received. The commentator, the Commission, suggested that rather than adopt a separate regulation governing the processing of complaints of discrimination, the Board should adopt the Commission's Government-wide complaint processing procedures. As the Board has pointed out in prior amendments to part 268, however, the Board believes that based on the specific provisions of the Federal Reserve Act and established precedent, the adoption of part 268 is necessary to authorize and ensure the Board's compliance with important national laws and policies prohibiting discrimination in employment on the basis of race, color, religion, sex, national origin, age, disability, or retaliation.

The Commission also questioned five provisions in the Board's rule that differ from the corresponding provisions in the Commission's rule on employee EEO complaints. Three of the provisions retain authority for the Board as to a decision issued by the Commission on employee complaints of discrimination. The Commission expressed concerns that it is not clear how these provisions relate to the Commission's rule or to the sections in the interim rule that set forth the time periods for a complainant to file a civil action. The other two provisions regard the overall relationship between the Commission and the Board and address how the Board will provide EEO program information to the Commission. Except as discussed below, the Board adopts the interim rule as a final rule.

As an initial matter, it should be noted that all of the provisions that the Commission points to as differing from its regulation are updated provisions rather than new provisions. Similar provisions were contained in the Board's rule on equal opportunity prior to the adoption of the interim rule on January 25, 2001. While the Board recognizes that the provisions in question retain authority that is not found in the Commission's regulation, the Board believes the retention of authority is necessary to comply with its statutorily mandated independence while also complying with the laws prohibiting discrimination in employment. The provisions at issue are based on the Board's traditional view of its authority under the Federal Reserve Act, which provides that the "employment, compensation, leave, and expenses" of Board employees is governed solely by that Act. Section 10(4).[1] The provisions address areas that the Board believes affect its independence and thus the distinctions are appropriate. As explained in the preamble to the interim rule, however, the Board has minimized, to the greatest extent possible, distinctions between its rule and the Commission's rule. Accordingly, with the few exceptions noted by the Commission, the Board's interim rule closely conforms to the Commission's rule. The Board will continue to work with the Commission

[1] 12 U.S.C. 244.

to ensure that the Board's rule is effectively implemented consistent with the laws and policies enforced by the Commission. Accordingly, the Board believes that no changes to these provisions in the interim rule are appropriate.

The Commission also commented on a provision in the Board's interim regulation implementing the Rehabilitation Act (29 U.S.C. 791), which prohibits discrimination against individuals with disabilities by the federal government. The particular provision at issue addresses alcoholism, 12 CFR 268.203(h)(3). The Commission questioned whether section 268.203(h)(3) was consistent with current law. Before the Board could address the Commission's concerns, however, the Commission adopted changes to the parallel provision in the Commission's rule. On May 21, 2002, the Commission published a final rule revising the sections in its rule regarding the Rehabilitation Act. (67 FR 35732). The Commission's rule provides that the federal government shall be a model employer of individuals with disabilities. The rule also provides that in determining whether the Rehabilitation Act, as amended, has been violated in a complaint alleging nonaffirmative action employment discrimination, the standards under Titles I and V of the Americans with Disabilities Act of 1990, insofar as they cover employment in the private sector, shall be applied. The rules also provide that these standards are set forth in the Commission's ADA regulation at 29 CFR part 1630. The Board has determined that it would be appropriate to revise its Rehabilitation Act rules consistent with the Commission's May 21, 2002, final rule. By making these changes, the Board is addressing the Commission's concern with the provision on alcoholism in the interim rule as that provision will be deleted.

In order to incorporate the Commission's May 21, 2002, final rule, section 268.102, paragraph (9) of the interim rule, which relates to the obligations of the Board's EEO program with respect to employees with physical or mental limitations, has also been deleted in the final rule. This provision corresponds to a provision in the Commission's prior regulation, which the Commission deleted.[2] In addition, the present language in section 268.203 has been replaced with the corresponding language from the Commission's final rule, which provides that the government shall be a model employer of individuals with disabilities and applies the ADA standards (Title I and V) to determine whether a violation of section 501 of the Rehabilitation Act has occurred. The Board's final rule also incorporates the reference to the Commission's ADA regulation. Thus, as these changes to the Board's rules are made in response to the comment received on the interim rule and are consistent with those made by the Commission in its May 21, 2002, final rule, additional comment would not serve the public interest as the Commission's rule was adopted only after public comment. As described above, the changes to the Rehabilitation Act provisions in the Board's corresponding rule incorporate existing Commission procedures which were adopted after public notice and comment. Further, as the Commission's changes to the Rehabilitation Act provisions are effective as of June 20, 2002, to ensure that EEO complaints by Board employees are handled consistently with the procedures of the Commission, it is important that the Board adopt corresponding changes without additional delay.

Finally, the Commission suggested that the Board apply the interim rule retroactively to cover employee complaints of discrimination pending on November 9, 1999, the effective date of the Commission's revised rule, which prompted the Board's revision of its corresponding rule. The Board does not believe that any further action in this regard is necessary, however, because the interim rule was effective immediately upon publication of the interim rule and applied to all pending cases as of January 25, 2001. Thus, to the extent an EEO complaint was in the administrative process on that date, it was processed under procedures similar to those adopted by the Commission. It appears that, for the most part, the administrative processing at the Board of complaints pending as of January 2001 has been completed, so that retroactive application at this time would have little effect.

Accordingly, with the exception of the substantive changes discussed above, the Board is now adopting the interim rule on equal employment opportunity as a final rule. No other substantive changes have been made to the interim rule. The final rule makes editorial changes to certain other parts of the Board's interim regulation, namely, the provision on employment of noncitizens and the subpart prohibiting discrimination in Board programs and activities on the basis of disability, which are not administered by the Commission.

Pursuant to the Administrative Procedures Act (APA), 5 U.S.C. 553(d)(3), the Board has determined that it is unnecessary and would be impracticable to defer the effective date of this final rule for 30 days. The final rule, like the interim rule, which was effective immediately on publication, in substance is applying the Commission's existing regulation, which was revised twice and in both instances adopted only after notice and public comment. Thus, the Board's rule will not cause unfair prejudice as the standards that are being applied in the final rule in virtually all respects are not new and are already in effect under the interim rule. The one major substantive change to the interim rule by the final rule conforms the Rehabilitation Act provisions covering Board employee to those governing Federal employers generally.

Paperwork Reduction Act

In accordance with the Paperwork Reduction Act of 1995 (44 U.S.C. 3506; 5 CFR 1320 Appendix A.1), the Board reviewed the proposed rule under the authority delegated to the Board by the Office of Management and Budget. No collections of information pursuant to the Paperwork Reduction Act are contained in the final rule.

Regulatory Flexibility Act Analysis

Pursuant to section 605(b) of the Regulatory Flexibility Act (Pub. L. 96–354, 5 U.S.C. 601, *et seq.*), the Board certifies that this rule will not have a significant economic impact on a substantial number of small entities. This rule governs the Board's dealings with its employees, applicants for employment, and others affected in a like manner.

Plain Language

Section 722 of the Gramm-Leach-Bliley Act requires each federal banking agency to use plain language in all proposed and final rules published after January 1, 2000. Because the Board has determined that this final rule, similar to the interim rule, should conform to the greatest possible with the parallel regulation of the Equal Employment Opportunity Commission, the Board's ability to specifically address the plain language requirement was limited.

[2] The Board's final rule, similar to the Commission's changes to its regulation, renumbers the remaining paragraphs. Further, the citation to section 268.203(a)(6) in section 268.702(e)(3) of Subpart H, which prohibits discrimination in Board programs and activities on the basis of disability and which is a matter not administered by the Commission, has been changed to section 268.203 as the prior citation is no longer valid.

List of Subjects in 12 CFR part 268

Administrative practice and procedure, Aged, Civil rights, Equal employment opportunity, Federal buildings and facilities, Federal Reserve System, Government employees, Individuals with disabilities, Religious discrimination, Sex discrimination, Wages.

■ For the reasons set out in the preamble, the Board revises 12 CFR part 268 to read:

PART 268—RULES REGARDING EQUAL OPPORTUNITY

Subpart A—General Provisions and Administration

Subpart B—Board Program To Promote Equal Opportunity

Subpart C—Provisions Applicable to Particular Complaints

Subpart D—Related Processes

Subpart E—Appeals to the Equal Employment Opportunity Commission

Subpart F—Remedies and Enforcement

Subpart G—Matters of General Applicability

Subpart H—Prohibition Against Discrimination in Board Programs and Activities Because of a Physical or Mental Disability

Authority: 12 U.S.C. 244 and 248(i), (k) and (1).

Subpart A—General Provisions and Administration

§ 268.1 Authority, purpose and scope.

(a) *Authority.* The regulations in this part (12 CFR part 268) are issued by the Board of Governors of the Federal Reserve System (Board) under the authority of sections 10(4) and 11(i), (k), and (l) of the Federal Reserve Act (partially codified in 12 U.S.C. 244 and 248(i), (k) and (1)).

(b) *Purpose and scope.* This part sets forth the Board's policy, program and procedures for providing equal opportunity to Board employees and applicants for employment without regard to race, color, religion, sex, national origin, age, or physical or mental disability. It also sets forth the Board's policy, program and procedures for prohibiting discrimination on the basis of physical or mental disability in programs and activities conducted by the Board. It also specifies the circumstances under which the Board will hire or decline to hire persons who are not citizens of the United States, consistent with the Board's operational needs and applicable law.

§ 268.2 Definitions.

The definitions contained in this section shall have the following meanings throughout this part unless otherwise stated.

(a) *Commission or EEOC* means the Equal Employment Opportunity Commission.

(b) *Title VII* means Title VII of the Civil Rights Act (42 U.S.C. 2000e *et seq.*).

Subpart B—Board Program To Promote Equal Opportunity

§ 268.101 General policy for equal opportunity.

(a) It is the policy of the Board to provide equal opportunity in employment for all persons, to prohibit discrimination in employment because of race, color, religion, sex, national origin, age or disability, and to promote the full realization of equal opportunity in employment through a continuing affirmative program.

(b) No person shall be subject to retaliation for opposing any practice made unlawful by Title VII of the Civil Rights Act (title VII) (42 U.S.C. 2000e *et seq.*), the Age Discrimination in Employment Act (ADEA) (29 U.S.C. 621 *et seq.*), the Equal Pay Act (29 U.S.C. 206(d)), or the Rehabilitation Act (29 U.S.C. 791 *et seq.*) or for participating in any stage of administrative or judicial proceedings under those statutes.

§ 268.102 Board program for equal employment opportunity.

(a) The Board shall maintain a continuing affirmative program to promote equal opportunity and to identify and eliminate discriminatory practices and policies. In support of this program, the Board shall:

(1) Provide sufficient resources to its equal opportunity program to ensure efficient and successful operation;

(2) Provide for the prompt, fair and impartial processing of complaints in accordance with this part and the instructions contained in the Commission's Management Directives;

(3) Conduct a continuing campaign to eradicate every form of prejudice or discrimination from the Board's personnel policies, practices and working conditions;

(4) Communicate the Board's equal employment opportunity policy and program and its employment needs to all sources of job candidates without regard to race, color, religion, sex, national origin, age or disability, and solicit their recruitment assistance on a continuing basis;

(5) Review, evaluate and control managerial and supervisory performance in such a manner as to insure a continuing affirmative application and vigorous enforcement of the policy of equal opportunity, and provide orientation, training and advice to managers and supervisors to assure their understanding and implementation of the equal

employment opportunity policy and program;

(6) Take appropriate disciplinary action against employees who engage in discriminatory practices;

(7) Make reasonable accommodation to the religious needs of employees and applicants for employment when those accommodations can be made without undue hardship on the business of the Board;

(8) Make reasonable accommodation to the known physical or mental limitations of qualified applicants and employees with a disability unless the accommodation would impose an undue hardship on the operations of the Board's program;

(9) Provide recognition to employees, supervisors, managers and units demonstrating superior accomplishment in equal employment opportunity;

(10) Establish a system for periodically evaluating the effectiveness of the Board's overall equal employment opportunity effort;

(11) Provide the maximum feasible opportunity to employees to enhance their skills through on-the-job training, work-study programs and other training measures so that they may perform at their highest potential and advance in accordance with their abilities;

(12) Inform its employees and recognized labor organizations of the Board's affirmative equal opportunity policy and program and enlist their cooperation; and

(13) Participate at the community level with other employers, with schools and universities and with other public and private groups in cooperative action to improve employment opportunities and community conditions that affect employability.

(b) In order to implement its program, the Board shall:

(1) Develop the plans, procedures and regulations necessary to carry out its program;

(2) Establish or make available an alternative dispute resolution program. Such program must be available for both the precomplaint process and the formal complaint process.

(3) Appraise its personnel operations at regular intervals to assure their conformity with the Board's program, this part 268 and the instructions contained in the Commission's management directives;

(4) Designate a Director for Equal Employment Opportunity (EEO Programs Director), EEO Officer(s), and such Special Emphasis Program Managers/Coordinators (*e.g.*, People with Disabilities Program, Federal Women's Program and Hispanic Employment Program), clerical and administrative support as may be necessary to carry out the functions described in this part in all organizational units of the Board and at all Board installations. The EEO Programs Director shall be under the immediate supervision of the Chairman.

(5) Make written materials available to all employees and applicants informing them of the variety of equal employment opportunity programs and administrative and judicial remedial procedures available to them and prominently post such written materials in all personnel and EEO offices and throughout the workplace;

(6) Ensure that full cooperation is provided by all Board employees to EEO Counselors and Board EEO personnel in the processing and resolution of pre-complaint matters and complaints within the Board and that full cooperation is provided to the Commission in the course of appeals, including, granting the Commission routine access to personnel records of the Board when required in connection with an investigation;

(7) Publicize to all employees and post at all times the names, business telephone numbers and business addresses of the EEO Counselors (unless the counseling function is centralized, in which case only the telephone number and address need be publicized and posted), a notice of the time limits and necessity of contacting a Counselor before filing a complaint and the telephone numbers and addresses of the EEO Programs Director, EEO Officer(s) and the Special Emphasis Program Managers/Coordinators.

(c) The EEO Programs Director shall be responsible for:

(1) Advising the Board of Governors with respect to the preparation of national and regional equal employment opportunity plans, procedures, regulations, reports and other matters pertaining to the policy in § 268.101 and the Board's program;

(2) Evaluating from time to time the sufficiency of the total Board program for equal employment opportunity and reporting to the Board of Governors with recommendations as to any improvement or correction needed, including remedial or disciplinary action with respect to managerial, supervisory or other employees who have failed in their responsibilities;

(3) When authorized by the Board of Governors, making changes in programs and procedures designed to eliminate discriminatory practices and to improve the Board's program for equal employment opportunity;

(4) Providing for counseling of aggrieved individuals and for the receipt and processing of individual and class complaints of discrimination; and

(5) Assuring that individual complaints are fairly and thoroughly investigated and that final action is taken in a timely manner in accordance with this part.

(d) Directives, instructions, forms and other Commission materials referenced in this part may be obtained in accordance with the provisions of 29 CFR 1610.7.

§ 268.103 Complaints of discrimination covered by this part.

(a) Individual and class complaints of employment discrimination and retaliation prohibited by title VII (discrimination on the basis of race, color, religion, sex and national origin), the ADEA (discrimination on the basis of age when the aggrieved person is at least 40 years of age), the Rehabilitation Act (discrimination on the basis of disability), or the Equal Pay Act (sex-based wage discrimination) shall be processed in accordance with this part. Complaints alleging retaliation prohibited by these statutes are considered to be complaints of discrimination for purposes of this part.

(b) This part applies to all Board employees and applicants for employment at the Board, and to all employment policies or practices affecting Board employees or applicants for employment.

(c) This part does not apply to Equal Pay Act complaints of employees whose services are performed within a foreign country or certain United States territories as provided in 29 U.S.C. 213(f).

§ 268.104 Pre-complaint processing.

(a) Aggrieved persons who believe they have been discriminated against on the basis of race, color, religion, sex, national origin, age or disability must consult a Counselor prior to filing a complaint in order to try to informally resolve the matter.

(1) An aggrieved person must initiate contact with a Counselor within 45 days of the date of the matter alleged to be discriminatory or, in the case of a personnel action, within 45 days of the effective date of the action.

(2) The Board or the Commission shall extend the 45-day time limit in paragraph (a)(1) of this section when the individual shows that he or she was not notified of the time limits and was not otherwise aware of them, that he or she did not know and reasonably should not have known that the discriminatory matter or personnel action occurred, that despite due diligence he or she was prevented by circumstances beyond his

or her control from contacting the counselor within the time limits, or for other reasons considered sufficient by the Board or the Commission.

(b)(1) At the initial counseling session, Counselors must advise individuals in writing of their rights and responsibilities, including the right to request a hearing or an immediate final decision after an investigation by the Board in accordance with § 268.107(f), election rights pursuant to § 268.302, the right to file a notice of intent to sue pursuant to § 268.201(a) and a lawsuit under the ADEA instead of an administrative complaint of age discrimination under this part, the duty to mitigate damages, administrative and court time frames, and that only the claims raised in precomplaint counseling (or issues or claims like or related to issues or claims raised in pre-complaint counseling) may be alleged in a subsequent complaint filed with the Board. Counselors must advise individuals of their duty to keep the Board and the Commission informed of their current address and to serve copies of appeal papers on the Board. The notice required by paragraphs (d) or (e) of this section shall include a notice of the right to file a class complaint. If the aggrieved person informs the Counselor that he or she wishes to file a class complaint, the Counselor shall explain the class complaint procedures and the responsibilities of a class agent.

(2) Counselors shall advise aggrieved persons that, where the Board agrees to offer ADR in the particular case, they may choose between participation in the alternative dispute resolution program and the counseling activities provided for in paragraph (c) of this section.

(c) Counselors shall conduct counseling activities in accordance with instructions contained in Commission Management Directives. When advised that a complaint has been filed by an aggrieved person, the Counselor shall submit a written report within 15 days to the EEO Programs Director and the aggrieved person concerning the issues discussed and actions taken during counseling.

(d) Unless the aggrieved person agrees to a longer counseling period under paragraph (e) of this section, or the aggrieved person chooses an alternative dispute resolution procedure in accordance with paragraph (b)(2) of this section, the Counselor shall conduct the final interview with the aggrieved person within 30 days of the date the aggrieved person contacted the Board's EEO Programs Office to request counseling. If the matter has not been resolved, the aggrieved person shall be informed in writing by the Counselor, not later than the thirtieth day after contacting the Counselor, of the right to file a discrimination complaint with the Board. This notice shall inform the complainant of the right to file a discrimination complaint within 15 days of receipt of the notice, of the appropriate official with whom to file a complaint and of the complainant's duty to assure that the EEO Programs Director is informed immediately if the complainant retains counsel or a representative.

(e) Prior to the end of the 30-day period, the aggrieved person may agree in writing with the Board to postpone the final interview and extend the counseling period for an additional period of no more than 60 days. If the matter has not been resolved before the conclusion of the agreed extension, the notice described in paragraph (d) of this section shall be issued.

(f) Where the aggrieved person chooses to participate in an alternative dispute resolution procedure in accordance with paragraph (b)(2) of this section, the pre-complaint processing period shall be 90 days. If the claim has not been resolved before the 90th day, the notice described in paragraph (d) of this section shall be issued.

(g) The Counselor shall not attempt in any way to restrain the aggrieved person from filing a complaint. The Counselor shall not reveal the identity of an aggrieved person who consulted the Counselor, except when authorized to do so by the aggrieved person, or until the Board has received a discrimination complaint under this part from that person involving the same matter.

§ 268.105 Individual complaints.

(a) A complaint must be filed with the agency that allegedly discriminated against the complainant.

(b) A complaint must be filed within 15 days of receipt of the notice required by § 268.104 (d), (e) or (f).

(c) A complaint must contain a signed statement from the person claiming to be aggrieved or that person's attorney. This statement must be sufficiently precise to identify the aggrieved individual and the Board and to describe generally the action(s) or practice(s) that form the basis of the complaint. The complaint must also contain a telephone number and address where the complainant or the representative can be contacted.

(d) A complainant may amend a complaint at any time prior to the conclusion of the investigation to include issues or claims like or related to those raised in the complaint. After requesting a hearing, a complainant may file a motion with the administrative judge to ar
issues or c
raised in t

(e) The I
receipt of a complaint or an amendment to a complaint in writing and inform the complainant of the date on which the complaint or amendment was filed. The Board shall advise the complainant in the acknowledgment of the EEOC office and its address where a request for a hearing shall be sent. Such acknowledgment shall also advise the complainant that:

(1) The complainant has the right to appeal the final action on or dismissal of a complaint; and

(2) The Board is required to conduct an impartial and appropriate investigation of the complaint within 180 days of the filing of the complaint unless the parties agree in writing to extend the time period. When a complaint has been amended, the Board shall complete its investigation within the earlier of 180 days after the last amendment to the complaint or 360 days after the filing of the original complaint, except that the complainant may request a hearing from an administrative judge on the consolidated complaints any time after 180 days from the date of the first filed complaint.

§ 268.106 Dismissals of complaints.

(a) Prior to a request for a hearing in a case, the Board shall dismiss an entire complaint:

(1) That fails to state a claim under § 268.103 or § 268.105(a), or states the same claim that is pending before or has been decided by the Board or the Commission;

(2) That fails to comply with the applicable time limits contained in §§ 268.104, 268.105 and 268.204(c), unless the Board extends the time limits in accordance with § 268.604(c), or that raises a matter that has not been brought to the attention of a Counselor and is not like or related to a matter that has been brought to the attention of a Counselor;

(3) That is the basis of a pending civil action in a United States District Court in which the complainant is a party provided that at least 180 days have passed since the filing of the administrative complaint, or that was the basis of a civil action decided by a United States District Court in which the complainant was a party;

(4) Where a complainant has raised the matter in an appeal to the Merit Systems Protection Board and § 268.302 indicates that the complainant has elected to pursue the non-EEO process;

(5) That is moot or alleges that a proposal to take a personnel action, or other preliminary step to taking a personnel action, is discriminatory;

(6) Where the complainant cannot be located, provided that reasonable efforts have been made to locate the complainant and the complainant has not responded within 15 days to a notice of proposed dismissal sent to his or her last known address;

(7) Where the Board has provided the complainant with a written request to provide relevant information or otherwise proceed with the complaint, and the complainant has failed to respond to the request within 15 days of its receipt or the complainant's response does not address the Board's request, provided that the request included a notice of the proposed dismissal. Instead of dismissing for failure to cooperate, the complaint may be adjudicated if sufficient information for that purpose is available;

(8) That alleges dissatisfaction with the processing of a previously filed complaint; or

(9) Where the Board, strictly applying the criteria set forth in Commission decisions, finds that the complaint is part of a clear pattern of misuse of the EEO process for a purpose other than the prevention and elimination of employment discrimination. A clear pattern of misuse of the EEO process requires:

(i) Evidence of multiple complaint filings; and

(ii) Allegations that are similar or identical, lack specificity or involve matters previously resolved; or

(iii) Evidence of circumventing other administrative processes, retaliating against the Board's in-house administrative processes or overburdening the EEO complaint system.

(b) Where the Board believes that some but not all of the claims in a complaint should be dismissed for the reasons contained in paragraphs (a)(1) through (9) of this section, the Board shall notify the complainant in writing of its determination, the rationale for that determination and that those claims will not be investigated, and shall place a copy of the notice in the investigative file. A determination under this paragraph is reviewable by an administrative judge if a hearing is requested on the remainder of the complaint, but is not appealable until final action is taken on the remainder of the complaint.

§ 268.107 Investigation of complaints.

(a) The investigation of complaints filed against the Board shall be conducted by the Board.

(b) In accordance with instructions contained in Commission Management Directives, the Board shall develop an impartial and appropriate factual record upon which to make findings on the claims raised by the written complaint. An appropriate factual record is one that allows a reasonable fact finder to draw conclusions as to whether discrimination occurred. The Board may use an exchange of letters or memoranda, interrogatories, investigations, fact-finding conferences or any other fact-finding methods that efficiently and thoroughly address the matters at issue. The Board may incorporate alternative dispute resolution techniques into its investigative efforts in order to promote early resolution of complaints.

(c) The procedures in paragraphs (c)(1) through (3) of this section apply to the investigation of complaints:

(1) The complainant, the Board, and any employee of the Board shall produce such documentary and testimonial evidence as the investigator deems necessary.

(2) Investigators are authorized to administer oaths. Statements of witnesses shall be made under oath or affirmation or, alternatively, by written statement under penalty of perjury.

(3) When the complainant, or the Board or its employees fail without good cause shown to respond fully and in timely fashion to requests for documents, records, comparative data, statistics, affidavits or the attendance of witness(es), the investigator may note in the investigative record that the decisionmaker should, or the Commission on appeal may, in appropriate circumstances:

(i) Draw an adverse inference that the requested information, or the testimony of the requested witness, would have reflected unfavorably on the party refusing to provide the requested information;

(ii) Consider the matters to which the requested information or testimony pertains to be established in favor of the opposing party;

(iii) Exclude other evidence offered by the party failing to produce the requested information or witness;

(iv) Issue a decision fully or partially in favor of the opposing party; or

(v) Take such other actions as it deems appropriate.

(d) Any investigation will be conducted by investigators with appropriate security clearances.

(e)(1) The Board shall complete its investigation within 180 days of the date of filing of an individual complaint or within the time period contained in an order from the Office of Federal Operations on an appeal from a dismissal pursuant to § 268.106. By written agreement within those time periods, the complainant and the Board may voluntarily extend the time period for not more than an additional 90 days. The Board may unilaterally extend the time period or any period of extension for not more than 30 days where it must sanitize a complaint file that may contain information classified pursuant to Executive Order No. 12356, or successor orders, as secret in the interest of national defense or foreign policy, provided the Board notifies the complainant of the extension.

(2) Confidential supervisory information, as defined in 12 CFR 261.2(c), and other confidential information of the Board may be included in the investigative file by the investigator, the EEO Programs Director, or another appropriate officer of the Board, where such information is relevant to the complaint. Neither the complainant nor the complainant's personal representative may make further disclosure of such information, however, except in compliance with the Board's Rules Regarding Availability of Information, 12 CFR part 261, and where applicable, the Board's Rules Regarding Access to Personal Information under the Privacy Act of 1974, 12 CFR part 261a.

(f) Within 180 days from the filing of the complaint, or where a complaint was amended, within the earlier of 180 days after the last amendment to the complaint or 360 days after the filing of the original complaint, within the time period contained in an order from the Office of Federal Operations on an appeal from a dismissal, or within any period of extension provided for in paragraph (e) of this section, the Board shall provide the complainant with a copy of the investigative file, and shall notify the complainant that, within 30 days of receipt of the investigative file, the complainant has the right to request a hearing and decision from an administrative judge or may request an immediate final decision pursuant to § 268.109(b) from the Board.

(g) Where the complainant has received the notice required in paragraph (f) of this section or at any time after 180 days have elapsed from the filing of the complaint, the complainant may request a hearing by submitting a written request for a hearing directly to the EEOC office indicated in the Board's

acknowledgment letter. The complainant shall send a copy of the request for a hearing to the Board's EEO Programs Office. Within 15 days of receipt of the request for a hearing, the Board's EEO Programs Office shall provide a copy of the complaint file to EEOC and, if not previously provided, to the complainant.

§ 268.108 Hearings.

(a) When a complainant requests a hearing, the Commission shall appoint an administrative judge to conduct a hearing in accordance with this section. Upon appointment, the administrative judge shall assume full responsibility for the adjudication of the complaint, including overseeing the development of the record. Any hearing will be conducted by an administrative judge or hearing examiner with appropriate security clearances.

(b) *Dismissals.* Administrative judges may dismiss complaints pursuant to § 268.106, on their own initiative, after notice to the parties, or upon the Board's motion to dismiss a complaint.

(c) *Offer of resolution.* (1) Any time after the filing of the written complaint but not later than the date an administrative judge is appointed to conduct a hearing, the Board may make an offer of resolution to a complainant who is represented by an attorney.

(2) Any time after the parties have received notice that an administrative judge has been appointed to conduct a hearing, but not later than 30 days prior to the hearing, the Board may make an offer of resolution to the complainant, whether represented by an attorney or not.

(3) The offer of resolution shall be in writing and shall include a notice explaining the possible consequences of failing to accept the offer. The Board's offer, to be effective, must include attorney's fees and costs and must specify any non-monetary relief. With regard to monetary relief, the Board may make a lump sum offer covering all forms of monetary liability, or it may itemize the amounts and types of monetary relief being offered. The complainant shall have 30 days from receipt of the offer of resolution to accept it. If the complainant fails to accept an offer of resolution and the relief awarded in the administrative judge's decision, the Board's final decision, or the Commission's decision on appeal is not more favorable than the offer, then, except where the interest of justice would not be served, the complainant shall not receive payment from the Board of attorney's fees or costs incurred after the expiration of the 30-day acceptance period. An acceptance of an offer must be in writing and will be timely if postmarked or received within the 30-day period. Where a complainant fails to accept an offer of resolution, the Board may make other offers of resolution and either party may seek to negotiate a settlement of the complaint at any time.

(d) *Discovery.* The administrative judge shall notify the parties of the right to seek discovery prior to the hearing and may issue such discovery orders as are appropriate. Unless the parties agree in writing concerning the methods and scope of discovery, the party seeking discovery shall request authorization from the administrative judge prior to commencing discovery. Both parties are entitled to reasonable development of evidence on matters relevant to the issues raised in the complaint, but the administrative judge may limit the quantity and timing of discovery. Evidence may be developed through interrogatories, depositions, and requests for admissions, stipulations or production of documents. It shall be grounds for objection to producing evidence that the information sought by either party is irrelevant, overburdensome, repetitious, or privileged.

(e) *Conduct of hearing.* The Board shall provide for the attendance at a hearing of all employees approved as witnesses by an administrative judge. Attendance at hearings will be limited to persons determined by the administrative judge to have direct knowledge relating to the complaint. Hearings are part of the investigative process and are thus closed to the public. The administrative judge shall have the power to regulate the conduct of a hearing, limit the number of witnesses where testimony would be repetitious, and exclude any person from the hearing for contumacious conduct or misbehavior that obstructs the hearing. The administrative judge shall receive into evidence information or documents relevant to the complaint. Rules of evidence shall not be applied strictly, but the administrative judge shall exclude irrelevant or repetitious evidence. The administrative judge or the Commission may refer to the Disciplinary Committee of the appropriate Bar Association any attorney or, upon reasonable notice and an opportunity to be heard, suspend or disqualify from representing complainants or agencies in EEOC hearings any representative who refuses to follow the orders of an administrative judge, or who otherwise engages in improper conduct.

(f) *Procedures.* (1) The complainant, the Board and any employee of the Board shall produce such documentary and testimonial evidence as the administrative judge deems necessary. The administrative judge shall serve all orders to produce evidence on both parties.

(2) Administrative judges are authorized to administer oaths. Statements of witnesses shall be made under oath or affirmation or, alternatively, by written statement under penalty of perjury.

(3) When the complainant, or the Board, or its employees fail without good cause shown to respond fully and in timely fashion to an order of an administrative judge, or requests for the investigative file, for documents, records, comparative data, statistics, affidavits, or the attendance of witness(es), the administrative judge shall, in appropriate circumstances:

(i) Draw an adverse inference that the requested information, or the testimony of the requested witness, would have reflected unfavorably on the party refusing to provide the requested information;

(ii) Consider the matters to which the requested information or testimony pertains to be established in favor of the opposing party;

(iii) Exclude other evidence offered by the party failing to produce the requested information or witness;

(iv) Issue a decision fully or partially in favor of the opposing party; or

(v) Take such other actions as appropriate.

(g) *Decisions without hearing.* (1) If a party believes that some or all material facts are not in genuine dispute and there is no genuine issue as to credibility, the party may, at least 15 days prior to the date of the hearing or at such earlier time as required by the administrative judge, file a statement with the administrative judge prior to the hearing setting forth the fact or facts and referring to the parts of the record relied on to support the statement. The statement must demonstrate that there is no genuine issue as to any such material fact. The party shall serve the statement on the opposing party.

(2) The opposing party may file an opposition within 15 days of receipt of the statement in paragraph (g)(1) of this section. The opposition may refer to the record in the case to rebut the statement that a fact is not in dispute or may file an affidavit stating that the party cannot, for reasons stated, present facts to oppose the request. After considering the submissions, the administrative judge may order that discovery be permitted on the fact or facts involved, limit the hearing to the issues remaining in dispute, issue a decision without a

hearing or make such other ruling as is appropriate.

(3) If the administrative judge determines upon his or her own initiative that some or all facts are not in genuine dispute, he or she may, after giving notice to the parties and providing them an opportunity to respond in writing within 15 calendar days, issue an order limiting the scope of the hearing or issue a decision without holding a hearing.

(h) *Record of hearing.* The hearing shall be recorded and the Board shall arrange and pay for verbatim transcripts. All documents submitted to, and accepted by, the administrative judge at the hearing shall be made part of the record of the hearing. If the Board submits a document that is accepted, it shall furnish a copy of the document to the complainant. If the complainant submits a document that is accepted, the administrative judge shall make the document available to the Board's representative for reproduction.

(i) *Decisions by administrative judges.* Unless the administrative judge makes a written determination that good cause exists for extending the time for issuing a decision, an administrative judge shall issue a decision on the complaint, and shall order appropriate remedies and relief where discrimination is found, within 180 days of receipt by the administrative judge of the complaint file from the Board. The administrative judge shall send copies of the hearing record, including the transcript, and the decision to the parties. If the Board does not issue a final order within 40 days of receipt of the administrative judge's decision in accordance with § 268.109(a), then the decision of the administrative judge shall become the final action of the Board.

§ 268.109 Final action by the Board.

(a) *Final action by the Board following a decision by an administrative judge.* When an EEOC administrative judge has issued a decision under §§ 268.108(b), (g), or (i), the Board shall take final action on the complaint by issuing a final order within 40 days of receipt of the hearing file and the administrative judge's decision. The final order shall notify the complainant whether or not the Board will fully implement the decision of the administrative judge and shall contain notice of the complainant's right to appeal to the Equal Employment Opportunity Commission, the right to file a civil action in federal district court, the name of the proper defendant in any such lawsuit and the applicable time limits for appeals and lawsuits. If the final order does not fully implement the decision of the administrative judge, then the Board shall simultaneously file an appeal in accordance with § 268.403 and append a copy of its appeal to the final order. A copy of EEOC Form 573 shall be attached to the final order.

(b) *Final action by the Board in all other circumstances.* When the Board dismisses an entire complaint under § 268.106, receives a request for an immediate final decision or does not receive a reply to the notice issued under § 268.107(f), the Board shall take final action by issuing a final decision. The final decision shall consist of findings by the Board on the merits of each issue in the complaint, or, as appropriate, the rationale for dismissing any claims in the complaint and, when discrimination is found, appropriate remedies and relief in accordance with subpart F of this part. The Board shall issue the final decision within 60 days of receiving notification that a complainant has requested an immediate decision from the Board, or within 60 days of the end of the 30-day period for the complainant to request a hearing or an immediate final decision where the complainant has not requested either a hearing or a decision. The final action shall contain notice of the right to appeal the final action to the Equal Employment Opportunity Commission, the right to file a civil action in federal district court, the name of the proper defendant in any such lawsuit and the applicable time limits for appeals and lawsuits. A copy of EEOC Form 573 shall be attached to the final action. The Board may issue a final decision within 30 days after receiving a decision of the Commission pursuant to § 268.405(c) of this part.

Subpart C—Provisions Applicable to Particular Complaints

§ 268.201 Age Discrimination in Employment Act.

(a) As an alternative to filing a complaint under this part, an aggrieved individual may file a civil action in a United States district court under the ADEA against the Chairman of the Board of Governors after giving the Commission not less than 30 days' notice of the intent to file such an action. Such notice must be filed in writing with EEOC, at PO Box 19848, Washington, DC 20036, or by personal delivery or facsimile within 180 days of the occurrence of the alleged unlawful practice.

(b) The Commission may exempt a position from the provisions of the ADEA if the Commission establishes a maximum age requirement for the position on the basis of a determination that age is a bona fide occupational qualification necessary to the performance of the duties of the position.

(c) When an individual has filed an administrative complaint alleging age discrimination that is not a mixed case, administrative remedies will be considered to be exhausted for purposes of filing a civil action:

(1) 180 days after the filing of an individual complaint if the Board has not taken final action and the individual has not filed an appeal or 180 days after the filing of a class complaint if the Board has not issued a final decision;

(2) After final action on an individual or class complaint if the individual has not filed an appeal; or

(3) After the issuance of a final decision by the Commission on an appeal or 180 days after the filing of an appeal, if the Commission has not issued a final decision.

§ 268.202 Equal Pay Act.

Complaints alleging violations of the Equal Pay Act shall be processed under this part.

§ 268.203 Rehabilitation Act.

(a) *Model employer.* The Board shall be a model employer of individuals with disabilities. The Board shall give full consideration to the hiring, placement, and advancement of qualified individuals with disabilities.

(b) *ADA standards.* The standards used to determine whether section 501 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 791), has been violated in a complaint alleging nonaffirmative action employment discrimination under this part shall be the standards applied under Titles I and V (sections 501 through 504 and 510) of the Americans with Disabilities Act of 1990, as amended (42 U.S.C. 12101, 12111, 12201), as such sections relate to employment. These standards are set forth in the Commission's ADA regulation at 29 CFR part 1630.

§ 268.204 Class complaints.

(a) *Definitions*—(1) *Class* is a group of Board employees, former employees or applicants for employment who, it is alleged, have been or are being adversely affected by a Board personnel management policy or practice that discriminates against the group on the basis of their race, color, religion, sex, national origin, age or disability.

(2) *Class complaint* is a written complaint of discrimination filed on behalf of a class by the agent of the class alleging that:

(i) The class is so numerous that a consolidated complaint of the members of the class is impractical;

(ii) There are questions of fact common to the class;

(iii) The claims of the agent of the class are typical of the claims of the class;

(iv) The agent of the class, or, if represented, the representative, will fairly and adequately protect the interests of the class.

(3) An *agent of the class* is a class member who acts for the class during the processing of the class complaint.

(b) *Pre-complaint processing.* An employee or applicant who wishes to file a class complaint must seek counseling and be counseled in accordance with § 268.104. A complainant may move for class certification at any reasonable point in the process when it becomes apparent that there are class implications to the claim raised in an individual complaint. If a complainant moves for class certification after completing the counseling process contained in § 268.104, no additional counseling is required. The administrative judge shall deny class certification when the complainant has unduly delayed in moving for certification.

(c) *Filing and presentation of a class complaint.* (1) A class complaint must be signed by the agent or representative and must identify the policy or practice adversely affecting the class as well as the specific action or matter affecting the class agent.

(2) The complaint must be filed with the Board not later than 15 days after the agent's receipt of the notice of right to file a class complaint.

(3) The complaint shall be processed promptly; the parties shall cooperate and shall proceed at all times without undue delay.

(d) *Acceptance or dismissal.* (1) Within 30 days of the Board's receipt of a complaint, the Board shall: Designate an agency representative who shall not be one of the individuals referenced in § 268.102(b)(4), and forward the complaint, along with a copy of the Counselor's report and any other information pertaining to timeliness or other relevant circumstances related to the complaint, to the Commission. The Commission shall assign the complaint to an administrative judge or complaints examiner with a proper security clearance when necessary. The administrative judge may require the complainant or the Board to submit additional information relevant to the complaint.

(2) The administrative judge may dismiss the complaint, or any portion, for any of the reasons listed in § 268.106 or because it does not meet the prerequisites of a class complaint under § 268.204(a)(2).

(3) If an allegation is not included in the Counselor's report, the administrative judge shall afford the agent 15 days to state whether the matter was discussed with the Counselor and, if not, explain why it was not discussed. If the explanation is not satisfactory, the administrative judge shall dismiss the allegation. If the explanation is satisfactory, the administrative judge shall refer the allegation to the Board for further counseling of the agent. After counseling, the allegation shall be consolidated with the class complaint.

(4) If an allegation lacks specificity and detail, the administrative judge shall afford the agent 15 days to provide specific and detailed information. The administrative judge shall dismiss the complaint if the agent fails to provide such information within the specified time period. If the information provided contains new allegations outside the scope of the complaint, the administrative judge shall advise the agent how to proceed on an individual or class basis concerning these allegations.

(5) The administrative judge shall extend the time limits for filing a complaint and for consulting with a Counselor in accordance with the time limit extension provisions contained in §§ 268.104(a)(2) and 268.604.

(6) When appropriate, the administrative judge may decide that a class be divided into subclasses and that each subclass be treated as a class, and the provisions of this section then shall be construed and applied accordingly.

(7) The administrative judge shall transmit his or her decision to accept or dismiss a complaint to the Board and the agent. The Board shall take final action by issuing a final order within 40 days of receipt of the hearing record and administrative judge's decision. The final order shall notify the agent whether or not the Board will implement the decision of the administrative judge. If the final order does not implement the decision of the administrative judge, the Board shall simultaneously appeal the administrative judge's decision in accordance with § 268.403 and append a copy of the appeal to the final order. A dismissal of a class complaint shall inform the agent either that the complaint is being filed on that date as an individual complaint of discrimination and will be processed under subpart B or that the complaint is also dismissed as an individual complaint in accordance with § 268.106. In addition, it shall inform the agent of the right to appeal the dismissal of the class complaint to the Equal Employment Opportunity Commission or to file a civil action and shall include EEOC Form 573, Notice of Appeal/Petition.

(e) *Notification.* (1) Within 15 days of receiving notice that the administrative judge has accepted a class complaint or a reasonable time frame specified by the administrative judge, the Board shall use reasonable means, such as delivery, mailing to last known address or distribution, to notify all class members of the acceptance of the class complaint.

(2) Such notice shall contain:

(i) An identification of the Board as the named agency, its location, and the date of acceptance of the complaint;

(ii) A description of the issues accepted as part of the class complaint;

(iii) An explanation of the binding nature of the final decision or resolution of the class complaint on class members; and

(iv) The name, address and telephone number of the class representative.

(f) Obtaining evidence concerning the complaint. (1) The administrative judge shall notify the agent and the Board's representative of the time period that will be allowed both parties to prepare their cases. This time period will include at least 60 days and may be extended by the administrative judge upon the request of either party. Both parties are entitled to reasonable development of evidence on matters relevant to the issues raised in the complaint. Evidence may be developed through interrogatories, depositions, and requests for admissions, stipulations or production of documents. It shall be grounds for objection to producing evidence that the information sought by either party is irrelevant, overburdensome, repetitious, or privileged.

(2) If mutual cooperation fails, either party may request the administrative judge to rule on a request to develop evidence. If a party fails without good cause shown to respond fully and in timely fashion to a request made or approved by the administrative judge for documents, records, comparative data, statistics or affidavits, and the information is solely in the control of one party, such failure may, in appropriate circumstances, cause the administrative judge:

(i) To draw an adverse inference that the requested information would have reflected unfavorably on the party refusing to provide the requested information;

(ii) To consider the matters to which the requested information pertains to be

established in favor of the opposing party;

(iii) To exclude other evidence offered by the party failing to produce the requested information;

(iv) To recommend that a decision be entered in favor of the opposing party; or

(v) To take such other actions as the administrative judge deems appropriate.

(3) During the period for development of evidence, the administrative judge may, in his or her discretion, direct that an investigation of facts relevant to the class complaint or any portion be conducted by an agency certified by the Commission.

(4) Both parties shall furnish to the administrative judge copies of all materials that they wish to be examined and such other material as may be requested.

(g) *Opportunity for resolution of the complaint.* (1) The administrative judge shall furnish the agent and the Board's representative a copy of all materials obtained concerning the complaint and provide opportunity for the agent to discuss the materials with the Board's representative and attempt resolution of the complaint.

(2) The complaint may be resolved by agreement of the Board and the agent at any time pursuant to the notice and approval procedure contained in paragraph (g)(4) of this section.

(3) If the complaint is resolved, the terms of the resolution shall be reduced to writing and signed by the agent and the Board.

(4) Notice of the resolution shall be given to all class members in the same manner as notification of the acceptance of the class complaint and to the administrative judge. It shall state the relief, if any, to be granted by the Board and the name and address of the EEOC administrative judge assigned to the case. It shall state that within 30 days of the date of the notice of resolution, any member of the class may petition the administrative judge to vacate the resolution because it benefits only the class agent, or is otherwise not fair, adequate and reasonable to the class as a whole. The administrative judge shall review the notice of resolution and consider any petitions to vacate filed. If the administrative judge finds that the proposed resolution is not fair, adequate and reasonable to the class as a whole, the administrative judge shall issue a decision vacating the agreement and may replace the original class agent with a petitioner or some other class member who is eligible to be the class agent during further processing of the class complaint. The decision shall inform the former class agent or the petitioner of the right to appeal the decision to the Equal Employment Opportunity Commission and include EEOC Form 573, Notice of Appeal/Petition. If the administrative judge finds that the resolution is fair, adequate and reasonable to the class as a whole, the resolution shall bind all members of the class.

(h) *Hearing.* On expiration of the period allowed for preparation of the case, the administrative judge shall set a date for hearing. The hearing shall be conducted in accordance with 12 CFR 268.108(a) through (f).

(i) *Report of findings and recommendations.* (1) The administrative judge shall transmit to the Board a report of findings and recommendations on the complaint, including a recommended decision, systemic relief for the class and any individual relief, where appropriate, with regard to the personnel action or matter that gave rise to the complaint.

(2) If the administrative judge finds no class relief appropriate, he or she shall determine if a finding of individual discrimination is warranted and, if so, shall recommend appropriate relief.

(3) The administrative judge shall notify the agent of the date on which the report of findings and recommendations was forwarded to the Board.

(j) *Board decision.* (1) Within 60 days of receipt of the report of findings and recommendations issued under § 268.204(i), the Board shall issue a final decision, which shall accept, reject, or modify the findings and recommendations of the administrative judge.

(2) The final decision of the Board shall be in writing and shall be transmitted to the agent by certified mail, return receipt requested, along with a copy of the report of findings and recommendations of the administrative judge.

(3) When the Board's final decision is to reject or modify the findings and recommendations of the administrative judge, the decision shall contain specific reasons for the Board's action.

(4) If the Board has not issued a final decision within 60 days of its receipt of the administrative judge's report of findings and recommendations, those findings and recommendations shall become the final decision. The Board shall transmit the final decision to the agent within five days of the expiration of the 60-day period.

(5) The final decision of the Board shall require any relief authorized by law and determined to be necessary or desirable to resolve the issue of discrimination.

(6) The final decision on a class complaint shall, subject to subpart E of this part, be binding on all members of the class and the Board.

(7) The final decision shall inform the agent of the right to appeal or to file a civil action in accordance with subpart E of this part and of the applicable time limits.

(k) *Notification of decision.* The Board shall notify class members of the final decision and relief awarded, if any, through the same media employed to give notice of the existence of the class complaint. The notice, where appropriate, shall include information concerning the rights of class members to seek individual relief, and of the procedures to be followed. Notice shall be given by the Board within 10 days of the transmittal of its final decision to the agent.

(l) *Relief for individual class members.* (1) When discrimination is found, the Board must eliminate or modify the employment policy or practice out of which the complaint arose and provide individual relief, including an award of attorney's fees and costs, to the agent in accordance with § 268.501.

(2) When class-wide discrimination is not found, but it is found that the class agent is a victim of discrimination, § 268.501 shall apply. The Board shall also, within 60 days of the issuance of the final decision finding no class-wide discrimination, issue the acknowledgment of receipt of an individual complaint as required by § 268.105(d) and process in accordance with the provisions of subpart B of this part, each individual complaint that was subsumed into the class complaint.

(3) When discrimination is found in the final decision and a class member believes that he or she is entitled to individual relief, the class member may file a written claim with the Board or the Board's EEO Programs Director within 30 days of receipt of notification by the Board of its final decision. Administrative judges shall retain jurisdiction over the complaint in order to resolve any disputed claims by class members. The claim must include a specific, detailed showing that the claimant is a class member who was affected by the discriminatory policy or practice, and that this discriminatory action took place within the period of time for which the Board found class-wide discrimination in its final decision. Where a finding of discrimination against a class has been made, there shall be a presumption of discrimination as to each member of the class. The Board must show by clear and convincing evidence that any class

member is not entitled to relief. The administrative judge may hold a hearing or otherwise supplement the record on a claim filed by a class member. The Board or the Commission may find class-wide discrimination and order remedial action for any policy or practice in existence within 45 days of the agent's initial contact with the Counselor. Relief otherwise consistent with this Part may be ordered for the time the policy or practice was in effect. The Board shall issue a final decision on each such claim within 90 days of filing. Such decision must include a notice of the right to file an appeal or a civil action in accordance with subpart E of this part and the applicable time limits.

§ 268.205 Employment of noncitizens.

(a) *Definitions.* The definitions contained in this paragraph (a) shall apply only to this section.

(1) *Intending citizen* means a citizen or national of the United States, or a noncitizen who:

(i) Is a protected individual as defined in 8 U.S.C. 1324b(a)(3); and

(ii) Has evidenced an intention to become a United States citizen.

(2) *Noncitizen* means any person who is not a citizen of the United States.

(3) *Sensitive information* means:

(i)(A) Information that is classified for national security purposes under Executive Order No. 12356 (3 CFR, 1982 Comp., p. 166), including any amendments or superseding orders that the President of the United States may issue from time to time;

(B) Information that consists of confidential supervisory information of the Board, as defined in 12 CFR 261.2(c); or

(C) Information the disclosure or premature disclosure of which to unauthorized persons may be reasonably likely to impair the formulation or implementation of monetary policy, or cause unnecessary or unwarranted disturbances in securities or other financial markets, such that access to such information must be limited to persons who are loyal to the United States.

(ii) For purposes of paragraph (a)(3)(i)(C) of this section, information may not be deemed sensitive information merely because it would be exempt from disclosure under the Freedom of Information Act (5 U.S.C. 552) but sensitive information must be information the unauthorized disclosure or premature disclosure of which may be reasonably likely to impair important functions or operations of the Board.

(4) *Sensitive position* means any position of employment in which the employee will be required to have access to sensitive information.

(b) *Prohibitions*—(1) *Unauthorized aliens.* The Board shall not hire any person unless that person is able to satisfy the requirements of Section 101 of the Immigration Reform and Control Act of 1986.

(2) *Employment in sensitive positions.* The Board shall not hire any person to a sensitive position unless such person is a citizen of the United States or, if a noncitizen, is an intending citizen.

(3) *Preference.* Consistent with the Immigration Reform and Control Act of 1986, and other applicable law, applicants for employment at the Board who are citizens of the United States shall be preferred over equally qualified applicants who are not United States citizens.

(c) *Exception.* The prohibition of paragraph (b)(2) of this section does not apply to hiring for positions for which a security clearance is required under Executive Order No. 10450, including any subsequent amendments or superseding orders that the President of the United States may issue from time to time, where the noncitizen either has or can obtain the necessary security clearance. Any offer of employment authorized by this paragraph (c) shall be contingent upon receipt of the required security clearance in the manner prescribed by law.

(d) *Applicability.* This section applies to employment in all positions at the Board and to employment by Federal Reserve Banks of examiners who must be appointed, or selected and approved by the Board pursuant to 12 U.S.C. 325, 326, 338, or 625.

Subpart D—Related Processes

§ 268.301 Negotiated grievance procedure.

When an employee of the Board, which is not an agency subject to 5 U.S.C. 7121(d), is covered by a negotiated grievance procedure, allegations of discrimination shall be processed as complaints under this part, except that the time limits for processing the complaint contained in § 268.105 and for appeal to the Commission contained in § 268.402 may be held in abeyance during processing of a grievance covering the same matter as the complaint if the Board notifies the complainant in writing that the complaint will be held in abeyance pursuant to this section.

§ 268.302 Mixed case complaints.

A *mixed case complaint* is a complaint of employment discrimination filed with the Board based on race, color, religion, sex, national origin, age or disability related to or stemming from an action that can be appealed to the Merit System Protection Board (MSPB). The complaint may contain only an allegation of employment discrimination or it may contain additional allegations that the MSPB has jurisdiction to address. A *mixed case appeal* is an appeal filed with the MSPB that alleges that an appealable Board action was effected, in whole or in part, because of discrimination on the basis of race, color, religion, sex, national origin, disability or age. Only a Board employee who is a preference eligible employee as defined by the Veterans Preference Act can file a mixed case complaint with the Board or a mixed case appeal with the MSPB. A mixed case complaint or mixed case appeal may only be filed for action(s) over which the MSPB has jurisdiction. The Board will apply sections 1614.302 to 1614.310 of 29 CFR to the processing of a mixed case complaint or mixed case appeal.

Subpart E—Appeals to the Equal Employment Opportunity Commission

§ 268.401 Appeals to the Equal Employment Opportunity Commission.

(a) A complainant may appeal the Board's final action or dismissal of a complaint.

(b) The Board may appeal as provided in § 268.109(a).

(c) A class agent or the Board may appeal an administrative judge's decision accepting or dismissing all or part of a class complaint; a class agent may appeal a final decision on a class complaint; a class member may appeal a final decision on a claim for individual relief under a class complaint; and a class member, a class agent or the Board may appeal a final decision on a petition pursuant to § 268.204(g)(4).

(d) A complainant, agent of the class or individual class claimant may appeal to the Commission the Board's alleged noncompliance with a settlement agreement or final decision in accordance with § 268.504.

§ 268.402 Time for appeals to the Equal Employment Opportunity Commission.

(a) Appeals described in § 268.401(a) and (c) must be filed within 30 days of receipt of the dismissal, final action or decision. Appeals described in § 268.401(b) must be filed within 40 days of receipt of the hearing file and decision. Where a complainant has notified the Board's EEO Programs Director of alleged noncompliance with a settlement agreement in accordance

with § 268.504, the complainant may file an appeal 35 days after service of the allegations of noncompliance, but no later than 30 days after receipt of the Board's determination.

(b) If the complainant is represented by an attorney of record, then the 30-day time period provided in paragraph (a) of this section within which to appeal shall be calculated from the receipt of the required document by the attorney. In all other instances, the time within which to appeal shall be calculated from the receipt of the required document by the complainant.

§ 268.403 How to appeal.

(a) The complainant, the Board, agent or individual class claimant (hereinafter appellant) must file an appeal with the Director, Office of Federal Operations, Equal Employment Opportunity Commission, at PO Box 19848, Washington, DC 20036, or by personal delivery or facsimile. The appellant should use EEOC Form 573, Notice of Appeal/Petition, and should indicate what is being appealed.

(b) The appellant shall furnish a copy of the appeal to the opposing party at the same time it is filed with the Commission. In or attached to the appeal to the Commission, the appellant must certify the date and method by which service was made on the opposing party.

(c) If an appellant does not file an appeal within the time limits of this subpart, the appeal shall be dismissed by the Commission as untimely.

(d) Any statement or brief on behalf of a complainant in support of the appeal must be submitted to the Office of Federal Operations within 30 days of filing the notice of appeal. Any statement or brief on behalf of the Board in support of its appeal must be submitted to the Office of Federal Operations within 20 days filing the notice of appeal. The Office of Federal Operations will accept statements or briefs in support of an appeal by facsimile transmittal, provided they are no more than 10 pages long.

(e) The Board must submit the complaint file to the Office of Federal Operations within 30 days of initial notification that the complainant has filed an appeal or within 30 days of submission of an appeal by the Board.

(f) Any statement or brief in opposition to an appeal must be submitted to the Commission and served on the opposing party within 30 days of receipt of the statement or brief supporting the appeal, or, if no statement or brief supporting the appeal is filed, within 60 days of receipt of the appeal. The Office of Federal Operations will accept statements or briefs in opposition to an appeal by facsimile provided they are no more than 10 pages long.

§ 268.404 Appellate Procedure.

(a) On behalf of the Commission, the Office of Federal Operations shall review the complaint file and all written statements and briefs from either party. The Commission may supplement the record by an exchange of letters or memoranda, investigation, remand to the Board or other procedures.

(b) If the Office of Federal Operations requests information from one or both of the parties to supplement the record, each party providing information shall send a copy of the information to the other party.

(c) When either party to an appeal fails without good cause shown to comply with the requirements of this section or to respond fully and in timely fashion to requests for information, the Office of Federal Operations shall, in appropriate circumstances:

(1) Draw an adverse inference that the requested information would have reflected unfavorably on the party refusing to provide the requested information;

(2) Consider the matters to which the requested information or testimony pertains to be established in favor of the opposing party;

(3) Issue a decision fully or partially in favor of the opposing party; or

(4) Take such other actions as appropriate.

§ 268.405 Decisions on appeals.

(a) The Office of Federal Operations, on behalf of the Commission, shall issue a written decision setting forth its reasons for the decision. The Commission shall dismiss appeals in accordance with §§ 268.106, 268.403(c) and 268.408. The decision on an appeal from the Board's final action shall be based on a de novo review, except that the review of the factual findings in a decision by an administrative judge issued pursuant to § 268.108(i) shall be based on a substantial evidence standard of review. If the decision contains a finding of discrimination, appropriate remedy(ies) shall be included and, where appropriate, the entitlement to interest, attorney's fees or costs shall be indicated. The decision shall reflect the date of its issuance, inform the complainant of his or her civil action rights, and be transmitted to the complainant and the Board by first class mail.

(b) A decision issued under paragraph (a) of this section is final, subject to paragraph (c) of this section, within the meaning of § 268.406 unless the Commission reconsiders the case. A party may request reconsideration within 30 days of receipt of a decision of the Commission, which the Commission in its discretion may grant, if the party demonstrates that:

(1) The appellate decision involved a clearly erroneous interpretation of material fact or law; or

(2) The decision will have a substantial impact on the policies, practices or operations of the Board.

(c) The Board, within 30 days of receiving the decision of the Commission, shall issue a final decision based upon that decision.

§ 268.406 Civil action: Title VII, Age Discrimination in Employment Act and Rehabilitation Act.

A complainant who has filed an individual complaint, an agent who has filed a class complaint or a claimant who has filed a claim for individual relief pursuant to a class complaint is authorized under title VII, the ADEA and the Rehabilitation Act to file a civil action in an appropriate United States District Court:

(a) Within 90 days of receipt of the final action on an individual or class complaint if no appeal has been filed;

(b) After 180 days from the date of filing an individual or class complaint if an appeal has not been filed and final action has not been taken;

(c) Within 90 days of receipt of the Commission's final decision on an appeal; or

(d) After 180 days from the date of filing an appeal with the Commission if there has been no final decision by the Commission.

§ 268.407 Civil action: Equal Pay Act.

A complainant is authorized under section 16(b) of the Fair Labor Standards Act (29 U.S.C. 216(b)) to file a civil action in a court of competent jurisdiction within two years or, if the violation is willful, three years of the date of the alleged violation of the Equal Pay Act regardless of whether he or she pursued any administrative complaint processing. Recovery of back wages is limited to two years prior to the date of filing suit, or to three years if the violation is deemed willful; liquidated damages in an equal amount may also be awarded. The filing of a complaint or appeal under this part shall not toll the time for filing a civil action.

§ 268.408 Effect of filing a civil action.

Filing a civil action under §§ 268.406 or 268.407 shall terminate Commission processing of the appeal. If private suit is filed subsequent to the filing of an

appeal, the parties are requested to notify the Commission in writing.

Subpart F—Remedies and Enforcement

§ 268.501 Remedies and relief.

(a) When the Board, or the Commission, in an individual case of discrimination, finds that an applicant or an employee has been discriminated against, the Board shall provide full relief which shall include the following elements in appropriate circumstances:

(1) Notification to all employees of the Board in the affected facility of their right to be free of unlawful discrimination and assurance that the particular types of discrimination found will not recur;

(2) Commitment that corrective, curative or preventive action will be taken, or measures adopted, to ensure that violations of the law similar to those found unlawful will not recur;

(3) An unconditional offer to each identified victim of discrimination of placement in the position the person would have occupied but for the discrimination suffered by that person, or a substantially equivalent position;

(4) Payment to each identified victim of discrimination on a make whole basis for any loss of earnings the person may have suffered as a result of the discrimination; and

(5) Commitment that the Board shall cease from engaging in the specific unlawful employment practice found in the case.

(b) *Relief for an applicant.* (1)(i) When the Board, or the Commission, finds that an applicant for employment has been discriminated against, the Board shall offer the applicant the position that the applicant would have occupied absent discrimination or, if justified by the circumstances, a substantially equivalent position unless clear and convincing evidence indicates that the applicant would not have been selected even absent the discrimination. The offer shall be made in writing. The individual shall have 15 days from receipt of the offer within which to accept or decline the offer. Failure to accept the offer within the 15-day period will be considered a declination of the offer, unless the individual can show that circumstances beyond his or her control prevented a response within the time limit.

(ii) If the offer is accepted, appointment shall be retroactive to the date the applicant would have been hired. Back pay, computed in the manner prescribed in 5 CFR 550.805, shall be awarded from the date the individual would have entered on duty until the date the individual actually enters on duty unless clear and convincing evidence indicates that the applicant would not have been selected even absent discrimination. Interest on back pay shall be included in the back pay computation where sovereign immunity has been waived. The individual shall be deemed to have performed service for the Board during this period for all purposes except for meeting service requirements for completion of a required probationary or trial period.

(iii) If the offer of employment is declined, the Board shall award the individual a sum equal to the back pay he or she would have received, computed in the manner prescribed in 5 CFR 550.805, from the date he or she would have been appointed until the date the offer was declined, subject to the limitation of paragraph (b)(3) of this section. Interest on back pay shall be included in the back pay computation. The Board shall inform the applicant, in its offer of employment, of the right to this award in the event the offer is declined.

(2) When the Board, or the Commission, finds that discrimination existed at the time the applicant was considered for employment but also finds by clear and convincing evidence that the applicant would not have been hired even absent discrimination, the Board shall nevertheless take all steps necessary to eliminate the discriminatory practice and ensure it does not recur.

(3) Back pay under this paragraph (b) for complaints under title VII or the Rehabilitation Act may not extend from a date earlier than two years prior to the date on which the complaint was initially filed by the applicant.

(c) *Relief for an employee.* When the Board, or the Commission, finds that an employee of the Board was discriminated against, the Board shall provide relief, which shall include, but need not be limited to, one or more of the following actions:

(1) Nondiscriminatory placement, with back pay computed in the manner prescribed in 5 CFR 550.805, unless clear and convincing evidence contained in the record demonstrates that the personnel action would have been taken even absent the discrimination. Interest on back pay shall be included in the back pay computation where sovereign immunity has been waived. The back pay liability under title VII or the Rehabilitation Act is limited to two years prior to the date the discrimination complaint was filed.

(2) If clear and convincing evidence indicates that, although discrimination existed at the time the personnel action was taken, the personnel action would have been taken even absent discrimination, the Board shall nevertheless eliminate any discriminatory practice and ensure it does not recur.

(3) Cancellation of an unwarranted personnel action and restoration of the employee.

(4) Expunction from the Board's records of any adverse materials relating to the discriminatory employment practice.

(5) Full opportunity to participate in the employee benefit denied (*e.g.*, training, preferential work assignments, overtime scheduling).

(d) The Board has the burden of proving by a preponderance of the evidence that the complainant has failed to mitigate his or her damages.

(e) *Attorney's fees or costs*—(1) *Awards of attorney's fees or costs.* The provisions of this paragraph relating to the award of attorney's fees or costs shall apply to allegations of discrimination prohibited by title VII and the Rehabilitation Act. In a decision or final action, the Board, administrative judge, or Commission may award the applicant or employee or reasonable attorney's fees (including expert witness fees) and other costs incurred in the processing of the complaint.

(i) A finding of discrimination raises a presumption of entitlement to an award of attorney's fees.

(ii) Any award of attorney's fees or costs shall be paid by the Board.

(iii) Attorney's fees are allowable only for the services of members of the Bar and law clerks, paralegals or law students under the supervision of members of the Bar, except that no award is allowable for the services of any employee of the Federal Government.

(iv) Attorney's fees shall be paid for services performed by an attorney after the filing of a written complaint, provided that the attorney provides reasonable notice of representation to the Board, administrative judge or Commission, except that fees are allowable for a reasonable period of time prior to the notification of representation for any services performed in reaching a determination to represent the complainant. The Board is not required to pay attorney's fees for services performed during the pre-complaint process, except that fees are allowable when the Commission affirms on appeal an administrative judge's decision finding discrimination after the Board takes final action by not implementing an administrative judge's decision. Written submissions to the

Board that are signed by the representative shall be deemed to constitute notice of representation.

(2) *Amount of awards.* (i) When the Board, administrative judge or the Commission determines an entitlement to attorney's fees or costs, the complainant's attorney shall submit a verified statement of attorney's fees (including expert witness fees) and other costs, as appropriate, to the Board or administrative judge within 30 days of receipt of the decision and shall submit a copy of the statement to the Board. A statement of attorney's fees and costs shall be accompanied by an affidavit executed by the attorney of record itemizing the attorney's charges for legal services. The Board may respond to a statement of attorney's fees and costs within 30 days of its receipt. The verified statement, accompanying affidavit and any Board response shall be made a part of the complaint file.

(ii)(A) The Board or administrative judge shall issue a decision determining the amount of attorney's fees or costs due within 60 days of receipt of the statement and affidavit. The decision shall include a notice of right to appeal to the EEOC along with EEOC Form 573, Notice of Appeal/Petition and shall include the specific reasons for determining the amount of the award.

(B) The amount of attorney's fees shall be calculated using the following standards: The starting point shall be the number of hours reasonably expended multiplied by a reasonable hourly rate. There is a strong presumption that this amount represents the reasonable fee. In limited circumstances, this amount may be reduced or increased in consideration of the degree of success, quality of representation, and long delay caused by the Board.

(C) The costs that may be awarded are those authorized by 28 U.S.C. 1920 to include: Fees of the reporter for all or any of the stenographic transcript necessarily obtained for use in the case; fees and disbursements for printing and witnesses; and fees for exemplification and copies necessarily obtained for use in the case.

(iii) Witness fees shall be awarded in accordance with the provisions of 28 U.S.C. 1821, except that no award shall be made for a Federal employee who is in a duty status when made available as a witness.

§ 268.502 Compliance with final Commission decisions.

(a) Relief ordered in a final Commission decision, if accepted pursuant to § 268.405(c) as a final decision, or not acted upon the Board within the time periods of § 268.405(c), is mandatory and binding on the Board except as provided in this section. Failure to implement ordered relief shall be subject to judicial enforcement as specified in § 268.503(f).

(b) Notwithstanding paragraph (a) of this section, when the Board requests reconsideration and the case involves removal, separation, or a suspension continuing beyond the date of the request for reconsideration, and when the decision orders retroactive restoration, the Board shall comply with the decision to the extent of the temporary or conditional restoration of the employee to duty status in the position specified by the Commission, pending the outcome of the Board's request for reconsideration.

(1) Service under the temporary or conditional restoration provisions of this paragraph (b) shall be credited toward the completion of a probationary or trial period or the completion of the service requirement for career tenure, if the Commission upholds its decision after reconsideration.

(2) When the Board requests reconsideration, it may delay the payment of any amounts ordered to be paid to the complainant until after the request for reconsideration is resolved. If the Board delays payment of any amount pending the outcome of the request to reconsider and the resolution of the request requires the Board to make the payment, then the Board shall pay interest from the date of the original appellate decision until payment is made.

(3) The Board shall notify the Commission and the employee in writing at the same time it requests reconsideration that the relief it provides is temporary or conditional and, if applicable, that it will delay the payment of any amounts owed but will pay interest as specified in paragraph (b)(2) of this section. Failure of the Board to provide notification will result in the dismissal of the Board's request.

(c) When no request for reconsideration is filed or when a request for reconsideration is denied, the Board shall provide the relief ordered and there is no further right to delay implementation of the ordered relief. The relief shall be provided in full not later than 60 days after receipt of the final decision unless otherwise ordered in the decision.

§ 268.503 Enforcement of final EEOC decisions.

(a) *Petition for enforcement.* A complainant may petition the Commission for enforcement of a decision issued under the Commission's appellate jurisdiction. The petition shall be submitted to the Office of Federal Operations. The petition shall specifically set forth the reasons that lead the complainant to believe that the Board is not complying with the decision.

(b) *Compliance.* On behalf of the Commission, the Office of Federal Operations shall take all necessary action to ascertain whether the Board is implementing the decision of the Commission. If the Board is found not to be in compliance with the decision, efforts shall be undertaken to obtain compliance.

(c) *Clarification.* On behalf of the Commission, the Office of Federal Operations may, on its own motion or in response to a petition for enforcement or in connection with a timely request for reconsideration, issue a clarification of a prior decision. A clarification cannot change the result of a prior decision or enlarge or diminish the relief ordered but may further explain the meaning or intent of the prior decision.

(d) *Referral to the Commission.* Where the Director, Office of Federal Operations, is unable to obtain satisfactory compliance with the final decision, the Director shall submit appropriate findings and recommendations for enforcement to the Commission, or, as directed by the Commission, refer the matter to another appropriate agency.

(e) *Commission notice to show cause.* The Commission may issue a notice to the Chairman of the Board to show cause why there is noncompliance. Such notice may request the Chairman of the Board or a representative to appear before the Commission or to respond to the notice in writing with adequate evidence of compliance or with compelling reasons for noncompliance.

(f) *Notification to complainant of completion of administrative efforts.* Where the Commission has determined that the Board is not complying with a prior decision, or where the Board has failed or refused to submit any required report of compliance, the Commission shall notify the complainant the right to file a civil action for enforcement of the decision pursuant to title VII, the ADEA, the Equal Pay Act or the Rehabilitation Act and to seek judicial review of the Board's refusal to implement the ordered relief pursuant to the Administrative Procedures Act, 5 U.S.C. 701 *et seq.*, and the mandamus statute, 28 U.S.C. 1361, or to commence *de novo* proceedings pursuant to the appropriate statutes.

§ 268.504 Compliance with settlement agreements and final actions.

(a) Any settlement agreement knowingly and voluntarily agreed to by the parties, reached at any stage of the complaint process, shall be binding on both parties. Final action that has not been the subject of an appeal or a civil action shall be binding on the Board. If the complainant believes that the Board has failed to comply with the terms of a settlement agreement or decision, the complainant shall notify the Board's EEO Programs Director, in writing, of the alleged noncompliance within 30 days of when the complainant knew or should have known of the alleged noncompliance. The complainant may request that the terms of the settlement agreement be specifically implemented or, alternatively, that the complaint be reinstated for further processing from the point processing ceased.

(b) The Board shall resolve the matter and respond to the complainant, in writing. If the Board has not responded to the complainant, in writing, or if the complainant is not satisfied with the Board's attempt to resolve the matter, the complainant may appeal to the Commission for a determination as to whether the Board has complied with the terms of the settlement agreement or decision. The complainant may file such an appeal 35 days after he or she has served the Board with the allegations of noncompliance, but must file an appeal within 30 days of his or her receipt of the Board's determination. The complainant must serve a copy of the appeal on the Board and the Board may submit a response to the Commission within 30 days of receiving notice of the appeal.

(c) Prior to rendering its determination, the Commission may request that the parties submit whatever additional information or documentation it deems necessary or may direct that an investigation or hearing on the matter be conducted. If the Commission determines that the Board is not in compliance and the noncompliance is not attributable to acts or conduct of the complainant, it may order such compliance or it may order that the complaint be reinstated for further processing from the point processing ceased. Allegations that subsequent acts of discrimination violate a settlement agreement shall be processed as separate complaints under §§ 268.105 or 268.204, as appropriate, rather than under this section.

§ 268.505 Interim relief.

(a)(1) When the Board appeals and the case involves removal, separation, or suspension continuing beyond the date of the appeal, and when the administrative judge orders retroactive restoration, the Board shall comply with the decision to the extent of the temporary or conditional restoration of the employee to duty status in the position specified in the decision, pending the outcome of the Board appeal. The employee may decline the offer of interim relief.

(2) Service under the temporary or conditional restoration provisions of paragraph (a)(1) of this section shall be credited toward the completion of a probationary or trial period, eligibility for a within-grade increase, or the completion of the service requirement for career tenure, if the Commission upholds the decision on appeal. Such service shall not be credited toward the completion of any applicable probationary or trial period or the completion of the service requirement for career tenure if the Commission reverses the decision on appeal.

(3) When the Board appeals, it may delay the payment of any amount, other than prospective pay and benefits, ordered to be paid to the complainant until after the appeal is resolved. If the Board delays payment of any amount pending the outcome of the appeal and the resolution of the appeal requires the Board to make the payment, then the Board shall pay interest from the date of the original decision until payment is made.

(4) The Board shall notify the Commission and the employee in writing at the same time it appeals that the relief it provides is temporary or conditional and, if applicable, that it will delay the payment of any amounts owed but will pay interest as specified in paragraph (b)(2) of this section. Failure of the Board to provide notification will result in the dismissal of the Board's appeal.

(5) The Board may, by notice to the complainant, decline to return the complainant to his or her place of employment if it determines that the return or presence of the complainant will be unduly disruptive to the work environment. However, prospective pay and benefits must be provided. The determination not to return the complainant to his or her place of employment is not reviewable. A grant of interim relief does not insulate a complainant from subsequent disciplinary or adverse action.

(b) If the Board files an appeal and has not provided required interim relief, the complainant may request dismissal of the Board's appeal. Any such request must be filed with the Office of Federal Operations within 25 days of the date of service of the Board's appeal. A copy of the request must be served on the Board at the same time it is filed with EEOC. The Board may respond with evidence and argument to the complainant's request to dismiss within 15 days of the date of service of the request.

Subpart G—Matters of General Applicability

§ 268.601 EEO group statistics.

(a) The Board shall establish a system to collect and maintain accurate employment information on the race, national origin, sex and disability(ies) of its employees.

(b) Data on race, national origin and sex shall be collected by voluntary self-identification. If an employee does not voluntarily provide the requested information, the Board shall advise the employee of the importance of the data and of the Board's obligation to report it. If the employee still refuses to provide the information, the Board must make a visual identification and inform the employee of the data it will be reporting. If the Board believes that information provided by an employee is inaccurate, the Board shall advise the employee about the solely statistical purpose for which the data is being collected, the need for accuracy, the Board's recognition of the sensitivity of the information and the existence of procedures to prevent its unauthorized disclosure. If, thereafter, the employee declines to change the apparently inaccurate self identification, the Board must accept it.

(c) Subject to applicable law, the information collected under paragraph (b) of this section shall be disclosed only in the form of gross statistics. The Board shall not collect or maintain any information on the race, national origin or sex of individual employees except in accordance with applicable law and when an automated data processing system is used in accordance with standards and requirements prescribed by the Commission to insure individual privacy and the separation of that information from personnel records.

(d) The Board's system is subject to the following controls:

(1) Only those categories of race and national origin prescribed by the Commission may be used;

(2) Only the specific procedures for the collection and maintenance of data that are prescribed or approved by the Commission may be used.

(e) The Board may use the data only in studies and analyses which contribute affirmatively to achieving the objectives of the Board's equal employment opportunity program. The Board shall not establish a quota for the

employment of persons on the basis of race, color, religion, sex, or national origin.

(f) Data on disabilities shall also be collected by voluntary self-identification. If an employee does not voluntarily provide the requested information, the Board shall advise the employee of the importance of the data and of the Board's obligation to report it. If an employee who has been appointed pursuant to a special Board program for hiring individuals with a disability still refuses to provide the requested information, the Board must identify the employee's disability based upon the records supporting the appointment. If any other employee still refuses to provide the requested information or provides information that the Board believes to be inaccurate, the Board should report the employee's disability status as unknown.

(g) The Board shall report to the Commission on employment by race, national origin, sex and disability in the form and at such times as the Board and Commission shall agree.

§ 268.602 Reports to the Commission.

(a) The Board shall report to the Commission information concerning pre-complaint counseling and the status, processing, and disposition of complaints under this part at such times and in such manner as the Board and Commission shall agree.

(b) The Board shall advise the Commission whenever it is served with a Federal court complaint based upon a complaint that is pending on appeal at the Commission.

(c) The Board shall submit annually for the review and approval of the Commission written equal employment opportunity plans of action. Plans shall be submitted in the format prescribed by the Commission and shall include, but not be limited to:

(1) Provision for the establishment of training and education programs designed to provide maximum opportunity for employees to advance so as to perform at their highest potential;

(2) Description of the qualifications, in terms of training and experience relating to equal employment opportunity, of the principal and operating officials concerned with administration of the Board's equal employment opportunity program; and

(3) Description of the allocation of personnel and resources proposed by the Board to carry out its equal employment opportunity program.

§ 268.603 Voluntary settlement attempts.

The Board shall make reasonable efforts to voluntarily settle complaints of discrimination as early as possible in, and throughout, the administrative processing of complaints, including the pre-complaint counseling stage. Any settlement reached shall be in writing and signed by both parties and shall identify the claims resolved.

§ 268.604 Filing and computation of time.

(a) All time periods in this part that are stated in terms of days are calendar days unless otherwise stated.

(b) A document shall be deemed timely if it is received or postmarked before the expiration of the applicable filing period, or, in the absence of a legible postmark, if it is received by mail within five days of the expiration of the applicable filing period.

(c) The time limits in this part are subject to waiver, estoppel and equitable tolling.

(d) The first day counted shall be the day after the event from which the time period begins to run and the last day of the period shall be included, unless it falls on a Saturday, Sunday or Federal holiday, in which case the period shall be extended to include the next business day.

§ 268.605 Representation and official time.

(a) At any stage in the processing of a complaint, including the counseling stage under § 268.104, the complainant shall have the right to be accompanied, represented, and advised by a representative of complainant's choice.

(b) If the complainant is an employee of the Board, he or she shall have a reasonable amount of official time, if otherwise on duty, to prepare the complaint and to respond to Board and EEOC requests for information. If the complainant is an employee of the Board and he designates another employee of the Board as his or her representative, the representative shall have a reasonable amount of official time, if otherwise on duty, to prepare the complaint and respond to Board and EEOC requests for information. The Board is not obligated to change work schedules, incur overtime wages, or pay travel expenses to facilitate the choice of a specific representative or to allow the complainant and representative to confer. The complainant and the representative, if employed by the Board and otherwise in a pay status, shall be on official time, regardless of their tour of duty, when their presence is authorized or required by the Board or the Commission during the investigation, informal adjustment, or hearing on the complaint.

(c) In cases where the representation of a complainant or the Board would conflict with the official or collateral duties of the representative, the Commission or the Board may, after giving the representative an opportunity to respond, disqualify the representative.

(d) Unless the complainant states otherwise in writing, after the Board has received written notice of the name, address and telephone number of a representative for the complainant, all official correspondence shall be with the representative with copies to the complainant. When the complainant designates an attorney as representative, service of all official correspondence shall be made on the attorney and the complainant, but time frames for receipt of material shall be computed from the time of receipt by the attorney. The complainant must serve all official correspondence on the designated representative of the Board.

(e) The complainant shall at all times be responsible for proceeding with the complaint whether or not he or she has designated a representative.

(f) Witnesses who are Board employees shall be in a duty status when their presence is authorized or required by Commission or Board officials in connection with a complaint.

§ 268.606 Joint processing and consolidation of complaints.

Complaints of discrimination filed by two or more complainants consisting of substantially similar allegations of discrimination or relating to the same matter may be consolidated by the Board or the Commission for joint processing after appropriate notification to the parties. Two or more complaints of discrimination filed by the same complainant shall be consolidated by the Board for joint processing after appropriate notification to the complainant. When a complaint has been consolidated with one or more earlier filed complaints, the Board shall complete its investigation within the earlier of 180 days after the filing of the last complaint or 360 days after the filing of the original complaint, except that the complainant may request a hearing from an administrative judge on the consolidated complaints any time after 180 days from the date of the first filed complaint. Administrative judges or the Commission may, in their discretion, consolidate two or more complaints of discrimination filed by the same complainant.

§ 268.607 Delegation of authority.

The Board of Governors may delegate authority under this part, to one or more designees.

Subpart H—Prohibition Against Discrimination in Board Programs and Activities Because of Physical or Mental Disability

§ 268.701 Purpose and application.

(a) *Purpose.* The purpose of this subpart H is to prohibit discrimination on the basis of a disability in programs or activities conducted by the Board.

(b) *Application.* (1) This subpart H applies to all programs and activities conducted by the Board. Such programs and activities include:

(i) Holding open meetings of the Board or other meetings or public hearings at the Board's office in Washington, DC;

(ii) Responding to inquiries, filing complaints, or applying for employment at the Board's office;

(iii) Making available the Board's library facilities; and

(iv) Any other lawful interaction with the Board or its staff in any official matter with people who are not employees of the Board.

(2) This subpart H does not apply to Federal Reserve Banks or to financial institutions or other companies supervised or regulated by the Board.

§ 268.702 Definitions.

For purposes of this subpart, the following definitions apply:

(a) *Auxiliary aids* means services or devices that enable persons with impaired sensory, manual, or speaking skills to have an equal opportunity to participate in, and enjoy the benefits of, programs or activities conducted by the Board. For example, auxiliary aids useful for persons with impaired vision include readers, Brailled materials, audio recordings, telecommunications devices and other similar services and devices. Auxiliary aids useful for persons with impaired hearing include telephone handset amplifiers, telephones compatible with hearing aids, telecommunication devices for deaf persons (TDD's), interpreters, notetakers, written materials, and other similar services and devices.

(b) *Complete complaint* means a written statement that contains the complainant's name and address and describes the Board's alleged discriminatory action in sufficient detail to inform the Board of the nature and date of the alleged violation. It shall be signed by the complainant or by someone authorized to do so on his or her behalf. Complaints filed on behalf of classes or third parties shall describe or identify (by name, if possible) the alleged victims of discrimination.

(c) *Facility* means all or any portion of buildings, structures, equipment, roads, walks, parking lots, rolling stock or other conveyances, or other real or personal property.

(d) *Person with a disability* means any person who has a physical or mental impairment that substantially limits one or more major life activities, has a record of such an impairment, or is regarded as having such an impairment. As used in this definition, the phrase:

(1) Physical or mental impairment includes—

(i) Any physiological disorder or condition, cosmetic disfigurement, or anatomical loss affecting one of more of the following body systems: Neurological; musculoskeletal; special sense organs; respiratory, including speech organs; cardiovascular; reproductive; digestive; genitourinary; hemic and lymphatic; skin; and endocrine; or

(ii) Any mental or psychological disorder, such as mental retardation, organic brain syndrome, emotional or mental illness, and specific learning disabilities. The term physical or mental impairment includes, but is not limited to, such diseases and conditions as orthopedic, visual, speech, and hearing impairments, cerebral palsy, epilepsy, muscular dystrophy, multiple sclerosis, cancer, heart disease, diabetes, mental retardation, emotional illness, and drug addiction and alcoholism.

(2) Major life activities includes functions such as caring for one's self, performing manual tasks, walking, seeing, hearing, speaking, breathing, learning, and working.

(3) Has a record of such an impairment means has a history of, or has been misclassified as having, a mental or physical impairment that substantially limits one or more major life activities.

(4) Is regarded as having an impairment means—

(i) Has a physical or mental impairment that does not substantially limit major life activities but is treated by the Board as constituting such a limitation;

(ii) Has a physical or mental impairment that substantially limits major life activities only as a result of the attitudes of others toward such impairment; or

(iii) Has none of the impairments defined in paragraph (d)(1) of this section but is treated by Board as having such an impairment.

(e) *Qualified person with a disability* means—

(1) With respect to any Board program or activity under which a person is required to perform services or to achieve a level of accomplishment, a person with a disability who meets the essential eligibility requirements and who can achieve the purpose of the program or activity without modifications in the program or activity that the Board can demonstrate would result in a fundamental alteration in its nature; or

(2) With respect to any other program or activity, a person with a disability who meets the essential eligibility requirements for participation in, or receipt of benefits from, that program or activity.

(3) Qualified individual with a disability is defined for purposes of employment in § 268.203 of this part, which is made applicable to this subpart by § 268.705.

§ 268.703 Notice.

The Board shall make available to employees, applicants for employment, participants, beneficiaries, and other interested persons information regarding the provisions of this subpart and its applicability to the programs and activities conducted by the Board, and make this information available to them in such manner as the Board finds necessary to apprise such persons of the protections against discrimination assured them by this subpart.

§ 268.704 General prohibitions against discrimination.

(a) No qualified individual with a disability shall, on the basis of a disability, be excluded from participation in, be denied the benefits of, or otherwise be subjected to discrimination in any program or activity conducted by the Board.

(b)(1) The Board, in providing any aid, benefit, or service, may not, directly or through contractual, licensing, or other arrangements, on the basis of a disability:

(i) Deny a qualified individual with a disability the opportunity to participate in or benefit from the aid, benefit, or service that is not equal to that provided to others;

(ii) Afford a qualified individual with a disability an opportunity to participate in or benefit from the aid, benefit, or service that is not equal to that afforded others;

(iii) Provide a qualified individual with a disability with an aid, benefit, or service that is not as effective in affording equal opportunity to obtain the same result, to gain the same benefit, or to reach the same level of achievement as that provided to others;

(iv) Provide different or separate aid, benefits, or services to individuals with a disability or to any class of individuals with a disability than is provided to others unless such action is necessary to provide qualified individuals with a disability with aid, benefits, or services that are as effective as those provided to others;

(v) Deny a qualified individual with a disability the opportunity to participate as a member of planning or advisory boards; or

(vi) Otherwise limit a qualified individual with a disability in the enjoyment of any right, privilege, advantage, or opportunity enjoyed by others receiving the aid, benefit, or service.

(2) The Board may not deny a qualified individual with a disability the opportunity to participate in programs or activities that are not separate or different, despite the existence of permissibly separate or different programs or activities.

(3) The Board may not, directly or through contractual or other arrangements, utilize criteria or methods of administration, the purpose or effect of which would:

(i) Subject qualified individuals with a disability to discrimination on the basis of a disability; or

(ii) Defeat or substantially impair accomplishment of the objectives of a program or activity with respect to individuals with a disability.

(4) The Board may not, in determining the site or location of a facility, make selections the purpose or effect of which would:

(i) Exclude individuals with a disability from, deny them the benefits of, or otherwise subject them to discrimination under any program or activity conducted by the Board; or

(ii) Defeat or substantially impair the accomplishment of the objectives or a program or activity with respect to individuals with a disability.

(5) The Board, in the selection of procurement contractors, may not use criteria that subject qualified individuals with a disability to discrimination on the basis of a disability.

(6) The Board may not administer a licensing or certification program in a manner that subjects qualified individuals with a disability to discrimination on the basis of a disability, nor may the Board establish requirements for the programs and activities of licensees or certified entities that subject qualified individuals with a disability to discrimination on the basis of a disability. However, the programs and activities of entities that are licensed or certified by the Board are not, themselves, covered by this subpart.

(c) The exclusion of individuals who do not have a disability from the benefits of a program limited by Federal statute or Board order to individuals with a disability or the exclusion of a specific class of individuals with a disability from a program limited by Federal statute or Board order to a different class of individuals with a disability is not prohibited by this subpart.

(d) The Board shall administer programs and activities in the most integrated setting appropriate to the needs of qualified individuals with a disability.

§ 268.705 Employment.

No qualified individual with a disability shall, on the basis of a disability, be subjected to discrimination in employment under any program or activity conducted by the Board. The definitions, requirements and procedures of § 268.203 of this part shall apply to discrimination in employment in federally conducted programs or activities.

§ 268.706 Program accessibility: Discrimination prohibited.

Except as otherwise provided in § 268.707 of this subpart, no qualified individual with a disability shall, because the Board's facilities are inaccessible to or unusable by individuals with a disability, be denied the benefits of, be excluded from participation in, or otherwise be subjected to discrimination under any program or activity conducted by the Board.

§ 268.707 Program accessibility: Existing facilities.

(a) *General.* The Board shall operate each program or activity so that the program or activity, when viewed in its entirety, is readily accessible to and usable by individuals with a disability. This paragraph (a) does not:

(1) Necessarily require the Board to make each of its existing facilities accessible to and usable by individuals with a disability; or

(2) Require the Board to take any action that it can demonstrate would result in a fundamental alteration in the nature of a program or activity or in undue financial and administrative burdens. In those circumstances where the Board believes that the proposed action would fundamentally alter the program or activity or would result in undue financial and administrative burdens, the Board has the burden of proving that compliance with this paragraph (a) would result in such alterations or burdens. The decision that compliance would result in such alterations or burdens shall be made by the Board of Governors or their designee after considering all Board resources available for use in the funding and operation of the conducted program or activity, and must be accompanied by a written statement of the reasons for reaching that conclusion. If an action would result in such an alteration or such burdens, the Board shall take any other action that would not result in such an alteration or such burdens but would nevertheless ensure that individuals with a disability receive the benefits and services of the program or activity.

(b) *Methods.* The Board may comply with the requirements of this subpart H through such means as redesign of equipment, reassignment of services to accessible buildings, assignment of aides to individuals with a disability, home visits, delivery of service at alternate accessible sites, alteration of existing facilities and construction of new facilities, use of accessible rolling stock, or any other methods that result in making its programs or activities readily accessible to and usable by individuals with a disability. The Board is not required to make structural changes in existing facilities where other methods are effective in achieving compliance with this section. In choosing among available methods for meeting the requirements of this section, the Board shall give priority to those methods that offer programs and activities to qualified individuals with a disability in the most integrated setting appropriate.

(c) *Time period for compliance.* The Board shall comply with any obligations established under this section as expeditiously as possible.

§ 268.708 Program accessibility: New construction and alterations.

Each building or part of a building that is constructed or altered by, on behalf of, or for the use of the Board shall be designed, constructed, or altered so as to be readily accessible to and usable by individuals with a disability.

§ 268.709 Communications.

(a) The Board shall take appropriate steps to ensure effective communication with applicants, participants, personnel of other Federal entities, and members of the public.

(1) The Board shall furnish appropriate auxiliary aids where necessary to afford an individual with a

disability an equal opportunity to participate in, and enjoy the benefits of, a program or activity conducted by the Board.

(i) In determining what type of auxiliary aid is necessary, the Board shall give primary consideration to the requests of the individual with a disability.

(ii) The Board need not provide individually prescribed devices, readers for personal use or study, or other devices of a personal nature.

(2) Where the Board communicates with employees and others by telephone, telecommunication devices for deaf persons (TDD's) or equally effective telecommunication systems shall be used.

(b) The Board shall ensure that interested persons, including persons with impaired vision or hearing, can obtain information as to the existence and location of accessible services, activities, and facilities.

(c) The Board shall provide signage at a primary entrance to each of its inaccessible facilities, directing users to a location at which they can obtain information about accessible facilities. The international symbol for accessibility shall be used at each primary entrance of an accessible facility.

(d) This section does not require the Board to take any action that would result in a fundamental alteration in the nature of a program or activity or in undue financial and administrative burdens. In those circumstances where the Board believes that the proposed action would fundamentally alter the program or activity or would result in undue financial and administrative burdens, the Board has the burden of proving that compliance with section 268.709 would result in such alterations or burdens. The determination that compliance would result in such alteration or burdens must be made by the Board of Governors or their designee after considering all Board resources available for use in the funding and operation of the conducted program or activity, and must be accompanied by a written statement of the reasons for reaching that conclusion. If an action required to comply with this section would result in such an alteration or such burdens, the Board shall take any other action that would not result in such an alteration or such burdens but would nevertheless ensure that, to the maximum extent possible, individuals with a disability receive the benefits and services of the program or activity.

§ 268.710 Compliance procedures.

(a) *Applicability.* Except as provided in paragraph (b) of this section, this section, rather than subpart B and § 268.203 of this part, applies to all allegations of discrimination on the basis of a disability in programs or activities conducted by the Board.

(b) *Employment complaints.* The Board shall process complaints alleging discrimination in employment on the basis of a disability in accordance with subparts A through G of this part.

(c) *Responsible official.* The EEO Programs Director shall be responsible for coordinating implementation of this section.

(d) *Filing the complaint*—(1) *Who may file.* Any person who believes that he or she has been subjected to discrimination prohibited by this subpart may, personally or by his or her authorized representative, file a complaint of discrimination with the EEO Programs Director.

(2) *Confidentiality.* The EEO Programs Director shall not reveal the identity of any person submitting a complaint, except when authorized to do so in writing by the complainant, and except to the extent necessary to carry out the purposes of this subpart , including the conduct of any investigation, hearing, or proceeding under this subpart.

(3) *When to file.* Complaints shall be filed within 180 days of the alleged act of discrimination. The EEO Programs Director may extend this time limit for good cause shown. For the purpose of determining when a complaint is timely filed under this paragraph (d), a complaint mailed to the Board shall be deemed filed on the date it is postmarked. Any other complaint shall be deemed filed on the date it is received by the Board.

(4) *How to file.* Complaints may be delivered or mailed to the Administrative Governor, the Staff Director for Management, the EEO Programs Director, the Federal Women's Program Manager, the Hispanic Employment Program Coordinator, or the People with Disabilities Program Coordinator. Complaints should be sent to the EEO Programs Director, Board of Governors of the Federal Reserve System, 20th and C Street NW., Washington, DC 20551. If any Board official other than the EEO Programs Director receives a complaint, he or she shall forward the complaint to the EEO Programs Director.

(e) *Acceptance of complaint.* (1) The EEO Programs Director shall accept a complete complaint that is filed in accordance with paragraph (d) of this section and over which the Board has jurisdiction. The EEO Programs Director shall notify the complainant of receipt and acceptance of the complaint.

(2) If the EEO Programs Director receives a complaint that is not complete, he or she shall notify the complainant, within 30 days of receipt of the incomplete complaint, that additional information is needed. If the complainant fails to complete the complaint within 30 days of receipt of this notice, the EEO Programs Director shall dismiss the complaint without prejudice.

(3) If the EEO Programs Director receives a complaint over which the Board does not have jurisdiction, the EEO Programs Director shall notify the complainant and shall make reasonable efforts to refer the complaint to the appropriate government entity.

(f) *Investigation/conciliation.* (1) Within 180 days of the receipt of a complete complaint, the EEO Programs Director shall complete the investigation of the complaint, attempt informal resolution of the complaint, and if no informal resolution is achieved, the EEO Programs Director shall forward the investigative report to the Staff Director for Management.

(2) The EEO Programs Director may request Board employees to cooperate in the investigation and attempted resolution of complaints. Employees who are requested by the EEO Programs Director to participate in any investigation under this section shall do so as part of their official duties and during the course of regular duty hours.

(3) The EEO Programs Director shall furnish the complainant with a copy of the investigative report promptly after completion of the investigation and provide the complainant with an opportunity for informal resolution of the complaint.

(4) If a complaint is resolved informally, the terms of the agreement shall be reduced to writing and made a part of the complaint file, with a copy of the agreement provided to the complainant. The written agreement may include a finding on the issue of discrimination and shall describe any corrective action to which the complainant has agreed.

(g) *Letter of findings.* (1) If an informal resolution of the complaint is not reached, the EEO Programs Director shall transmit the complaint file to the Staff Director for Management. The Staff Director for Management shall, within 180 days of the receipt of the complete complaint by the EEO Programs Director, notify the complainant of the results of the investigation in a letter sent by certified mail, return receipt requested, containing:

(i) Findings of fact and conclusions of law;

(ii) A description of a remedy for each violation found;

(iii) A notice of right of the complainant to appeal the letter of findings under paragraph (k) of this section; and

(iv) A notice of right of the complainant to request a hearing.

(2) If the complainant does not file a notice of appeal or does not request a hearing within the times prescribed in paragraph (h)(1) and (j)(1) of this section, the EEO Programs Director shall certify that the letter of findings under this paragraph (g) is the final decision of the Board at the expiration of those times.

(h) *Filing an appeal.* (1) Notice of appeal, with or without a request for hearing, shall be filed by the complainant with the EEO Programs Director within 30 days of receipt from the Staff Director for Management of the letter of findings required by paragraph (g) of this section.

(2) If the complainant does not request a hearing, the EEO Programs Director shall notify the Board of Governors of the appeal by the complainant and that a decision must be made under paragraph (k) of this section.

(i) *Acceptance of appeal.* The EEO Programs Director shall accept and process any timely appeal. A complainant may appeal to the Administrative Governor from a decision by the EEO Programs Director that an appeal is untimely. This appeal shall be filed within 15 calendar days of receipt of the decision from the EEO Programs Director.

(j) *Hearing.* (1) Notice of a request for a hearing, with or without a request for an appeal, shall be filed by the complainant with the EEO Programs Director within 30 days of receipt from the Staff Director for Management of the letter of findings required by paragraph (g) of this section. Upon a timely request for a hearing, the EEO Programs Director shall request that the Board of Governors, or its designee, appoint an administrative law judge to conduct the hearing. The administrative law judge shall issue a notice to the complainant and the Board specifying the date, time, and place of the scheduled hearing. The hearing shall be commenced no earlier than 15 calendar days after the notice is issued and no later than 60 days after the request for a hearing is filed, unless all parties agree to a different date.

(2) The hearing, decision, and any administrative review thereof shall be conducted in conformity with 5 U.S.C. 554–557. The administrative law judge shall have the duty to conduct a fair hearing, to take all necessary actions to avoid delay, and to maintain order. He or she shall have all powers necessary to these ends, including (but not limited to) the power to:

(i) Arrange and change the dates, times, and places of hearings and prehearing conferences and to issue notice thereof;

(ii) Hold conferences to settle, simplify, or determine the issues in a hearing, or to consider other matters that may aid in the expeditious disposition of the hearing;

(iii) Require parties to state their positions in writing with respect to the various issues in the hearing and to exchange such statements with all other parties;

(iv) Examine witnesses and direct witnesses to testify;

(v) Receive, rule on, exclude, or limit evidence;

(vi) Rule on procedural items pending before him or her; and

(vii) Take any action permitted to the administrative law judge as authorized by this subpart G or by the provisions of the Administrative Procedures Act (5 U.S.C. 554–557).

(3) Technical rules of evidence shall not apply to hearings conducted pursuant to this paragraph (j), but rules or principles designed to assure production of credible evidence and to subject testimony to cross-examination shall be applied by the administrative law judge wherever reasonably necessary. The administrative law judge may exclude irrelevant, immaterial, or unduly repetitious evidence. All documents and other evidence offered or taken for the record shall be open to examination by the parties, and opportunity shall be given to refute facts and arguments advanced on either side of the issues. A transcript shall be made of the oral evidence except to the extent the substance thereof is stipulated for the record. All decisions shall be based upon the hearing record.

(4) The costs and expenses for the conduct of a hearing shall be allocated as follows:

(i) Employees of the Board shall, upon the request of the administrative law judge, be made available to participate in the hearing and shall be on official duty status for this purpose. They shall not receive witness fees.

(ii) Employees of other Federal agencies called to testify at a hearing, at the request of the administrative law judge and with the approval of the employing agency, shall be on official duty status during any absence from normal duties caused by their testimony, and shall not receive witness fees.

(iii) The fees and expenses of other persons called to testify at a hearing shall be paid by the party requesting their appearance.

(iv) The administrative law judge may require the Board to pay travel expenses necessary for the complainant to attend the hearing.

(v) The Board shall pay the required expenses and charges for the administrative law judge and court reporter.

(vi) All other expenses shall be paid by the parties incurring them.

(5) The administrative law judge shall submit in writing recommended findings of fact, conclusions of law, and remedies to the complainant and the EEO Programs Director within 30 days, after the receipt of the hearing transcripts, or within 30 days after the conclusion of the hearing if no transcripts are made. This time limit may be extended with the permission of the EEO Programs Director.

(6) Within15 calendar days after receipt of the recommended decision of the administrative law judge, the complainant may file exceptions to the recommended decision with the EEO Programs Director. On behalf of the Board, the EEO Programs Director may, within 15 calendar days after receipt of the recommended decision of the administrative law judge, take exception to the recommended decision of the administrative law judge and shall notify the complainant in writing of the Board's exception. Thereafter, the complainant shall have 10 calendar days to file reply exceptions with the EEO Programs Director. The EEO Programs Director shall retain copies of the exceptions and replies to the Board's exception for consideration by the Board. After the expiration of the time to reply, the recommended decision shall be ripe for a decision under paragraph (k) of this section.

(k) *Decision.* (1) The EEO Programs Director shall notify the Board of Governors when a complaint is ripe for decision under this paragraph (k). At the request of any member of the Board of Governors made within 3 business days of such notice, the Board of Governors shall make the decision on the complaint. If no such request is made, the Administrative Governor, or the Staff Director for Management if he or she is delegated the authority to do so, shall make the decision on the complaint. The decision shall be made based on information in the investigative record and, if a hearing is held, on the hearing record. The decision shall be made within 60 days

of the receipt by the EEO Programs Director of the notice of appeal and investigative record pursuant to paragraph (h)(1) of this section or 60 days following the end of the period for filing reply exceptions set forth in paragraph (j)(6) of this section, whichever is applicable. If the decision-maker under this paragraph (k) determines that additional information is needed from any party, the decision-maker shall request the information and provide the other party or parties an opportunity to respond to that information. The decision-maker shall have 60 days from receipt of the additional information to render the decision on the appeal. The decision-maker shall transmit the decision by letter to all parties. The decision shall set forth the findings, any remedial actions required, and the reasons for the decision. If the decision is based on a hearing record, the decision-maker shall consider the recommended decision of the administrative law judge and render a final decision based on the entire record. The decision-maker may also remand the hearing record to the administrative law judge for a fuller development of the record.

(2) The Board shall take any action required under the terms of the decision promptly. The decision-maker may require periodic compliance reports specifying:

(i) The manner in which compliance with the provisions of the decision has been achieved;

(ii) The reasons any action required by the final Board decision has not been taken; and

(iii) The steps being taken to ensure full compliance.

(3) The decision-maker may retain responsibility for resolving disputes that arise between parties over interpretation of the final Board decision, or for specific adjudicatory decisions arising out of implementation.

By order of the Board of Governors of the Federal Reserve System, April 9, 2003.

Jennifer J. Johnson,

Secretary of the Board.

[FR Doc. 03–9111 Filed 4–14–03; 8:45 am]

BILLING CODE 6210–01–P

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Part 39

[Docket No. 2003–NE–06–AD; Amendment 39–13112; AD 2003–08–01]

RIN 2120–AA64

Airworthiness Directives; Rolls-Royce Deutschland Ltd. & Co KG, Model Tay 650–15 Turbofan Engines

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Final rule; request for comments.

SUMMARY: The FAA is adopting a new airworthiness directive (AD) for certain serial numbers (SNs) of Rolls-Royce Deutschland Ltd. & Co KG (RRD) Model Tay 650–15 turbofan engines. This action requires initial and repetitive visual inspections of low pressure (LP) turbine stage 2 rotor discs and LP turbine stage 3 rotor discs on certain SNs of engines, for corrosion. This AD is prompted by reports of excessive corrosion found during disc inspection. The actions specified in this AD are intended to prevent uncontained LP turbine stage 2 rotor disc or LP turbine stage 3 rotor disc failure due to excessive corrosion, and damage to the airplane.

DATES: Effective May 20, 2003.

We must receive any comments on this AD by June 16, 2003.

ADDRESSES: Use one of the following addresses to submit comments on this AD:

- By mail: The Federal Aviation Administration (FAA), New England Region, Office of the Regional Counsel, Attention: Rules Docket No. 2003–NE–06–AD, 12 New England Executive Park, Burlington, MA 01803–5299.
- By fax: (781) 238–7055.
- By e-mail: *9-ane-adcomment@faa.gov*

You may get the service information referenced in this AD from Rolls-Royce Deutschland Ltd & Co KG, Eschenweg 11, D–15827 Dahlewitz, Germany, telephone +49 (0) 33–7086–1768; fax +49 (0) 33–7086–3356.

You may examine the AD docket, by appointment, at the FAA, New England Region, Office of the Regional Counsel, 12 New England Executive Park, Burlington, MA.

FOR FURTHER INFORMATION CONTACT: James Lawrence, Aerospace Engineer, Engine Certification Office, FAA, Engine and Propeller Directorate, 12 New England Executive Park, Burlington, MA 01803–5299; telephone (781) 238–7176; fax (781) 238–7199.

SUPPLEMENTARY INFORMATION: The Luftfahrt-Bundesamt (LBA), which is the airworthiness authority for Germany, recently notified the FAA that an unsafe condition may exist on certain SNs of RRD Model Tay 650–15 turbofan engines. The LBA advises that the LP turbine stage 2 rotor discs and LP turbine stage 3 rotor discs of seventeen Tay 650–15 turbofan engines have been found to have excessive corrosion. RRD has determined that this excessive corrosion is the result of the specific environment in which these engines operate. This AD requires initial and repetitive visual inspections for corrosion of low pressure (LP) turbine stage 2 rotor discs and LP turbine stage 3 rotor discs on certain SNs of engines. Because disc deterioration may already have begun, repetitive inspections are also required if any affected disc is removed from the corrosive environment and put in service in a noncorrosive environment. The actions specified in this AD are intended to prevent uncontained LP turbine stage 2 rotor disc or LP turbine stage 3 rotor disc failure due to excessive corrosion, and damage to the airplane.

Relevant Service Information

The LBA issued AD 2002–287, dated October 17, 2002, in order to assure the airworthiness of these RRD Model Tay 650–15 turbofan engines in Germany.

FAA's Determination and Requirements of This AD

Although none of these affected disc SNs are used on any airplanes that are registered in the United States, the possibility exists that these disc SNs could be installed into engines used on airplanes that are registered in the United States in the future. Since an unsafe condition has been identified that is likely to exist or develop on other RRD Tay 650–15 turbofan engines of the same type design, this AD is being issued to prevent uncontained LP turbine stage 2 rotor disc or LP turbine stage 3 rotor disc failure due to excessive corrosion, and damage to the airplane. For engine SNs 17251, 17255, 17256, 17273, 17275, 17280, 17281, 17282, 17300, 17301, 17327, 17332, 17365, 17393, 17437, 17563, and 17618, this AD requires initial and repetitive visual inspections of LP turbine stage 2 rotor discs and LP turbine stage 3 rotor discs for corrosion.

Bilateral Airworthiness Agreement

This engine model is manufactured in Germany, and is type certificated for operation in the United States under the provisions of § 21.29 of the Federal Aviation Regulations (14 CFR 21.29)

SEC. 342. OFFICE OF MINORITY AND WOMEN INCLUSION

(a) OFFICE OF MINORITY AND WOMEN INCLUSION.—

(1) ESTABLISHMENT.—

(A) IN GENERAL.—Except as provided in subparagraph

(B), not later than 6 months after the date of enactment of this Act, each agency shall establish an Office of Minority and Women Inclusion that shall be responsible for all matters of the agency relating to diversity in management, employment, and business activities.

(B) BUREAU.—The Bureau shall establish an Office of Minority and Women Inclusion not later than 6 months after the designated transfer date established under section 1062.

(2) TRANSFER OF RESPONSIBILITIES.—Each agency that, on the day before the date of enactment of this Act, assigned the responsibilities described in paragraph (1) (or comparable responsibilities) to another office of the agency shall ensure that such responsibilities are transferred to the Office.

(3) DUTIES WITH RESPECT TO CIVIL RIGHTS LAWS.—The responsibilities described in paragraph (1) do not include enforcement of statutes, regulations, or executive orders pertaining to civil rights, except each Director shall coordinate with the agency administrator, or the designee of the agency administrator, regarding the design and implementation of any remedies resulting from violations of such statutes, regulations, or executive orders.

(b) DIRECTOR.—

(1) IN GENERAL.—The Director of each Office shall be appointed by, and shall report to, the agency administrator. The position of Director shall be a career reserved position in the Senior Executive Service, as that position is defined in section 3132 of title 5, United States Code, or an equivalent designation.

(2) DUTIES.—Each Director shall develop standards for—

(A) equal employment opportunity and the racial, ethnic, and gender diversity of the workforce and senior management of the agency;

(B) increased participation of minority-owned and women-owned businesses in the programs and contracts of the agency, including standards for coordinating technical assistance to such businesses; and

(C) assessing the diversity policies and practices of entities regulated by the agency.

(3) OTHER DUTIES.—Each Director shall advise the agency administrator on the impact of the policies and regulations of the agency on minority-owned and women-owned businesses.

(4) RULE OF CONSTRUCTION.—Nothing in paragraph (2)(C) may be construed to mandate any requirement on or otherwise affect the lending policies and practices of any regulated entity, or to require any specific action based on the findings of the assessment.

(c) INCLUSION IN ALL LEVELS OF BUSINESS ACTIVITIES.—

(1) IN GENERAL.—The Director of each Office shall develop and implement standards and procedures to ensure, to the maximum extent possible, the fair inclusion and utilization of minorities, women, and minority-owned and women-owned businesses in all business and activities of the agency at all levels, including in procurement, insurance, and all types of contracts.

(2) CONTRACTS.—The procedures established by each agency for review and evaluation of contract proposals and for hiring service providers shall include, to the extent consistent with applicable law, a component that gives consideration to the diversity of the applicant. Such procedure shall include a written statement, in a form and with such content as the Director shall prescribe, that a contractor shall ensure, to the maximum extent possible, the fair inclusion of women and minorities in the workforce of the contractor and, as applicable, subcontractors.

(3) TERMINATION.—

(A) DETERMINATION.—The standards and procedures developed and implemented under this subsection shall include a procedure for the Director to make a determination whether an agency contractor, and, as applicable, a subcontractor has failed to make a good faith effort to include minorities and women in their workforce.

(B) EFFECT OF DETERMINATION.—

(i) RECOMMENDATION TO AGENCY ADMINISTRATOR.— Upon a determination described in subparagraph (A), the Director shall make a recommendation to the agency administrator that the contract be terminated.

(ii) ACTION BY AGENCY ADMINISTRATOR.—Upon receipt of a recommendation under clause (i), the agency administrator may—

(I) terminate the contract;

(II) make a referral to the Office of Federal Contract Compliance Programs of the Department of Labor; or

(III) take other appropriate action.

(d) APPLICABILITY.—This section shall apply to all contracts of an agency for services of any kind, including the services of financial institutions, investment banking firms, mortgage banking firms, asset management firms, brokers, dealers, financial services entities, underwriters, accountants, investment consultants, and providers of legal services. The contracts referred to in this subsection include all contracts for all business and activities of an agency, at all levels, including contracts for the issuance or guarantee of any debt, equity, or security, the sale of assets, the management of the assets of the agency, the making of equity investments by the agency, and the implementation by the agency of programs to address economic recovery.

(e) REPORTS.—Each Office shall submit to Congress an annual report regarding the actions taken by the agency and the Office pursuant to this section, which shall include—

(1) a statement of the total amounts paid by the agency to contractors since the previous report;
(2) the percentage of the amounts described in paragraph (1) that were paid to contractors described in subsection (c)(1);
(3) the successes achieved and challenges faced by the agency in operating minority and women outreach programs;
(4) the challenges the agency may face in hiring qualified minority and women employees and contracting with qualified minority-owned and women-owned businesses; and
(5) any other information, findings, conclusions, and recommendations for legislative or agency action, as the Director determines appropriate.

(f) DIVERSITY IN AGENCY WORKFORCE.—Each agency shall take affirmative steps to seek diversity in the workforce of the agency at all levels of the agency in a manner consistent with applicable law. Such steps shall include—

(1) recruiting at historically black colleges and universities, Hispanic-serving institutions, women's colleges, and colleges that typically serve majority minority populations;
(2) sponsoring and recruiting at job fairs in urban communities;
(3) placing employment advertisements in newspapers and magazines oriented toward minorities and women;
(4) partnering with organizations that are focused on developing opportunities for minorities and women to place talented young minorities and women in industry internships, summer employment, and full-time positions;
(5) where feasible, partnering with inner-city high schools, girls' high schools, and high schools with majority minority populations to establish or enhance financial literacy programs and provide mentoring; and
(6) any other mass media communications that the Office determines necessary.

(g) DEFINITIONS.—For purposes of this section, the following definitions shall apply:

(1) AGENCY.—The term ''agency'' means—
  (A) the Departmental Offices of the Department of the Treasury;
  (B) the Corporation;
  (C) the Federal Housing Finance Agency;
  (D) each of the Federal reserve banks;
  (E) the Board;
  (F) the National Credit Union Administration;
  (G) the Office of the Comptroller of the Currency;
  (H) the Commission; and
  (I) the Bureau.
(2) AGENCY ADMINISTRATOR.—The term ''agency administrator'' means the head of an agency.
(3) MINORITY.—The term ''minority'' has the same meaning as in section 1204(c) of the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (12 U.S.C. 1811 note).
(4) MINORITY-OWNED BUSINESS.—The term ''minority-owned business'' has the same meaning as in section 21A(r)(4)(A) of the Federal Home Loan Bank Act (12 U.S.C. 1441a(r)(4)(A)), as in effect on the day before the transfer date.
(5) OFFICE.—The term ''Office'' means the Office of Minority and Women Inclusion established by an agency under subsection (a).
(6) WOMEN-OWNED BUSINESS.—The term ''women-owned business'' has the meaning given the term ''women's business'' in section 21A(r)(4)(B) of the Federal Home Loan Bank Act (12 U.S.C. 1441a(r)(4)(B)), as in effect on the day before the transfer date.

ELECTRONIC CODE OF FEDERAL REGULATIONS

e-CFR Data is current as of January 16, 2015

Title 29: Labor
PART 1614—FEDERAL SECTOR EQUAL EMPLOYMENT OPPORTUNITY

Subpart G—Procedures Under the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (No FEAR Act)

Contents

AUTHORITY: Sec. 303, Pub. L. 107-174, 116 Stat. 574.

SOURCE: 71 FR 43650, Aug. 2, 2006, unless otherwise noted.

Back to Top

§1614.701 Purpose and scope.

This subpart implements Title III of the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (No FEAR Act), Pub. L. 107-174. It sets forth the basic responsibilities of Federal agencies and the Commission to post certain information on their public Web sites.

Back to Top

§1614.702 Definitions.

The following definitions apply for purposes of this subpart.

(a) The term *Federal agency* or *agency* means an Executive agency (as defined in 5 U.S.C. 105), the United States Postal Service, and the Postal Rate Commission.

(b) The term *Commission* means the Equal Employment Opportunity Commission and any subdivision thereof authorized to act on its behalf.

(c) The term *investigation* refers to the step of the federal sector EEO process described in 29 CFR 1614.108 and 1614.106(e)(2) and, for purposes of this subpart, it commences when the complaint is filed and ceases when the complainant is given notice under §1614.108(f) of the right to

request a hearing or to receive an immediate final decision without a hearing.

(d) The term *hearing* refers to the step of the federal sector EEO process described in 29 CFR 1614.109 and, for purposes of §1614.704(l)(2)(ii), it commences on the date the agency is informed by the complainant or EEOC, whichever occurs first, that the complainant has requested a hearing and ends on the date the agency receives from the EEOC notice that the EEOC Administrative Judge (AJ) is returning the case to the agency to take final action. For all other purposes under this subpart, a hearing commences when the AJ receives the complaint file from the agency and ceases when the AJ returns the case to the agency to take final action.

(e) For purposes of §1614.704(i), (j), and (k) the phrase without a hearing refers to a final action by an agency that is rendered:

(1) When an agency does not receive a reply to a notice issued under §1614.108(f);

(2) After a complainant requests an immediate final decision;

(3) After a complainant withdraws a request for a hearing; and

(4) After an administrative judge cancels a hearing and remands the matter to the agency.

(f) For purposes of §1614.704(i), (j), and (k), the term *after a hearing* refers to a final action by an agency that is rendered following a decision by an administrative judge under §1614.109(f)(3)(iv), (g) or (i).

(g) The phrase *final action by an agency* refers to the step of the federal sector EEO process described in 29 CFR 1614.110 and, for purposes of this subpart, it commences when the agency receives a decision by an Administrative Judge (AJ), receives a request from the complainant for an immediate final decision without a hearing or fails to receive a response to a notice issued under §1614.108(f) and ceases when the agency issues a final order or final decision on the complaint.

(h) The phrase *final action by an agency involving a finding of discrimination* means:

(1) A final order issued by an agency pursuant to §1614.110(a) following a finding of discrimination by an administrative judge; and

(2) A final decision issued by an agency pursuant to §1614.110(b) in which the agency finds discrimination.

(i) The term *appeal* refers to the step of the federal sector EEO process described in 29 CFR 1614.401 and, for purposes of this subpart, it commences when the appeal is received by the Commission and ceases when the appellate decision is issued.

(j) The term basis of alleged discrimination refers to the individual's protected status (i.e., race, color, religion, reprisal, sex, national origin, Equal Pay Act, age, disability, or genetic information). Only those bases protected by Title VII of the Civil Rights Act of 1964, as amended, 42 U.S.C. 2000e *et seq.,* the Equal Pay Act of 1963, 29 U.S.C. 206(d), the Age Discrimination in Employment Act of 1967, as amended, 29 U.S.C. 621 *et seq.,* the Rehabilitation Act of 1973, as amended, 29 U.S.C. 791 *et seq.,* and the Genetic Information Nondiscrimination Act, 42 U.S.C. 2000ff *et seq.,* are covered by the federal EEO process.

(k) The term *issue of alleged discrimination* means one of the following challenged agency actions affecting a term or condition of employment as listed on EEOC Standard Form 462 (“Annual Federal Equal Employment Opportunity Statistical Report of Discrimination Complaints”): Appointment/hire; assignment of duties; awards; conversion to full time; disciplinary action/demotion; disciplinary action/reprimand; disciplinary action/suspension; disciplinary action/removal; duty hours;

evaluation/appraisal; examination/test; harassment/non-sexual; harassment/sexual; medical examination; pay/overtime; promotion/non-selection; reassignment/denied; reassignment/directed; reasonable accommodation; reinstatement; retirement; termination; terms/conditions of employment; time and attendance; training; and, other.

(l) The term *subordinate component* refers to any organizational sub-unit directly below the agency or department level which has 1,000 or more employees and is required to submit EEOC Form 715-01 to EEOC pursuant to EEOC Equal Employment Opportunity Management Directive 715.

[57 FR 12646, Apr. 10, 1992, as amended at 74 FR 63984, Dec. 7, 2009]

Back to Top

§1614.703 Manner and format of data.

(a) Agencies shall post their statistical data in the following two formats: Portable Document Format (PDF); and an accessible text format that complies with section 508 of the Rehabilitation Act.

(b) Agencies shall prominently post the date they last updated the statistical information on the Web site location containing the statistical data.

(c) In addition to providing aggregate agency-wide data, an agency shall include separate data for each subordinate component. Such data shall be identified as pertaining to the particular subordinate component.

(d) Data posted under this subpart will be titled “Equal Employment Opportunity Data Posted Pursuant to Title III of the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (No FEAR Act), Pub. L. 107-174,” and a hyperlink to the data, entitled “No FEAR Act Data” will be posted on the homepage of an agency's public Web site. In the case of agencies with subordinate components, the data shall be made available by hyperlinks from the homepages of the Web sites (if any exist) of the subordinate components as well as the homepage of the Web site of the parent agency.

(e) Agencies shall post cumulative data pursuant to §1614.704 for the current fiscal year. Agencies may not post separate quarterly statistics for the current fiscal year.

(f) Data posted pursuant to §1614.704 by agencies having 100 or more employees, and all subordinate component data posted pursuant to subsection 1614.703(c), shall be presented in the manner and order set forth in the template EEOC has placed for this purpose on its public Web site.

(1) Cumulative quarterly and fiscal year data shall appear in vertical columns. The oldest fiscal year data shall be listed first, reading left to right, with the other fiscal years appearing in the adjacent columns in chronological order. The current cumulative quarterly or year-end data shall appear in the last, or far-right, column.

(2) The categories of data as set forth in §1614.704(a) through (m) of this subpart shall appear in horizontal rows. When reading from top to bottom, the order of the categories shall be in the same order as those categories appear in §1614.704(a) through (m).

(3) When posting data pursuant to §1614.704(d) and (j), bases of discrimination shall be arranged in the order in which they appear in §1614.702(j). The category “non-EEO basis” shall be posted last, after the basis of “disability.”

(4) When posting data pursuant to §1614.704(e) and (k), issues of discrimination shall be arranged in the order in which they appear in §1614.702(k). Only those issues set forth in §1614.702(k) shall be listed.

(g) Agencies shall ensure that the data they post under this subpart can be readily accessed through one or more commercial search engines.

(h) Within 60 days of the effective date of this rule, an agency shall provide the Commission the Uniform Resource Locator (URL) for the data it posts under this subpart. Thereafter, new or changed URLs shall be provided within 30 days.

(i) Processing times required to be posted under this subpart shall be recorded using number of days.

Back to Top

§1614.704 Information to be posted—all Federal agencies.

Commencing on January 31, 2004 and thereafter no later than 30 days after the end of each fiscal quarter beginning on or after January 1, 2004, each Federal agency shall post the following current fiscal year statistics on its public Internet Web site regarding EEO complaints filed under 29 CFR part 1614.

(a) The number of complaints filed in such fiscal year.

(b) The number of individuals filing those complaints (including as the agent of a class).

(c) The number of individuals who filed two or more of those complaints.

(d) The number of those complaints, whether initially or through amendment, raising each of the various bases of alleged discrimination and the number of complaints in which a non-EEO basis is alleged.

(e) The number of those complaints, whether initially or through amendment, raising each of the various issues of alleged discrimination.

(f) The average length of time it has taken an agency to complete, respectively, investigation and final action by an agency for:

(1) All complaints pending for any length of time during such fiscal year;

(2) All complaints pending for any length of time during such fiscal year in which a hearing was not requested; and

(3) All complaints pending for any length of time during such fiscal year in which a hearing was requested.

(g) The number of complaints dismissed by an agency pursuant to 29 CFR 1614.107(a), and the average length of time such complaints had been pending prior to dismissal.

(h) The number of complaints withdrawn by complainants.

(i)(1) The total number of final actions by an agency rendered in such fiscal year involving a finding of discrimination and, of that number,

(2) The number and percentage that were rendered without a hearing, and

(3) The number and percentage that were rendered after a hearing.

(j) Of the total number of final actions by an agency rendered in such fiscal year involving a finding of discrimination,

(1) The number and percentage of those based on each respective basis,

(2) The number and percentage for each respective basis that were rendered without a hearing, and

(3) The number and percentage for each respective basis that were rendered after a hearing.

(k) Of the total number of final actions by an agency rendered in such fiscal year involving a finding of discrimination,

(1) The number and percentage for each respective issue,

(2) The number and percentage for each respective issue that were rendered without a hearing, and

(3) The number and percentage for each respective issue that were rendered after a hearing.

(l) Of the total number of complaints pending for any length of time in such fiscal year,

(1) The number that were first filed before the start of the then current fiscal year,

(2) Of those complaints falling within subsection (l)(1),

(i) The number of individuals who filed those complaints, and

(ii) The number that are pending, respectively, at the investigation, hearing, final action by an agency, and appeal step of the process.

(m) Of the total number of complaints pending for any length of time in such fiscal year, the total number of complaints in which the agency has not completed its investigation within the time required by 29 CFR 1614.106(e)(2) plus any extensions authorized by that section or §1614.108(e).

Back to Top

§1614.705 Comparative data—all Federal agencies.

Commencing on January 31, 2004 and no later than January 31 of each year thereafter, each Federal agency shall post year-end data corresponding to that required to be posted by §1614.704 for each of the five immediately preceding fiscal years (or, if not available for all five fiscal years, for however many of those five fiscal years for which data are available). For each category of data, the agency shall post a separate figure for each fiscal year.

Back to Top

§1614.706 Other data.

Agencies shall not include or otherwise post with the data required to be posted under §1614.704 and 1614.705 of this subpart any other data, whether or not EEO related, but may post such other data on another, separate, Web page.

Back to Top

§1614.707 Data to be posted by EEOC.

(a) Commencing on January 31, 2004 and thereafter no later than 30 days after the end of each fiscal quarter beginning on or after January 1, 2004, the Commission shall post the following current fiscal year statistics on its public Internet Web site regarding hearings requested under this part 1614.

(1) The number of hearings requested in such fiscal year.

(2) The number of individuals filing those requests.

(3) The number of individuals who filed two or more of those requests.

(4) The number of those hearing requests involving each of the various bases of alleged discrimination.

(5) The number of those hearing requests involving each of the various issues of alleged discrimination.

(6) The average length of time it has taken EEOC to complete the hearing step for all cases pending at the hearing step for any length of time during such fiscal year.

(7)(i) The total number of administrative judge (AJ) decisions rendered in such fiscal year involving a finding of discrimination and, of that number,

(ii) The number and percentage that were rendered without a hearing, and

(iii) The number and percentage that were rendered after a hearing.

(8) Of the total number of AJ decisions rendered in such fiscal year involving a finding of discrimination,

(i) The number and percentage of those based on each respective basis,

(ii) The number and percentage for each respective basis that were rendered without a hearing, and

(iii) The number and percentage for each respective basis that were rendered after a hearing.

(9) Of the total number of AJ decisions rendered in such fiscal year involving a finding of discrimination,

(i) The number and percentage for each respective issue,

(ii) The number and percentage for each respective issue that were rendered without a hearing, and

(iii) The number and percentage for each respective issue that were rendered after a hearing.

(10) Of the total number of hearing requests pending for any length of time in such fiscal year,

(i) The number that were first filed before the start of the then current fiscal year, and

(ii) The number of individuals who filed those hearing requests in earlier fiscal years.

(11) Of the total number of hearing requests pending for any length of time in such fiscal year, the total number in which the Commission failed to complete the hearing step within the time required by §1614.109(i).

(b) Commencing on January 31, 2004 and thereafter no later than 30 days after the end of each fiscal quarter beginning on or after January 1, 2004, the Commission shall post the following current fiscal year statistics on its public Internet Web site regarding EEO appeals filed under part 1614.

(1) The number of appeals filed in such fiscal year.

(2) The number of individuals filing those appeals (including as the agent of a class).

(3) The number of individuals who filed two or more of those appeals.

(4) The number of those appeals raising each of the various bases of alleged discrimination.

(5) The number of those appeals raising each of the various issues of alleged discrimination.

(6) The average length of time it has taken EEOC to issue appellate decisions for:

(i) All appeals pending for any length of time during such fiscal year;

(ii) All appeals pending for any length of time during such fiscal year in which a hearing was not requested; and

(iii) All appeals pending for any length of time during such fiscal year in which a hearing was requested.

(7)(i) The total number of appellate decisions rendered in such fiscal year involving a finding of discrimination and, of that number,

(ii) The number and percentage that involved a final action by an agency rendered without a hearing, and

(iii) The number and percentage that involved a final action by an agency after a hearing.

(8) Of the total number of appellate decisions rendered in such fiscal year involving a finding of discrimination,

(i) The number and percentage of those based on each respective basis of discrimination,

(ii) The number and percentage for each respective basis that involved a final action by an agency rendered without a hearing, and

(iii) The number and percentage for each respective basis that involved a final action by an agency rendered after a hearing.

(9) Of the total number of appellate decisions rendered in such fiscal year involving a finding of discrimination,

(i) The number and percentage for each respective issue of discrimination,

(ii) The number and percentage for each respective issue that involved a final action by an agency rendered without a hearing, and

(iii) The number and percentage for each respective issue that involved a final action by an agency rendered after a hearing.

(10) Of the total number of appeals pending for any length of time in such fiscal year,

(i) The number that were first filed before the start of the then current fiscal year, and

(ii) The number of individuals who filed those appeals in earlier fiscal years.

Back to Top

For questions or comments regarding e-CFR editorial content, features, or design, email ecfr@nara.gov.
For questions concerning e-CFR programming and delivery issues, email webteam@gpo.gov.

(1) continue to operate any branch or agency that the savings association operated immediately before the savings association became a bank; and

(2) establish, acquire, and operate additional branches and agencies at any location within any State in which the savings association operated a branch immediately before the savings association became a bank, if the law of the State in which the branch is located, or is to be located, would permit establishment of the branch if the bank were a State bank chartered by such State.

SEC. 342. OFFICE OF MINORITY AND WOMEN INCLUSION. 12 USC 5452.

(a) OFFICE OF MINORITY AND WOMEN INCLUSION.—

(1) ESTABLISHMENT.— Deadlines.

(A) IN GENERAL.—Except as provided in subparagraph (B), not later than 6 months after the date of enactment of this Act, each agency shall establish an Office of Minority and Women Inclusion that shall be responsible for all matters of the agency relating to diversity in management, employment, and business activities.

(B) BUREAU.—The Bureau shall establish an Office of Minority and Women Inclusion not later than 6 months after the designated transfer date established under section 1062.

(2) TRANSFER OF RESPONSIBILITIES.—Each agency that, on the day before the date of enactment of this Act, assigned the responsibilities described in paragraph (1) (or comparable responsibilities) to another office of the agency shall ensure that such responsibilities are transferred to the Office.

(3) DUTIES WITH RESPECT TO CIVIL RIGHTS LAWS.—The responsibilities described in paragraph (1) do not include enforcement of statutes, regulations, or executive orders pertaining to civil rights, except each Director shall coordinate with the agency administrator, or the designee of the agency administrator, regarding the design and implementation of any remedies resulting from violations of such statutes, regulations, or executive orders.

(b) DIRECTOR.—

(1) IN GENERAL.—The Director of each Office shall be appointed by, and shall report to, the agency administrator. The position of Director shall be a career reserved position in the Senior Executive Service, as that position is defined in section 3132 of title 5, United States Code, or an equivalent designation.

(2) DUTIES.—Each Director shall develop standards for— Standards.

(A) equal employment opportunity and the racial, ethnic, and gender diversity of the workforce and senior management of the agency;

(B) increased participation of minority-owned and women-owned businesses in the programs and contracts of the agency, including standards for coordinating technical assistance to such businesses; and

(C) assessing the diversity policies and practices of entities regulated by the agency.

(3) OTHER DUTIES.—Each Director shall advise the agency administrator on the impact of the policies and regulations of the agency on minority-owned and women-owned businesses.

(4) RULE OF CONSTRUCTION.—Nothing in paragraph (2)(C) may be construed to mandate any requirement on or otherwise affect the lending policies and practices of any regulated entity, or to require any specific action based on the findings of the assessment.

(c) INCLUSION IN ALL LEVELS OF BUSINESS ACTIVITIES.—

Standards. Procedures.

(1) IN GENERAL.—The Director of each Office shall develop and implement standards and procedures to ensure, to the maximum extent possible, the fair inclusion and utilization of minorities, women, and minority-owned and women-owned businesses in all business and activities of the agency at all levels, including in procurement, insurance, and all types of contracts.

(2) CONTRACTS.—The procedures established by each agency for review and evaluation of contract proposals and for hiring service providers shall include, to the extent consistent with applicable law, a component that gives consideration to the diversity of the applicant. Such procedure shall include a written statement, in a form and with such content as the Director shall prescribe, that a contractor shall ensure, to the maximum extent possible, the fair inclusion of women and minorities in the workforce of the contractor and, as applicable, subcontractors.

(3) TERMINATION.—

(A) DETERMINATION.—The standards and procedures developed and implemented under this subsection shall include a procedure for the Director to make a determination whether an agency contractor, and, as applicable, a subcontractor has failed to make a good faith effort to include minorities and women in their workforce.

(B) EFFECT OF DETERMINATION.—

(i) RECOMMENDATION TO AGENCY ADMINISTRATOR.—Upon a determination described in subparagraph (A), the Director shall make a recommendation to the agency administrator that the contract be terminated.

(ii) ACTION BY AGENCY ADMINISTRATOR.—Upon receipt of a recommendation under clause (i), the agency administrator may—

(I) terminate the contract;

(II) make a referral to the Office of Federal Contract Compliance Programs of the Department of Labor; or

(III) take other appropriate action.

(d) APPLICABILITY.—This section shall apply to all contracts of an agency for services of any kind, including the services of financial institutions, investment banking firms, mortgage banking firms, asset management firms, brokers, dealers, financial services entities, underwriters, accountants, investment consultants, and providers of legal services. The contracts referred to in this subsection include all contracts for all business and activities of an agency, at all levels, including contracts for the issuance or guarantee of any debt, equity, or security, the sale of assets, the management of the assets of the agency, the making of equity investments by the agency, and the implementation by the agency of programs to address economic recovery.

(e) REPORTS.—Each Office shall submit to Congress an annual report regarding the actions taken by the agency and the Office pursuant to this section, which shall include—

(1) a statement of the total amounts paid by the agency to contractors since the previous report;

(2) the percentage of the amounts described in paragraph (1) that were paid to contractors described in subsection (c)(1);

(3) the successes achieved and challenges faced by the agency in operating minority and women outreach programs;

(4) the challenges the agency may face in hiring qualified minority and women employees and contracting with qualified minority-owned and women-owned businesses; and

(5) any other information, findings, conclusions, and recommendations for legislative or agency action, as the Director determines appropriate.

(f) DIVERSITY IN AGENCY WORKFORCE.—Each agency shall take affirmative steps to seek diversity in the workforce of the agency at all levels of the agency in a manner consistent with applicable law. Such steps shall include—

(1) recruiting at historically black colleges and universities, Hispanic-serving institutions, women's colleges, and colleges that typically serve majority minority populations;

(2) sponsoring and recruiting at job fairs in urban communities;

(3) placing employment advertisements in newspapers and magazines oriented toward minorities and women;

(4) partnering with organizations that are focused on developing opportunities for minorities and women to place talented young minorities and women in industry internships, summer employment, and full-time positions;

(5) where feasible, partnering with inner-city high schools, girls' high schools, and high schools with majority minority populations to establish or enhance financial literacy programs and provide mentoring; and

(6) any other mass media communications that the Office determines necessary.

Applicability.

(g) DEFINITIONS.—For purposes of this section, the following definitions shall apply:

(1) AGENCY.—The term "agency" means—

(A) the Departmental Offices of the Department of the Treasury;

(B) the Corporation;

(C) the Federal Housing Finance Agency;

(D) each of the Federal reserve banks;

(E) the Board;

(F) the National Credit Union Administration;

(G) the Office of the Comptroller of the Currency;

(H) the Commission; and

(I) the Bureau.

(2) AGENCY ADMINISTRATOR.—The term "agency administrator" means the head of an agency.

(3) MINORITY.—The term "minority" has the same meaning as in section 1204(c) of the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (12 U.S.C. 1811 note).

(4) MINORITY-OWNED BUSINESS.—The term "minority-owned business" has the same meaning as in section 21A(r)(4)(A)

Executive Order 13583—Establishing a Coordinated Government-Wide Initiative To Promote Diversity and Inclusion in the Federal Workforce

August 18, 2011

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to promote the Federal workplace as a model of equal opportunity, diversity, and inclusion, it is hereby ordered as follows:

Section 1. Policy. Our Nation derives strength from the diversity of its population and from its commitment to equal opportunity for all. We are at our best when we draw on the talents of all parts of our society, and our greatest accomplishments are achieved when diverse perspectives are brought to bear to overcome our greatest challenges.

A commitment to equal opportunity, diversity, and inclusion is critical for the Federal Government as an employer. By law, the Federal Government's recruitment policies should "endeavor to achieve a work force from all segments of society." (5 U.S.C. 2301(b)(1)). As the Nation's largest employer, the Federal Government has a special obligation to lead by example. Attaining a diverse, qualified workforce is one of the cornerstones of the merit-based civil service.

Prior Executive Orders, including but not limited to those listed below, have taken a number of steps to address the leadership role and obligations of the Federal Government as an employer. For example, Executive Order 13171 of October 12, 2000 (Hispanic Employment in the Federal Government), directed executive departments and agencies to implement programs for recruitment and career development of Hispanic employees and established a mechanism for identifying best practices in doing so. Executive Order 13518 of November 9, 2009 (Employment of Veterans in the Federal Government), required the establishment of a Veterans Employment Initiative. Executive Order 13548 of July 26, 2010 (Increasing Federal Employment of Individuals with Disabilities), and its related predecessors, Executive Order 13163 of July 26, 2000 (Increasing the Opportunity for Individuals With Disabilities to be Employed in the Federal Government), and Executive Order 13078 of March 13, 1998 (Increasing Employment of Adults With Disabilities), sought to tap the skills of the millions of Americans living with disabilities.

To realize more fully the goal of using the talents of all segments of society, the Federal Government must continue to challenge itself to enhance its ability to recruit, hire, promote, and retain a more diverse workforce. Further, the Federal Government must create a culture that encourages collaboration, flexibility, and fairness to enable individuals to participate to their full potential.

Wherever possible, the Federal Government must also seek to consolidate compliance efforts established through related or overlapping statutory mandates, directions from Executive Orders, and regulatory requirements. By this order, I am directing executive departments and agencies (agencies) to develop and implement a more comprehensive, integrated, and strategic focus on diversity and inclusion as a key component of their human resources strategies. This approach should include a continuing effort to identify and adopt best practices, implemented in an integrated manner, to promote diversity and remove barriers to equal employment opportunity, consistent with merit system principles and applicable law.

Sec. 2. Government-Wide Diversity and Inclusion Initiative and Strategic Plan. The Director of the Office of Personnel Management (OPM) and the Deputy Director for Management of the Office of Management and Budget (OMB), in coordination with the President's Management Council (PMC) and the Chair of the Equal Employment Opportunity Commission (EEOC), shall:

(a) establish a coordinated Government-wide initiative to promote diversity and inclusion in the Federal workforce;

(b) within 90 days of the date of this order:

(i) develop and issue a Government-wide Diversity and Inclusion Strategic Plan (Government-wide Plan), to be updated as appropriate and at a minimum every 4 years, focusing on workforce diversity, workplace inclusion, and agency accountability and leadership. The Government-wide Plan shall highlight comprehensive strategies for agencies to identify and remove barriers to equal employment opportunity that may exist in the Federal Government's recruitment, hiring, promotion, retention, professional development, and training policies and practices;

(ii) review applicable directives to agencies related to the development or submission of agency human capital and other workforce plans and reports in connection with recruitment, hiring, promotion, retention, professional development, and training policies and practices, and develop a strategy for consolidating such agency plans and reports where appropriate and permitted by law; and

(iii) provide guidance to agencies concerning formulation of agency-specific Diversity and Inclusion Strategic Plans prepared pursuant to section 3(b) of this order;

(c) identify appropriate practices to improve the effectiveness of each agency's efforts to recruit, hire, promote, retain, develop, and train a diverse and inclusive workforce, consistent with merit system principles and applicable law; and

(d) establish a system for reporting regularly on agencies' progress in implementing their agency-specific Diversity and Inclusion Strategic Plans and in meeting the objectives of this order.

Sec. 3. Responsibilities of Executive Departments and Agencies. All agencies shall implement the Government-wide Plan prepared pursuant to section 2 of this order, and such other related guidance as issued from time to time by the Director of OPM and Deputy Director for Management of OMB. In addition, the head of each executive department and agency referred to under subsections (1) and (2) of section 901(b) of title 31, United States Code, shall:

(a) designate the agency's Chief Human Capital Officer to be responsible for enhancing employment and promotion opportunities within the agency, in collaboration with the agency's Director of Equal Employment Opportunity and Director of Diversity and Inclusion, if any, and consistent with law and merit system principles, including development and implementation of the agency-specific Diversity and Inclusion Strategic Plan;

(b) within 120 days of the issuance of the Government-wide Plan or its update under section 2(b)(i) of this order, develop and submit for review to the Director of OPM and the Deputy Director for Management of OMB an agency-specific Diversity and Inclusion Strategic Plan for recruiting, hiring, training, developing, advancing, promoting, and retaining a diverse workforce consistent with applicable law, the Government-wide Plan, merit system principles,

the agency's overall strategic plan, its human capital plan prepared pursuant to Part 250 of title 5 of the Code of Federal Regulations, and other applicable workforce planning strategies and initiatives;

(c) implement the agency-specific Diversity and Inclusion Strategic Plan after incorporating it into the agency's human capital plan; and

(d) provide information as specified in the reporting requirements developed under section 2(d).

Sec. 4. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) authority granted to a department or agency or the head thereof, including the authority granted to EEOC by other Executive Orders (including Executive Order 12067) or any agency's authority to establish an independent Diversity and Inclusion Office; or

(ii) functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

BARACK OBAMA

The White House,
August 18, 2011.

[Filed with the Office of the Federal Register, 11:15 a.m., August 22, 2011]

NOTE: This Executive order was published in the *Federal Register* on August 23.

Categories: Executive Orders : Federal workforce, Government-wide initiative to promote diversity and inclusion, establishment.

Subjects: Government organization and employees : Federal workforce, Government-wide initiative to promote diversity and inclusion; Government organizations and employees : Recruitment and retention, strengthening efforts.

DCPD Number: DCPD201100581.

Table of Corresponding U.S. Code Citations

Paragraph or Subsection	*Topic*	*USC Section*
Section 1	**Short Title and Definitions**	
1	Short Title	12 U.S.C. § 226
2	Definition of "Bank"	12 U.S.C. § 221
3	Definitions of Other Terms	12 U.S.C. § 221
4	Definition of "Bonds and Notes of the United States"	12 U.S.C. § 221
Section 2	**Federal Reserve Districts**	
1	Establishment of Reserve Cities and Districts	12 U.S.C. § 222 and § 223 in part
2	Powers of Organization Committee	12 U.S.C. § 225 in part
3	Subscription to Stock by National Banks	12 U.S.C. § 282 in part
4	Liability of Shareholders of Reserve Banks	12 U.S.C. § 502
5	Failure of National Bank to Accept Terms of Act	omitted from U.S.C.
6	Penalty for Violation of Act by National Banks	12 U.S.C. § 501a
7	Effect of Dissolution	12 U.S.C. § 501a
8	Stock Offered to Public	omitted from U.S.C.
9	Limitation on Amount to One Subscriber	12 U.S.C. § 283
10	Stock Allotted to United States (rendered obsolete)	deleted from U.S.C.; formerly at 12 U.S.C. § 284
11	Voting Rights	12 U.S.C. § 285
12	Transfer of Stock	12 U.S.C. § 286
13	Minimum Capital; Status of Reserve Cities	12 U.S.C. § 224 and § 281 in part

Paragraph or Subsection	*Topic*	*USC Section*
Section 2A	**Monetary Policy Objectives**	12 U.S.C. §225a
Section 2B	**Appearance Before and Reports to the Congress**	12 U.S.C. §225b
(a)	Appearances Before the Congress	12 U.S.C. §225b(a)
(b)	Congressional Budget	12 U.S.C. §225b(b)
(c)	Public Access to Information	12 U.S.C. §225b(c)
Section 3	**Branch Offices**	
1	Establishment of Branches of Reserve Banks	12 U.S.C. §521
2	Discontinuance of Branches	12 U.S.C. §521
3	Erection of Branch Buildings	12 U.S.C. §521
Section 4	**Federal Reserve Banks**	
1	Organization of Reserve Banks	omitted from U.S.C.
2	Organization Certificate	omitted from U.S.C.
3	Acknowledgment and Filing	omitted from U.S.C.
4	General Corporate Powers	12 U.S.C. §341
5	Authority to Commence Business	12 U.S.C. §341
6	Board of Directors	12 U.S.C. §301
7	Duties of Directors Generally	12 U.S.C. §301
8	Administration of Affairs; Extension of Credit	12 U.S.C. §301
9	Number and Classes of Directors	12 U.S.C. §302
10	Class A Directors	12 U.S.C. §302
11	Class B Directors	12 U.S.C. §302
12	Class C Directors	12 U.S.C. §302
13	Senator or Representative Ineligible	12 U.S.C. §303
14	Class B Directors as Employees of Banks	12 U.S.C. §303
15	Class C Directors as Employees or Stockholders of Banks	12 U.S.C. §303
16	Nomination and Election of Class A and B Directors	12 U.S.C. §304
17	Preferential Ballot	12 U.S.C. §304
18	Candidates Serving More than One Member Bank	12 U.S.C. §304

Paragraph or Subsection	*Topic*	*USC Section*
19	Counting the Ballots	12 U.S.C. §304
20	Class C Directors; Chairman and Federal Reserve Agent; Deputy Chairman	12 U.S.C. §305
21	Assistant Federal Reserve Agents	12 U.S.C. §306
22	Compensation and Expenses of Directors, Officers, and Employees	12 U.S.C. §307
23	Meetings of Directors Pending Organizations	omitted from U.S.C.
24	Terms of Directors; Vacancies	12 U.S.C. §308
Section 5	**Stock Issues; Increase and Decrease of Capital**	12 U.S.C. §287
Section 6	**Insolvency of Member Banks**	
1	Insolvency of Member Banks	12 U.S.C. §288
2	National Bank Discontinuing Banking Operations	12 U.S.C. §288
Section 7	**Division of Earnings**	
1	Dividends and Surplus Fund of Reserve Banks	12 U.S.C. §289
2	Disposition of Surplus on Dissolution or Liquidation	12 U.S.C. §290
3	Exemption from Taxation	12 U.S.C. §531
Section 8	**Conversion of State Banks into National Banks**	
1	Conversion of State Banks into National Banks	12 U.S.C. §35
2	Disposition of Surplus on Dissolution or Liquidation	12 U.S.C. §35
3	Retention of Assets by Converting Bank	12 U.S.C. §35
Section 9	**State Banks as Members**	
1	Applications for Membership by State Banks	12 U.S.C. §321
2	Continued Membership in Federal Reserve System	12 U.S.C. §321
3	Branches of State Member Banks	12 U.S.C. §321

Paragraph or Subsection	*Topic*	*USC Section*
4	Financial Condition, Management, and Powers	12 U.S.C. §322
5	Payment of Subscription	12 U.S.C. §323
6	Provision of Law to be Complied with; Reports of Condition	12 U.S.C. §324
7	Examinations	12 U.S.C. §325
8	Acceptance of State Examinations; Expenses; Reports of Examinations	12 U.S.C. §326
9	Forfeiture of Membership	12 U.S.C. §327
10	Voluntary Withdrawal from Membership	12 U.S.C. §328
11	Capital Required for Membership	12 U.S.C. §329
12	Waiver of Membership Requirements as to Insured Banks (rendered obsolete)	deleted from U.S.C.; formerly at 12 U.S.C. §329a
13	Laws to Which Subject	12 U.S.C. §330
14	False Certification of Checks	12 U.S.C. §331
15	Government Depositaries and Financial Agents	12 U.S.C. §332
16	Admission to Membership of Mutual Savings Banks	12 U.S.C. §333
17	Reports of Affiliates	12 U.S.C. §334
18	Additional Reports of Affiliates	12 U.S.C. §334
19	Failure to Obtain Reports of Affiliates	12 U.S.C. §334
20	Dealings in Investment Securities and Stock	12 U.S.C. §335
21	Stock Representing Stock of Other Corporations	12 U.S.C. §336
	Voting Requirements of State Member Banks (repealed)	formerly at 12 U.S.C. §337
22	Examinations of Affiliates	12 U.S.C. §338
23	Community Development Authority	12 U.S.C. §338a
Section 9A	**Participation in Lotteries Prohibited**	
(a)	Prohibited Activities	12 U.S.C. §339(a)
(b)	Use of Banking Premises Prohibited	12 U.S.C. §339(b)
(c)	Definitions	12 U.S.C. §339(c)
(d)	Lawful Banking Services Connected with Operation of Lottery	12 U.S.C. §339(d)

Paragraph or Subsection	*Topic*	*USC Section*
(e)	Regulations; Enforcement	12 U.S.C. §339(e)
Section 9B	**Resolution of Clearing Banks**	12 U.S.C. §339a
Section 10	**Board of Governors of the Federal Reserve System**	
1	Appointment and Qualification of Members	12 U.S.C. §241
2	Members Ineligible to Serve Member Banks; Term of Office; Chairman and Vice Chairman	12 U.S.C. §242
3	Assessments on Federal Reserve Banks	12 U.S.C. §243
4	Principal Offices; Expenses; Deposit of Funds; Members Not to Be Officers or Stockholders of Banks	12 U.S.C. §244
5	Vacancies During Recess of Senate	12 U.S.C. §245
6	Reservation of Power of Secretary of Treasury	12 U.S.C. §246
7	Annual Report	12 U.S.C. §247
8	Issuance of National Currency and Federal Reserve Notes	12 U.S.C. §1
9	Branch Federal Reserve Bank Buildings	12 U.S.C. §522
10	Record of Open Market and Other Policies	12 U.S.C. §247a
12	Appearance Before Congress	12 U.S.C. §247b
Section 10A	**Emergency Advances to Groups of Member Banks**	
1	Authority of Reserve Banks to Make Advances	12 U.S.C. §347a
2	Foreign Obligations as Security for Advances	12 U.S.C. §347a
3	Authority of Member Banks to Obligate Themselves	12 U.S.C. §347a
Section 10B	**Advances to Individual Member Banks**	12 U.S.C. §347b
Section 11	**Powers of Board of Governors of the Federal Reserve System**	
(a)	Examinations and Reports	12 U.S.C. §248(a)
(b)	Rediscounts by One Reserve Bank to Another	12 U.S.C. §248(b)
(c)	Suspension of Reserve Requirements	12 U.S.C. §248(c)
(d)	Issue and Retirement of Federal Reserve Notes	12 U.S.C. §248(d)

Paragraph or Subsection	*Topic*	*USC Section*
(e)	Reclassification of Reserve Cities	12 U.S.C. §248(e)
(f)	Suspension or Removal of Officers and Directors of Reserve Banks	12 U.S.C. §248(f)
(g)	Charging Off Losses of Reserve Banks	12 U.S.C. §248(g)
(h)	Suspension, Liquidation, or Reorganization of Reserve Banks	12 U.S.C. §248(h)
(i)	Rules and Regulations	12 U.S.C. §248(i)
(j)	Supervision over Reserve Banks	12 U.S.C. §248(j)
(k)	Delegation of Functions	12 U.S.C. §248(k)
(*l*)	Employees of Board of Governors of the Federal Reserve System	12 U.S.C. §248(*l*)
(m)	Loans by Member Banks on Stock or Bond Collateral (repealed)	formerly at 12 U.S.C. §248(m)
(n)	Enforced Exchange of Gold Coin, Bullion, and Certificates for other Currency (repealed)	formerly at 12 U.S.C. §248(n)
(n)	Board's Authority to Examine Depository Institutions and Affiliates	12 U.S.C. §248(n)
(o)	Authority to Appoint Conservator or Receiver	12 U.S.C. §248(o)
(q)	Uniform Protection for Federal Reserve Facilities	12 U.S.C. §248(q)
(r)	Authority of Available Board Members in Unusual and Exigent Circumstances	12 U.S.C. §248(r)
(s)	Federal Reserve Transparency and Release of Information	12 U.S.C. §248(s)
(s)	Assessments, Fees, and Other Changes for Certain Companies	12 U.S.C. §248(s)
Section 11A	**Pricing of Services**	12 U.S.C. §248a
Section 11B	**Annual Independent Audits of Federal Reserve Banks and Board**	12 U.S.C. §248b
Section 12	**Federal Advisory Council**	
1	Creation, Members, and Meetings	12 U.S.C. §261
2	Powers	12 U.S.C. §262

Paragraph or Subsection	*Topic*	*USC Section*
Section 12A	**Federal Open Market Committee**	
(a)	Creation, Members, and Meetings	12 U.S.C. § 263(a)
(b)	Participation of Reserve Banks; Regulations of Committee	12 U.S.C. § 263(b)
(c)	Governing Principles	12 U.S.C. § 263(c)
Section 12B	**Federal Deposit Insurance Corporation** (transferred to 12 U.S.C. §§ 1811–1833e)	formerly at 12 U.S.C. § 264

Paragraph or Subsection	*Topic*	*USC Section*
Section 13	**Powers of Federal Reserve Banks**	
1	Receipt of Deposits and Collections	12 U.S.C. §342
2	Discount of Obligations Arising Out of Actual Commercial Transactions	12 U.S.C. §343
3	Discounts in Unusual and Exigent Circumstances	12 U.S.C. §343
4	Discount or Purchase of Sight Drafts	12 U.S.C. §344
5	Limitation on Discount of Paper of One Borrower	12 U.S.C. §345
6	Discount of Acceptances	12 U.S.C. §346
7	Bankers' Acceptance	12 U.S.C. §372
8	Advances to Member Banks on Promissory Notes	12 U.S.C. §347
9	Aggregate Liabilities of National Banks (repealed)	formerly at 12 U.S.C. §82
10	Regulation by Board of Governors of Discounts, Purchases and Sales	12 U.S.C. §361
11	National Banks as Insurance Agents or Real Estate Loan Brokers	12 U.S.C. §92
12	Bank Acceptances to Create Dollar Exchange	12 U.S.C. §373
13	Advances to Individuals, Partnerships, and Corporations on Obligations of United States	12 U.S.C. §347c
14	Receipt of Deposits From, Discount Paper Endorsed by, and Advances to Foreign Banks	12 U.S.C. §347d
Section 13A	**Discount of Agricultural Paper**	
1	Authority of Federal Reserve Banks to Discount Agricultural Paper	12 U.S.C. §348
2	Rediscounts for, and Discount of Notes Payable to, Federal Intermediate Credit Banks	12 U.S.C. §349
3	Purchase and Sale of Debentures of Federal Intermediate Credit Banks	12 U.S.C. §350
4	Paper of Cooperative Marketing Associations	12 U.S.C. §351
5	Limitations	12 U.S.C. §352

Paragraph or Subsection	*Topic*	*USC Section*
Section 13b	**Loans Authorized for Industrial of Commercial Business** (repealed)	formerly at 12 U.S.C. §352a
Section 14	**Open Market Operations**	
	Purchase and Sale of Cable Transfers, Bank Acceptances and Bills of Exchange	12 U.S.C. §353
(a)	Dealings In, and Loans On, Gold	12 U.S.C. §354
(b)	Purchase and Sale of Obligations of United States, States, Counties, etc., or of a Foreign Government	12 U.S.C. §355
(c)	Purchase and Sale of Bills of Exchange	12 U.S.C. §356
(d)	Rates of Discount	12 U.S.C. §357
(e)	Foreign Correspondents and Agencies	12 U.S.C. §358
(f)	Purchase and Sale of Acceptances of Federal Intermediate Credit Banks	12 U.S.C. §359
(g)	Relationships and Transactions with Foreign Banks and Bankers	12 U.S.C. §348a
(h)	Treasury Authority to Borrow and Sell in Open Market (expired)	formerly at 12 U.S.C. §359a
Section 15	**Government Deposits**	
1	Federal Reserve Banks as Depositaries and Fiscal Agents of United States	12 U.S.C. §391
2	Nonmember Banks as Depositaries of United States	12 U.S.C. §392
3	Depositaries and Fiscal Agents of Institutions of the Farm Credit System	12 U.S.C. §393
Section 16	**Federal Reserve Notes and Gold Deposits**	
1	Issuance of Federal Reserve Notes; Nature of Obligation; Where Redeemable	12 U.S.C. §411
2	Nonmember Banks as Depositaries of United States	12 U.S.C. §412
3	Distinctive Letter on Notes; Destruction of Unfit Notes	12 U.S.C. §413
4	Granting Right to Issue Notes	12 U.S.C. §414

Paragraph or Subsection	*Topic*	*USC Section*
5	Deposit to Reduce Liability for Outstanding Notes	12 U.S.C. §415
6	Substitution of Collateral; Retirement of Federal Reserve Notes	12 U.S.C. §416
7	Custody of Reserve Notes, Gold Certificates, and Lawful Money	12 U.S.C. §417
8	Engraving of Plates; Denominations and Form of Notes	12 U.S.C. §418
9	Custody of Unissued Notes	12 U.S.C. §419
10	Custody of Plates and Dies; Expenses of Issue and Retirement of Notes	12 U.S.C. §420
11	Examination of Plates, Dies, Etc.	12 U.S.C. §421
12	Appropriation for Engraving, Etc.	deleted from U.S.C.; formerly at 12 U.S.C. §422
13	Checks and Drafts to be Received on Deposit at Par	12 U.S.C. §360
14	Transfer of Funds Among Federal Reserve Banks	12 U.S.C. §248-1
15	Gold Deposits and Gold Certificate Deposits	12 U.S.C. §467
16	Expenses	12 U.S.C. §467
17	Preservation of Provisions of Act of March 14, 1900	12 U.S.C. §467
Section 17	**Deposit of Bonds by National Banks**	12 U.S.C. §101a
Section 18	**Refunding Bonds**	
1	Application to Sell Bonds Securing Circulation	12 U.S.C. §441
2	Purchase of Bonds by Federal Reserve Banks	12 U.S.C. §442
3	Allotment of Bonds to be Purchased	12 U.S.C. §442
4	Transfer and Payment	12 U.S.C. §443
5	Federal Reserve Bank Notes	12 U.S.C. §444
6	Collateral for Notes; Form and Tenor; Redemption; Etc. (repealed, in effect)	deleted from U.S.C.; formerly at 12 U.S.C. §445

Paragraph or Subsection	*Topic*	*USC Section*
7	Exchange of 2 Percent Gold Bonds for One-Year Gold Notes and 30-Year 3 Percent Gold Bonds	12 U.S.C. §446
8	Issue of One-Year Treasury Notes and 30-Year 3 Percent Gold Bonds	12 U.S.C. §447
9	Exchange of 3 Percent Bonds for One-Year Notes	12 U.S.C. §448
Section 19	**Bank Reserves**	
(a)	Authority to Define Terms	12 U.S.C. §461(a)
(b)	Definitions, Reserve Requirements, Waivers	12 U.S.C. §461(b)
(c)	Promulgation of Rules and Regulations Regarding Maintenance of Balances	12 U.S.C. §461(c)
	Former Reserve Requirements (repealed)	formerly at 12 U.S.C. §§462, 462a, 462a–1, 462b, 462c
(d)	Member Banks Making Security Loans for Others	12 U.S.C. §374a
(e)	Deposits with Depository Institutions Without Access to Federal Reserve Advances; Discounts for Nonmember Banks	12 U.S.C. §463 and §374
(f)	Checking Against and Withdrawal of Reserve Balance	12 U.S.C. §464
(g)	Deductions in Computing Reserves	12 U.S.C. §465
(h)	Bank in Dependencies and Insular Possessions as Member Banks; Reserves	12 U.S.C. §466
(i)	Interest on Demand Deposits (repealed)	formerly at 12 U.S.C. §371a
(j)	Advertisement of Interest on Time and Savings Deposits	12 U.S.C. §371b
(k)	Applicability of State Using Ceilings to Certain Obligations Issued by Bank and Affiliates (repealed)	formerly at 12 U.S.C. §371b–1
(*l*)	Civil Money Penalties	12 U.S.C. §505
(m)	Notice Under this Section After Separation From Service	12 U.S.C. §506

Paragraph or Subsection	*Topic*	*USC Section*
Section 20	**National Bank Notes Redemption Fund as Reserve**	12 U.S.C. §121
Section 21	**Bank Examination**	
	Amendment of section §5240, Revised Statutes	omitted from U.S.C.
1	Examination of National Banks and Affiliates of National Banks	12 U.S.C. §481
2	Powers in Examining Affiliates; Expenses of Examinations	12 U.S.C. §481
3	Salaries of Examiners	12 U.S.C. §482
4	Assessments to Defray Expenses	12 U.S.C. §482
5	Special Examinations by Reserve Banks	12 U.S.C. §483
6	Visitatorial Powers	12 U.S.C. §484
7	Examinations of Federal Reserve Banks	12 U.S.C. §485
8	Waiver of Reports and Examinations of Affiliates	12 U.S.C. §486
Section 22	**Offenses of Examiners, Member Banks, Officers, and Directors**	
(a)	Prohibition on Member Banks in Making Loans or Grants to Bank Examiners (repealed, see 18 U.S.C. §§212, 213 and 655)	formerly at 12 U.S.C. §593
(b)	Prohibition on Bank Examiners in Compensation and Disclosure (repealed, see 18 U.S.C. §§1906 and 1907)	formerly at 12 U.S.C. §594
(c)	Prohibition on Member Bank Staff in Bribery and Conflict of Interest (repealed, see 18 U.S.C. §220)	formerly at 12 U.S.C. §595
(d)	[Reserved]	
(e)	Interest on Deposits of Directors, Officers, and Employees	12 U.S.C. §376
(f)	Liability for Damages Resulting from Violations	12 U.S.C. §503

Paragraph or Subsection	*Topic*	*USC Section*
(g)	Loans to Executive Officers by Member Banks	12 U.S.C. §375a
(h)	Extensions of Credit to Executive Officers, Directors, and Principal Shareholders of Member Banks	12 U.S.C. §375b
(i)	Prohibition on False Statements or Overevaluation of Securities (repealed, see 18 U.S.C. §1014)	formerly at 12 U.S.C. §598
(j)	Prohibition on Embezzlement (repealed, see 18 U.S.C. §655–1005)	formerly at 12 U.S.C. §597
(k)	Relating to application of parts of Criminal Code to Federal Reserve Bank Contracts or Agreements (repealed)	formerly at 12 U.S.C. §598
(*l*)	Prohibition on Fees, Commissions, and Bonuses to Secure Loan (repealed, see 18 U.S.C. §219)	formerly at 12 U.S.C. §599
Section 23	**Liability of National Bank Stockholders** (repealed)	formerly at 12 U.S.C. §64
Section 23	**Interbank Liabilities**	
(a)	Purpose	12 U.S.C. §371b–2(a)
(b)	Aggregate Limits on Insured Depository Institutions' Exposure to Other Depository Institutions	12 U.S.C. §371b–2(b)
(c)	Exposure Defined	12 U.S.C. §371b–2(c)
(d)	Insured Depository Institution	12 U.S.C. §371b–2(d)
(e)	Rulemaking Authority; Enforcement	12 U.S.C. §371b–2(e)
Section 23A	**Relations with Affiliates**	
(a)	Restrictions on Transactions with Affiliates	12 U.S.C. §371c(a)
(b)	Definitions	12 U.S.C. §371c(b)
(c)	Collateral for Certain Transactions with Affiliates	12 U.S.C. §371c(c)
(d)	Exemptions	12 U.S.C. §371c(d)

Paragraph or Subsection	*Topic*	*USC Section*
(e)	Rules Relating to Banks with Financial Subsidiaries	12 U.S.C. §371c(e)
(f)	Rulemaking and Additional Exemptions	12 U.S.C. §371c(f)
Section 23B	**Restrictions on Transactions with Affiliates**	
(a)	In General	12 U.S.C. §371c–1(a)(12/92)
(b)	Prohibited Transactions	12 U.S.C. §371c–1(b)
(c)	Advertising Restriction	12 U.S.C. §371c–1(c)
(d)	Definitions	12 U.S.C. §371c–1(d)
(e)	Regulations	12 U.S.C. §371c–1(e)
Section 24	**Real Estate Loans**	12 U.S.C. §371
Section 24A	**Investments in Bank Premises**	12 U.S.C. §371d
Section 25	**Foreign Branches**	
1	Capital and Surplus Required to Exercise Powers	12 U.S.C. §601
2	Establishment of Foreign Branches	12 U.S.C. §601
3	Purchase of Stock in Corporations Engaged in Foreign Banking	12 U.S.C. §601
4	Acquisition of Ownership of Foreign Banks	12 U.S.C. §601
5	Right of National Banks to Invest in Foreign Banking Corporations Until January 1, 1921	12 U.S.C. §601
6	Application for Permission to Exercise Powers	12 U.S.C. §601
7	Examinations and Reports of Condition	12 U.S.C. §602
8	Agreement to Restrict Operations	12 U.S.C. §603
9	Accounts of Foreign Branches	12 U.S.C. §604
10	Additional Banking Powers Authorized	12 U.S.C. §604a
	Interlocking Directorates and Employees (repealed, see 15 U.S.C. §19)	formerly at 12 U.S.C. §605

Paragraph or Subsection	*Topic*	*USC Section*
Section 25A	**Banking Corporations Authorized To Do Foreign Banking Business**	
1	Organization	12 U.S.C. §611
2	Purpose	12 U.S.C. §611a
3	Articles of Association	12 U.S.C. §612
4	Execution of Articles of Association	12 U.S.C. §613
5	Filing Organization Certificate; Issuance of Permit	12 U.S.C. §614
6	Powers; Regulations of the Board of Governors of the Federal Reserve System	12 U.S.C. §615
7	Purchase of Stock to Prevent Loss on Debt Previously Contracted	12 U.S.C. §615(c)
8	Restrictions on Business in United States	12 U.S.C. §616
9	Corporations Trading in Commodities or Attempting to Control Prices	12 U.S.C. §617
10	Capital Stock	12 U.S.C. §618
11	Citizenship of Stockholders	12 U.S.C. §619
12	Members of Board of Governors of the Federal Reserve System as Directors, Officers or Stockholders	12 U.S.C. §620
13	Shareholders' Liability; Corporation Not to Become Member	12 U.S.C. §621
14	Forfeiture of Charter for Violation of Law	12 U.S.C. §622
15	Voluntary Liquidation	12 U.S.C. §623
16	Appointment of Receiver or Conservator	12 U.S.C. §624
17	Stockholders' Meetings; Records; Reports; Examinations	12 U.S.C. §625
18	Dividends and Surplus Fund	12 U.S.C. §626
19	Taxation	12 U.S.C. §627
20	Extension of Corporate Existence	12 U.S.C. §628
21	Conversion of State Corporation into Federal Corporation	12 U.S.C. §629
22	Criminal Offenses of Directors, Officers, and Employees	12 U.S.C. §630
23	Representation that the United States is Liable for Obligations	12 U.S.C. §631

Paragraph or Subsection	*Topic*	*USC Section*
Section 25B	**Jurisdiction of Suits**	
1	Suits Arising Out of Foreign Banking Business	12 U.S.C. §632
2	Suits Involving Federal Reserve Banks	12 U.S.C. §632
3	Federal Reserve Banks Receiving Property of Foreign States and Central Banks	12 U.S.C. §632
4	Insured Banks Receiving Property of Foreign States and Central Banks	12 U.S.C. §632
5	Licenses Relating to Property of Foreign States and Central Banks	12 U.S.C. §632
6	Definitions	12 U.S.C. §632
Section 25C	**Potential Liability on Foreign Accounts**	12 U.S.C. §633
Section 26	**Borrowing Gold to Maintain Parity, Strenghten Gold Reserve** (deleted as obsolete)	formerly at 31 U.S.C. §409
Section 27	**Tax on National Bank Notes**	
1	National Currency Associations; Amendments to National Bank Act	omitted from U.S.C.
2	Tax on National Bank Notes Not Secured by United States Bonds	omitted from U.S.C.
Section 28	**Reduction of Capital of National Banks**	12 U.S.C. §59
Section 29	**Civil Money Penalties**	
(a)	First Tier	12 U.S.C. §504(a)
(b)	Second Tier	12 U.S.C. §504(b)
(c)	Third Tier	12 U.S.C. §504(c)
(d)	Maximum Amounts of Penalties for Violations in Subsection (c)	12 U.S.C. §504(d)
(e)	Assessment; etc.	12 U.S.C. §504(e)
(f)	Hearing	12 U.S.C. §504(f)
(g)	Disbursement	12 U.S.C. §504(g)

Paragraph or Subsection	*Topic*	*USC Section*
(h)	"Violate" Defined	12 U.S.C. §504(h)
(i)	Regulations	12 U.S.C. §504(i)
(m)	Notice Under This Section After Separation From Service	12 U.S.C. §504(m)
Section 30	**Saving Clause**	omitted from U.S.C.
Section 31	**Reservation of Right to Amend**	omitted from U.S.C.

[107th Congress Public Law 174]
[From the U.S. Government Printing Office]

<DOC>
[DOCID: f:publ174.107]

[[Page 565]]

NOTIFICATION AND FEDERAL EMPLOYEE ANTIDISCRIMINATION AND RETALIATION ACT OF 2002

[[Page 116 STAT. 566]]

Public Law 107-174
107th Congress

An Act

To require that Federal agencies be accountable for violations of antidiscrimination and whistleblower protection laws; to require that each Federal agency post quarterly on its public Web site, certain statistical data relating to Federal sector equal employment opportunity complaints filed with such agency; and for other purposes. <<NOTE: May 15, 2002 - [H.R. 169]>>

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, <<NOTE: Notification and Federal Employee Antidiscrimina- tion and Retaliation Act of 2002.>>

SECTION 1. SHORT TITLE; TABLE OF CONTENTS. <<NOTE: 5 USC 2301 note.>>

(a) Short Title.--This Act may be cited as the ``Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002''.
(b) Table of Contents.--The table of contents of this Act is as follows:

TITLE I--GENERAL PROVISIONS

SEC. 101. FINDINGS.

Congress finds that--

(1) Federal agencies cannot be run effectively if those agencies practice or tolerate discrimination;

(2) Congress has heard testimony from individuals, including representatives of the National Association for the Advancement of Colored People and the American Federation of Government Employees, that point to chronic problems of discrimination and retaliation against Federal employees;

[[Page 116 STAT. 567]]

(3) in August 2000, a jury found that the Environmental Protection Agency had discriminated against a senior social scientist, and awarded that scientist $600,000;

(4) in October 2000, an Occupational Safety and Health Administration investigation found that the Environmental Protection Agency had retaliated against a senior scientist for disagreeing with that agency on a matter of science and for helping Congress to carry out its oversight responsibilities;

(5) there have been several recent class action suits based on discrimination brought against Federal agencies, including the Federal Bureau of Investigation, the Bureau of Alcohol, Tobacco, and Firearms, the Drug Enforcement Administration, the Immigration and Naturalization Service, the United States Marshals Service, the Department of Agriculture, the United States Information Agency, and the Social Security Administration;

(6) notifying Federal employees of their rights under discrimination and whistleblower laws should increase Federal agency compliance with the law;

(7) requiring annual reports to Congress on the number and severity of discrimination and whistleblower cases brought against each Federal agency should enable Congress to improve its oversight over compliance by agencies with the law; and

(8) requiring Federal agencies to pay for any discrimination or whistleblower judgment, award, or settlement should improve agency accountability with respect to discrimination and whistleblower laws.

SEC. 102. SENSE OF CONGRESS.

It is the sense of Congress that--

(1) Federal agencies should not retaliate for court judgments or settlements relating to discrimination and whistleblower laws by targeting the claimant or other employees with reductions in compensation, benefits, or workforce to pay for such judgments or settlements;

(2) the mission of the Federal agency and the employment security of employees who are blameless in a whistleblower incident should not be compromised;

(3) Federal agencies should not use a reduction in force or furloughs as means of funding a reimbursement under this Act;

(4)(A) accountability in the enforcement of employee rights is not furthered by terminating--

(i) the employment of other employees; or
(ii) the benefits to which those employees are entitled through statute or contract; and

(B) this Act is not intended to authorize those actions;

(5)(A) nor is accountability furthered if Federal agencies react to the increased accountability under this Act by taking unfounded disciplinary actions against managers or by violating the procedural rights of managers who have been accused of discrimination; and

(B) Federal agencies should ensure that managers have adequate training in the management of a diverse workforce and in dispute resolution and other essential communication skills; and

[[Page 116 STAT. 568]]

(6)(A) Federal agencies are expected to reimburse the General Fund of the Treasury within a reasonable time under this Act; and

(B) a Federal agency, particularly if the amount of reimbursement under this Act is large relative to annual appropriations for that agency, may need to extend reimbursement over several years in order to avoid--

(i) reductions in force;
(ii) furloughs;
(iii) other reductions in compensation or benefits for the workforce of the agency; or
(iv) an adverse effect on the mission of the agency.

SEC. 103. DEFINITIONS.

For purposes of this Act--

(1) the term ``applicant for Federal employment'' means an individual applying for employment in or under a Federal agency;

(2) the term ``basis of alleged discrimination'' shall have the meaning given such term under section 303;

(3) the term ``Federal agency'' means an Executive agency (as defined in section 105 of title 5, United States Code), the United States Postal Service, or the Postal Rate Commission;

(4) the term ``Federal employee'' means an individual employed in or under a Federal agency;

(5) the term ``former Federal employee'' means an individual formerly employed in or under a Federal agency; and

(6) the term ``issue of alleged discrimination'' shall have the meaning given such term under section 303.

SEC. 104. EFFECTIVE DATE.

This Act and the amendments made by this Act shall take effect on the 1st day of the 1st fiscal year beginning more than 180 days after the date of the enactment of this Act.

TITLE II--FEDERAL EMPLOYEE DISCRIMINATION AND RETALIATION

SEC. 201. REIMBURSEMENT REQUIREMENT.

(a) Applicability.--This section applies with respect to any payment made in accordance with section 2414, 2517, 2672, or 2677 of title 28, United States Code, and under section 1304 of title 31, United States Code (relating to judgments, awards, and compromise settlements) to any Federal employee, former Federal employee, or applicant for Federal employment, in connection with any proceeding brought by or on behalf of

such employee, former employee, or applicant under--

(1) any provision of law cited in subsection (c); or

(2) any other provision of law which prohibits any form of discrimination, as identified under rules issued under section 204.

(b) Requirement.--An amount equal to the amount of each payment described in subsection (a) shall be reimbursed to the fund described in section 1304 of title 31, United States Code, out of any appropriation, fund, or other account (excluding any part of such appropriation, of such fund, or of such account available

[[Page 116 STAT. 569]]

for the enforcement of any Federal law) available for operating expenses of the Federal agency to which the discriminatory conduct involved is attributable as determined under section 204.

(c) Scope.--The provisions of law cited in this subsection are the following:

(1) Section 2302(b) of title 5, United States Code, as applied to discriminatory conduct described in paragraphs (1) and (8), or described in paragraph (9) of such section as applied to discriminatory conduct described in paragraphs (1) and (8), of such section.

(2) The provisions of law specified in section 2302(d) of title 5, United States Code.

SEC. 202. NOTIFICATION REQUIREMENT.

(a) In General.--Written notification of the rights and protections available to Federal employees, former Federal employees, and applicants for Federal employment (as the case may be) in connection with the respective provisions of law covered by paragraphs (1) and (2) of section 201(a) shall be provided to such employees, former employees, and applicants--

(1) in accordance with otherwise applicable provisions of law; or

(2) if, or to the extent that, no such notification would otherwise be required, in such time, form, and manner as shall under section 204 be required in order to carry out the requirements of this section.

(b) Posting on the Internet.--Any written notification under this section shall include, but not be limited to, the posting of the information required under paragraph (1) or (2) (as applicable) of subsection (a) on the Internet site of the Federal agency involved.

(c) Employee Training.--Each Federal agency shall provide to the employees of such agency training regarding the rights and remedies applicable to such employees under the laws cited in section 201(c).

SEC. 203. REPORTING REQUIREMENT. <<NOTE: Deadline.>>

(a) Annual Report.--Subject to subsection (b), not later than 180 days after the end of each fiscal year, each Federal agency shall submit to the Speaker of the House of Representatives, the President pro tempore of the Senate, the Committee on Governmental Affairs of the Senate, the Committee on Government Reform of the House of Representatives, each committee of Congress with jurisdiction relating to the agency, the Equal Employment Opportunity Commission, and the Attorney General an annual report which shall include, with respect to the fiscal year--

(1) the number of cases arising under each of the respective

provisions of law covered by paragraphs (1) and (2) of section 201(a) in which discrimination on the part of such agency was alleged;

(2) the status or disposition of cases described in paragraph (1);

(3) the amount of money required to be reimbursed by such agency under section 201 in connection with each of such cases, separately identifying the aggregate amount of such reimbursements attributable to the payment of attorneys' fees, if any;

[[Page 116 STAT. 570]]

(4) the number of employees disciplined for discrimination, retaliation, harassment, or any other infraction of any provision of law referred to in paragraph (1);

(5) the final year-end data posted under section 301(c)(1)(B) for such fiscal year (without regard to section 301(c)(2));

(6) a detailed description of--

(A) the policy implemented by that agency relating to appropriate disciplinary actions against a Federal employee who--

(i) discriminated against any individual in violation of any of the laws cited under section 201(a) (1) or (2); or

(ii) committed another prohibited personnel practice that was revealed in the investigation of a complaint alleging a violation of any of the laws cited under section 201(a) (1) or (2); and

(B) with respect to each of such laws, the number of employees who are disciplined in accordance with such policy and the specific nature of the disciplinary action taken;

(7) an analysis of the information described under paragraphs (1) through (6) (in conjunction with data provided to the Equal Employment Opportunity Commission in compliance with part 1614 of title 29 of the Code of Federal Regulations) including--

(A) an examination of trends;

(B) causal analysis;

(C) practical knowledge gained through experience; and

(D) any actions planned or taken to improve complaint or civil rights programs of the agency; and

(8) any adjustment (to the extent the adjustment can be ascertained in the budget of the agency) to comply with the requirements under section 201.

(b) First Report.--The 1st report submitted under subsection (a) shall include for each item under subsection (a) data for each of the 5 immediately preceding fiscal years (or, if data are not available for all 5 fiscal years, for each of those 5 fiscal years for which data are available).

SEC. 204. RULES AND GUIDELINES.

(a) Issuance <<NOTE: President.>> of Rules and Guidelines.--The President (or the designee of the President) shall issue--

(1) rules to carry out this title;

(2) rules to require that a comprehensive study be conducted in the executive branch to determine the best practices relating

to the appropriate disciplinary actions against Federal employees who commit the actions described under clauses (i) and (ii) of section 203(a)(6)(A); and

(3) based on the results of such study, advisory guidelines incorporating best practices that Federal agencies may follow to take such actions against such employees.

(b) Agency Notification <<NOTE: Deadline.>> Regarding Implementation of Guidelines.--Not later than 30 days after the issuance of guidelines under subsection (a), each Federal agency shall submit to the Speaker of the House of Representatives, the President pro tempore of the Senate, the Equal Employment Opportunity

[[Page 116 STAT. 571]]

Commission, and the Attorney General a written statement specifying in detail--

(1) whether such agency has adopted and will fully follow such guidelines;

(2) if such agency has not adopted such guidelines; the reasons for the failure to adopt such guidelines; and

(3) if such agency will not fully follow such guidelines, the reasons for the decision not to fully follow such guidelines and an explanation of the extent to which such agency will not follow such guidelines.

SEC. 205. CLARIFICATION OF REMEDIES.

Consistent with Federal law, nothing in this title shall prevent any Federal employee, former Federal employee, or applicant for Federal employment from exercising any right otherwise available under the laws of the United States.

SEC. 206. <<NOTE: Deadlines.>> STUDIES BY GENERAL ACCOUNTING OFFICE ON EXHAUSTION OF ADMINISTRATIVE REMEDIES AND ON ASCERTAINMENT OF CERTAIN DEPARTMENT OF JUSTICE COSTS.

(a) Study on Exhaustion of Administrative Remedies.--

(1) Study.--

(A) In general.--Not later than 180 days after the date of enactment of this Act, the General Accounting Office shall conduct a study relating to the effects of eliminating the requirement that Federal employees aggrieved by violations of any of the laws specified under section 201(c) exhaust administrative remedies before filing complaints with the Equal Employment Opportunity Commission.

(B) Contents.--The study shall include a detailed summary of matters investigated, information collected, and conclusions formulated that lead to determinations of how the elimination of such requirement will--

(i) expedite handling of allegations of such violations within Federal agencies and will streamline the complaint-filing process;

(ii) affect the workload of the Commission;

(iii) affect established alternative dispute resolution procedures in such agencies; and

(iv) affect any other matters determined by the General Accounting Office to be appropriate for consideration.

(2) Report.--Not later than 90 days after completion of the study required by paragraph (1), the General Accounting Office

shall submit to the Speaker of the House of Representatives, the President pro tempore of the Senate, the Equal Employment Opportunity Commission, and the Attorney General a report containing the information required to be included in such study.

(b) Study on Ascertainment of Certain Costs of the Department of Justice in Defending Discrimination and Whistleblower Cases.--

(1) Study.--Not later than 180 days after the date of enactment of this Act, the General Accounting Office shall conduct a study of the methods that could be used for, and the extent of any administrative burden that would be imposed on, the Department of Justice to ascertain the personnel and

[[Page 116 STAT. 572]]

administrative costs incurred in defending in each case arising from a proceeding identified under section 201(a) (1) and (2).

(2) Report.--Not later than 90 days after completion of the study required by paragraph (1), the General Accounting Office shall submit to the Speaker of the House of Representatives and the President pro tempore of the Senate a report containing the information required to be included in the study.

(c) Studies on Statutory Effects on Agency Operations.--

(1) In general.--Not later than 18 months after the date of enactment of this Act, the General Accounting Office shall conduct--

(A) a study on the effects of section 201 on the operations of Federal agencies; and

(B) a study on the effects of section 13 of the Contract Disputes Act of 1978 (41 U.S.C. 612) on the operations of Federal agencies.

(2) Contents.--Each study under paragraph (1) shall include, with respect to the applicable statutes of the study--

(A) a summary of the number of cases in which a payment was made in accordance with section 2414, 2517, 2672, or 2677 of title 28, United States Code, and under section 1304 of title 31, United States Code;

(B) a summary of the length of time Federal agencies used to complete reimbursements of payments described under subparagraph (A); and

(C) conclusions that assist in making determinations on how the reimbursements of payments described under subparagraph (A) will affect--

(i) the operations of Federal agencies;

(ii) funds appropriated on an annual basis;

(iii) employee relations and other human capital matters;

(iv) settlements; and

(v) any other matter determined by the General Accounting Office to be appropriate for consideration.

(3) Reports.--Not later than 90 days after the completion of each study under paragraph (1), the General Accounting Office shall submit a report on each study, respectively, to the Speaker of the House of Representatives, the President pro tempore of the Senate, the Committee on Governmental Affairs of the Senate, the Committee on Government Reform of the House of Representatives, and the Attorney General.

(d) Study on Administrative and Personnel Costs Incurred by the

Department of the Treasury.--

(1) In general.--Not later than 1 year after the date of enactment of this Act, the General Accounting Office shall conduct a study on the extent of any administrative and personnel costs incurred by the Department of the Treasury to account for payments made in accordance with section 2414, 2517, 2672, or 2677 of title 28, United States Code, and under section 1304 of title 31, United States Code, as a result of--

(A) this Act; and

(B) the Contracts Dispute Act of 1978 (41 U.S.C. 601 note; Public Law 95-563).

(2) Report.--Not later than 90 days after the completion of the study under paragraph (1), the General Accounting Office shall submit a report on the study to the Speaker of the

[[Page 116 STAT. 573]]

House of Representatives, the President pro tempore of the Senate, the Committee on Governmental Affairs of the Senate, the Committee on Government Reform of the House of Representatives, and the Attorney General.

TITLE III--EQUAL EMPLOYMENT OPPORTUNITY COMPLAINT DATA DISCLOSURE

SEC. 301. <<NOTE: Internet. Public information.>> DATA TO BE POSTED BY EMPLOYING FEDERAL AGENCIES.

(a) In General.--Each Federal agency shall post on its public Web site, in the time, form, and manner prescribed under section 303 (in conformance with the requirements of this section), summary statistical data relating to equal employment opportunity complaints filed with such agency by employees or former employees of, or applicants for employment with, such agency.

(b) Content Requirements.--The data posted by a Federal agency under this section shall include, for the then current fiscal year, the following:

(1) The number of complaints filed with such agency in such fiscal year.

(2) The number of individuals filing those complaints (including as the agent of a class).

(3) The number of individuals who filed 2 or more of those complaints.

(4) The number of complaints (described in paragraph (1)) in which each of the various bases of alleged discrimination is alleged.

(5) The number of complaints (described in paragraph (1)) in which each of the various issues of alleged discrimination is alleged.

(6) The average length of time, for each step of the process, it is taking such agency to process complaints (taking into account all complaints pending for any length of time in such fiscal year, whether first filed in such fiscal year or earlier). Average times under this paragraph shall be posted--

(A) for all such complaints,

(B) for all such complaints in which a hearing before an administrative judge of the Equal Employment Opportunity Commission is not requested, and

(C) for all such complaints in which a hearing before an administrative judge of the Equal Employment Opportunity Commission is requested.

(7) The total number of final agency actions rendered in such fiscal year involving a finding of discrimination and, of

that number--

(A) the number and percentage that were rendered without a hearing before an administrative judge of the Equal Employment Opportunity Commission, and

(B) the number and percentage that were rendered after a hearing before an administrative judge of the Equal Employment Opportunity Commission.

(8) Of the total number of final agency actions rendered in such fiscal year involving a finding of discrimination--

[[Page 116 STAT. 574]]

(A) the number and percentage involving a finding of discrimination based on each of the respective bases of alleged discrimination, and

(B) of the number specified under subparagraph (A) for each of the respective bases of alleged discrimination--

(i) the number and percentage that were rendered without a hearing before an administrative judge of the Equal Employment Opportunity Commission, and

(ii) the number and percentage that were rendered after a hearing before an administrative judge of the Equal Employment Opportunity Commission.

(9) Of the total number of final agency actions rendered in such fiscal year involving a finding of discrimination--

(A) the number and percentage involving a finding of discrimination in connection with each of the respective issues of alleged discrimination, and

(B) of the number specified under subparagraph (A) for each of the respective issues of alleged discrimination--

(i) the number and percentage that were rendered without a hearing before an administrative judge of the Equal Employment Opportunity Commission, and

(ii) the number and percentage that were rendered after a hearing before an administrative judge of the Equal Employment Opportunity Commission.

(10)(A) Of the total number of complaints pending in such fiscal year (as described in the parenthetical matter in paragraph (6)), the number that were first filed before the start of the then current fiscal year.

(B) With respect to those pending complaints that were first filed before the start of the then current fiscal year--

(i) the number of individuals who filed those complaints, and

(ii) the number of those complaints which are at the various steps of the complaint process.

(C) Of the total number of complaints pending in such fiscal year (as described in the parenthetical matter in paragraph (6)), the total number of complaints with respect to which the agency violated the requirements of section 1614.106(e)(2) of title 29 of the Code of Federal Regulations (as in effect on July 1, 2000, and amended from time to time) by failing to conduct within 180 days of the filing of such complaints an impartial and appropriate investigation of such complaints.

(c) Timing and Other Requirements.--

(1) Current year data.--Data posted under this section for the then current fiscal year shall include both--

(A) interim year-to-date data, updated quarterly, and

(B) final year-end data.

(2) Data for prior years.--The data posted by a Federal agency under this section for a fiscal year (both interim and final) shall include, for each item under subsection (b), such agency's corresponding year-end data for each of the 5 immediately preceding fiscal years (or, if not available for all 5 fiscal years, for however many of those 5 fiscal years for which data are available).

[[Page 116 STAT. 575]]

SEC. 302. <<NOTE: Internet. Public information.>> DATA TO BE POSTED BY THE EQUAL EMPLOYMENT OPPORTUNITY COMMISSION.

(a) In General.--The Equal Employment Opportunity Commission shall post on its public Web site, in the time, form, and manner prescribed under section 303 for purposes of this section, summary statistical data relating to--

(1) hearings requested before an administrative judge of the Commission on complaints described in section 301, and

(2) appeals filed with the Commission from final agency actions on complaints described in section 301.

(b) Specific Requirements.--The data posted under this section shall, with respect to the hearings and appeals described in subsection (a), include summary statistical data corresponding to that described in paragraphs (1) through (10) of section 301(b), and shall be subject to the same timing and other requirements as set forth in section 301(c).

(c) Coordination.--The data required under this section shall be in addition to the data the Commission is required to post under section 301 as an employing Federal agency.

SEC. 303. RULES.

The Equal Employment Opportunity Commission shall issue any rules necessary to carry out this title.

Approved May 15, 2002.

LEGISLATIVE HISTORY--H.R. 169:

HOUSE REPORTS: No. 107-101, Pt. 1 (Comm. on the Judiciary).
SENATE REPORTS: No. 107-143 (Comm. on Governmental Affairs).
CONGRESSIONAL RECORD, Vol. 147 (2001):
Oct. 2, considered and passed House.
Apr. 23, considered and passed Senate, amended.
Apr. 30, House concurred in Senate amendments.

<all>

ELECTRONIC CODE OF FEDERAL REGULATIONS

e-CFR Data is current as of January 16, 2015

Title 5 → Chapter I → Subchapter B → Part 724

Title 5: Administrative Personnel

PART 724—IMPLEMENTATION OF TITLE II OF THE NOTIFICATION AND FEDERAL EMPLOYEE ANTIDISCRIMINATION AND RETALIATION ACT OF 2002

Contents

AUTHORITY: Sec. 204 of Pub. L. 107-174, 116 Stat. 566; Presidential Memorandum dated July 8, 2003, "Delegation of Authority Under Section 204(a) of the Notification and Federal Employee Antidiscrimination Act of 2002."

SOURCE: 71 FR 27187, May 10, 2006, unless otherwise noted.

Back to Top

Subpart A—Reimbursement of Judgement Fund

Back to Top

§724.101 Purpose and scope.

This subpart implements Title II of the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 concerning the obligation of Federal agencies to reimburse the Judgment Fund for payments. The regulations describe agency obligations and the procedures for reimbursement and compliance.

Back to Top

§724.102 Definitions.

In this part:

Agency means an Executive agency as defined in 5 U.S.C. 105, the United States Postal Service, or the Postal Rate Commission;

Antidiscrimination Laws refers to 5 U.S.C. 2302(b)(1), 5 U.S.C. 2302(b)(9) as applied to conduct described in 5 U.S.C. 2302(b)(1), 29 U.S.C. 206(d), 29 U.S.C. 631, 29 U.S.C. 633a, 29 U.S.C. 791 and 42 U.S.C. 2000e-16.

Applicant for Federal employment means an individual applying for employment in or under a Federal agency;

Discipline means any one or a combination of the following actions: reprimand, suspension without pay, reduction in grade or pay, or removal.

Employee means an individual employed in or under a Federal agency;

Former Employee means an individual formerly employed in or under a Federal agency;

Judgment Fund means the Judgment Fund established by 31 U.S.C. 1304;

No FEAR Act means the “Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002;”

Notice means the written information provided by Federal agencies about the rights and protections available under Federal Antidiscrimination Laws and Whistleblower Protection Laws.

Payment, subject to the following exception, means a disbursement from the Judgment Fund on or after October 1, 2003, to an employee, former employee, or applicant for Federal employment, in accordance with 28 U.S.C. 2414, 2517, 2672, 2677 or with 31 U.S.C. 1304, that involves alleged discriminatory or retaliatory conduct described in 5 U.S.C. 2302(b)(1) and (b)(8) or (b)(9) as applied to conduct described in 5 U.S.C. 2302(b)(1) and/or (b)(8) or conduct described in 29 U.S.C. 206(d), 29 U.S.C. 631, 29 U.S.C. 633a, 29 U.S.C. 791 and 42 U.S.C. 2000e-16. For a proceeding involving more than one disbursement from the Judgment Fund, however, this term shall apply only if the first disbursement occurred on or after October 1, 2003.

Training means the process by which Federal agencies instruct their employees regarding the rights and remedies applicable to such employees under the Federal Antidiscrimination Laws and Whistleblower Protection Laws.

Whistleblower Protection Laws refers to 5 U.S.C. 2302(b)(8) or 5 U.S.C. 2302(b)(9) as applied to conduct described in 5 U.S.C. 2302(b)(8).

[71 FR 27187, May 10, 2006, as amended at 71 FR 41098, July 20, 2006; 71 FR 78037, Dec. 28, 2006]

Back to Top

§724.103 Agency obligations.

A Federal agency (or its successor agency) must reimburse the Judgment Fund for payments covered by the No FEAR Act. Such reimbursement must be made within a reasonable time as described in §724.104.

Back to Top

§724.104 Procedures.

(a) The procedures that agencies must use to reimburse the Judgment Fund are those prescribed by the Financial Management Service (FMS), the Department of the Treasury, in Chapter 3100 of the Treasury Financial Manual. All reimbursements to the Judgment Fund covered by the No FEAR Act are expected to be fully collectible from the agency. FMS will provide written notice to the agency's Chief Financial Officer within 15 business days after payment from the Judgment Fund.

(b) Within 45 business days of receiving the FMS notice, agencies must reimburse the Judgment Fund or contact FMS to make arrangements in writing for reimbursement.

Back to Top

§724.105 Compliance.

An agency's failure to reimburse the Judgment Fund, to contact FMS within 45 business days after receipt of an FMS notice for reimbursement under §724.104 will be recorded on an annual basis and posted on the FMS Web site. After an agency meets the requirements of §724.104, the recording will be eliminated no later than the next annual posting process.

Back to Top

§724.106 Effective date.

This subpart is effective on October 1, 2003.

Back to Top

Subpart B—Notification of Rights and Protections and Training

SOURCE: 71 FR 41098, July 20, 2006, unless otherwise noted.

Back to Top

§724.201 Purpose and scope.

(a) This subpart implements Title II of the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 concerning the obligation of Federal agencies to notify all employees, former employees, and applicants for Federal employment of the rights and protections available to them under the Federal Antidiscrimination Laws and Whistleblower Protection Laws. This subpart also implements Title II concerning the obligation of agencies to train their employees on such rights and remedies. The regulations describe agency obligations and the procedures for written notification and training.

(b) Pursuant to section 205 of the No FEAR Act, neither that Act nor this notice creates, expands or reduces any rights otherwise available to any employee, former employee or applicant under the

laws of the United States, including the provisions of law specified in 5 U.S.C. 2302(d).

Back to Top

§724.202 Notice obligations.

(a) Each agency must provide notice to all of its employees, former employees, and applicants for Federal employment about the rights and remedies available under the Antidiscrimination Laws and Whistleblower Protection Laws applicable to them.

(b) The notice under this part must be titled, “No FEAR Act Notice.”

(c) Each agency must provide initial notice within 60 calendar days after September 18, 2006. Thereafter, the notice must be provided by the end of each successive fiscal year and any posted materials must remain in place until replaced or revised.

(d) After the initial notice, each agency must provide the notice to new employees within 90 calendar days of entering on duty.

(e) Each agency must provide the notice to its employees in paper (e.g., letter, poster or brochure) and/or electronic form (e.g., e-mail, internal agency electronic site, or Internet Web site). Each agency must publish the *initial* notice in the FEDERAL REGISTER. Agencies with Internet Web sites must also post the notice on those Web sites, in compliance with section 508 of the Rehabilitation Act of 1973, as amended. For agencies with components that operate Internet Web sites, the notice must be made available by hyperlinks from the Internet Web sites of both the component and the parent agency. An agency may meet its paper and electronic notice obligation to former employees and applicants by publishing the initial notice in the FEDERAL REGISTER and posting the notice on its Internet Web site if it has one.

(f) To the extent required by law and upon request by employees, former employees and applicants, each agency must provide the notice in alternative, accessible formats.

(g) Unless an agency is exempt from the cited statutory provisions, the following is the minimum text to be included in the notice. Each agency may incorporate additional information within the model paragraphs, as appropriate.

MODEL PARAGRAPHS

NO FEAR ACT NOTICE

On May 15, 2002, Congress enacted the “Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002,” which is now known as the No FEAR Act. One purpose of the Act is to “require that Federal agencies be accountable for violations of antidiscrimination and whistleblower protection laws.” Public Law 107-174, Summary. In support of this purpose, Congress found that “agencies cannot be run effectively if those agencies practice or tolerate discrimination.” Public Law 107-174, Title I, General Provisions, section 101(1).

The Act also requires this agency to provide this notice to Federal employees, former Federal employees and applicants for Federal employment to inform you of the rights and protections available to you under Federal antidiscrimination and whistleblower protection laws.

ANTIDISCRIMINATION LAWS

A Federal agency cannot discriminate against an employee or applicant with respect to the terms, conditions or privileges of employment on the basis of race, color, religion, sex, national origin, age, disability, marital status or political affiliation. Discrimination on these bases is prohibited by one or more of the following statutes: 5 U.S.C. 2302(b)(1), 29 U.S.C. 206(d), 29 U.S.C. 631, 29 U.S.C. 633a, 29 U.S.C. 791 and 42 U.S.C. 2000e-16.

If you believe that you have been the victim of unlawful discrimination on the basis of race, color, religion, sex, national origin or disability, you must contact an Equal Employment Opportunity (EEO) counselor within 45 calendar days of the alleged discriminatory action, or, in the case of a personnel action, within 45 calendar days of the effective date of the action, before you can file a formal complaint of discrimination with your agency. *See, e.g.* 29 CFR 1614. If you believe that you have been the victim of unlawful discrimination on the basis of age, you must either contact an EEO counselor as noted above or give notice of intent to sue to the Equal Employment Opportunity Commission (EEOC) within 180 calendar days of the alleged discriminatory action. If you are alleging discrimination based on marital status or political affiliation, you may file a written complaint with the U.S. Office of Special Counsel (OSC) (*see* contact information below). In the alternative (or in some cases, in addition), you may pursue a discrimination complaint by filing a grievance through your agency's administrative or negotiated grievance procedures, if such procedures apply and are available.

Whistleblower Protection Laws

A Federal employee with authority to take, direct others to take, recommend or approve any personnel action must not use that authority to take or fail to take, or threaten to take or fail to take, a personnel action against an employee or applicant because of disclosure of information by that individual that is reasonably believed to evidence violations of law, rule or regulation; gross mismanagement; gross waste of funds; an abuse of authority; or a substantial and specific danger to public health or safety, unless disclosure of such information is specifically prohibited by law and such information is specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs.

Retaliation against an employee or applicant for making a protected disclosure is prohibited by 5 U.S.C. 2302(b)(8). If you believe that you have been the victim of whistleblower retaliation, you may file a written complaint (Form OSC-11) with the U.S. Office of Special Counsel at 1730 M Street NW., Suite 218, Washington, DC 20036-4505 or online through the OSC Web site—*http://www.osc.gov.*

Retaliation for Engaging in Protected Activity

A Federal agency cannot retaliate against an employee or applicant because that individual exercises his or her rights under any of the Federal antidiscrimination or whistleblower protection laws listed above. If you believe that you are the victim of retaliation for engaging in protected activity, you must follow, as appropriate, the procedures described in the Antidiscrimination Laws and Whistleblower Protection Laws sections or, if applicable, the administrative or negotiated grievance procedures in order to pursue any legal remedy.

Disciplinary Actions

Under the existing laws, each agency retains the right, where appropriate, to discipline a Federal employee for conduct that is inconsistent with Federal Antidiscrimination and Whistleblower Protection Laws up to and including removal. If OSC has initiated an investigation under 5 U.S.C. 1214, however, according to 5 U.S.C. 1214(f), agencies must seek approval from the Special Counsel to discipline employees for, among other activities, engaging in prohibited retaliation. Nothing in the No FEAR Act alters existing laws or permits an agency to take unfounded disciplinary action against a Federal employee or to violate the procedural rights of a Federal employee who has been accused of discrimination

Additional Information

For further information regarding the No FEAR Act regulations, refer to 5 CFR part 724, as well as the appropriate offices within your agency (e.g., EEO/civil rights office, human resources office or legal office). Additional information regarding Federal antidiscrimination, whistleblower protection and retaliation laws can be found at the EEOC Web site—*http://www.eeoc.gov* and the OSC Web site—*http://www.osc.gov.*

Existing Rights Unchanged

Pursuant to section 205 of the No FEAR Act, neither the Act nor this notice creates, expands or reduces any rights otherwise available to any employee, former employee or applicant under the laws of the United States, including the provisions of law specified in 5 U.S.C. 2302(d).

Back to Top

§724.203 Training obligations.

(a) Each agency must develop a written plan to train all of its employees (including supervisors and managers) about the rights and remedies available under the Antidiscrimination Laws and Whistleblower Protection Laws applicable to them.

(b) Each agency shall have the discretion to develop the instructional materials and method of its training plan. Each agency training plan shall describe:

(1) The instructional materials and method of the training,

(2) The training schedule, and

(3) The means of documenting completion of training.

(c) Each agency may contact EEOC and/or OSC for information and/or assistance regarding the agency's training program. Neither agency, however, shall have authority under this regulation to review or approve an agency's training plan.

(d) Each agency is *encouraged* to implement its training as soon as possible, but *required* to complete the initial training under this subpart for all employees (including supervisors and managers) by December 17, 2006. Thereafter, each agency must train all employees on a training cycle of no longer than every 2 years.

(e) After the initial training is completed, each agency must train new employees as part of its agency orientation program or other training program. Any agency that does not use a new employee orientation program for this purpose must train new employees within 90 calendar days of the new employees' appointment.

Back to Top

Subpart C—Annual Report

SOURCE: 71 FR 78037, Dec. 28, 2006, unless otherwise noted.

Back to Top

§724.301 Purpose and scope.

This subpart implements Title II of the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 concerning the obligation of Federal agencies to report on specific topics concerning Federal Antidiscrimination Laws and Whistleblower Protection Laws applicable to them covering employees, former employees, and applicants for Federal employment.

Back to Top

§724.302 Reporting obligations.

(a) Except as provided in paragraph (b) of this section, each agency must report no later than 180 calendar days after the end of each fiscal year the following items:

(1) The number of cases in Federal court pending or resolved in each fiscal year and arising under each of the respective provisions of the Federal Antidiscrimination Laws and Whistleblower Protection Laws applicable to them as defined in §724.102 of subpart A of this part in which an

employee, former Federal employee, or applicant alleged a violation(s) of these laws, separating data by the provision(s) of law involved;

(2) In the aggregate, for the cases identified in paragraph (a)(1) of this section and separated by provision(s) of law involved:

(i) The status or disposition (including settlement);

(ii) The amount of money required to be reimbursed to the Judgment Fund by the agency for payments as defined in §724.102 of subpart A of this part;

(iii) The amount of reimbursement to the Fund for attorney's fees where such fees have been separately designated;

(3) In connection with cases identified in paragraph (a)(1) of this section, the total number of employees in each fiscal year disciplined as defined in §724.102 of subpart A of this part and the specific nature, e.g., reprimand, etc., of the disciplinary actions taken, separated by the provision(s) of law involved;

(4) The final year-end data about discrimination complaints for each fiscal year that was posted in accordance with Equal Employment Opportunity Regulations at subpart G of title 29 of the Code of Federal Regulations (implementing section 301(c)(1)(B) of the No FEAR Act);

(5) Whether or not in connection with cases in Federal court, the number of employees in each fiscal year disciplined as defined in §724.102 of subpart A of this part in accordance with any agency policy described in paragraph (a)(6) of this section. The specific nature, e.g., reprimand, etc., of the disciplinary actions taken must be identified.

(6) A detailed description of the agency's policy for taking disciplinary action against Federal employees for conduct that is inconsistent with Federal Antidiscrimination Laws and Whistleblower Protection Laws or for conduct that constitutes another prohibited personnel practice revealed in connection with agency investigations of alleged violations of these laws;

(7) An analysis of the information provided in paragraphs (a)(1) through (6) of this section in conjunction with data provided to the Equal Employment Opportunity Commission in compliance with 29 CFR part 1614 subpart F of the Code of Federal Regulations. Such analysis must include:

(i) An examination of trends;

(ii) Causal analysis;

(iii) Practical knowledge gained through experience; and

(iv) Any actions planned or taken to improve complaint or civil rights programs of the agency with the goal of eliminating discrimination and retaliation in the workplace;

(8) For each fiscal year, any adjustment needed or made to the budget of the agency to comply with its Judgment Fund reimbursement obligation(s) incurred under §724.103 of subpart A of this part; and

(9) The agency's written plan developed under §724.203(a) of subpart B of this part to train its employees.

(b) The first report also must provide information for the data elements in paragraph (a) of this section for each of the five fiscal years preceding the fiscal year on which the first report is based to the extent that such data is available. Under the provisions of the No FEAR Act, the first report was due March 30, 2005 without regard to the status of the regulations. Thereafter, under the provisions of

the No FEAR Act, agency reports are due annually on March 30th. Agencies that have submitted their reports before these regulations became final must ensure that they contain data elements 1 through 8 of paragraph (a) of this section and provide any necessary supplemental reports by April 25, 2007. Future reports must include data elements 1 through 9 of paragraph (a) of this section.

(c) Agencies must provide copies of each report to the following:

(1) Speaker of the U.S. House of Representatives;

(2) President Pro Tempore of the U.S. Senate;

(3) Committee on Governmental Affairs, U.S. Senate;

(4) Committee on Government Reform, U.S. House of Representatives;

(5) Each Committee of Congress with jurisdiction relating to the agency;

(6) Chair, Equal Employment Opportunity Commission;

(7) Attorney General; and

(8) Director, U.S. Office of Personnel Management.

Back to Top

Subpart D—Best Practices

SOURCE: 71 FR 78037, Dec. 28, 2006, unless otherwise noted.

Back to Top

§724.401 Purpose and scope.

This subpart implements Title II of the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 concerning the obligation of the President or his designee (OPM) to conduct a comprehensive study of best practices in the executive branch for taking disciplinary actions against employees for conduct that is inconsistent with Federal Antidiscrimination and Whistleblower Protection Laws and the obligation to issue advisory guidelines for agencies to follow in taking appropriate disciplinary actions in such circumstances.

Back to Top

§724.402 Best practices study.

(a) OPM will conduct a comprehensive study in the executive branch to identify best practices for taking appropriate disciplinary actions against Federal employees for conduct that is inconsistent with Federal Antidiscrimination and Whistleblower Protection Laws.

(b) The comprehensive study will include a review of agencies' discussions of their policies for taking such disciplinary actions as reported under §724.302 of subpart C of this part.

Back to Top

§724.403 Advisory guidelines.

OPM will issue advisory guidelines to Federal agencies incorporating the best practices identified under §724.402 that agencies may follow to take appropriate disciplinary actions against employees

for conduct that is inconsistent with Federal Antidiscrimination Laws and Whistleblower Laws.

Back to Top

§724.404 Agency obligations.

(a) Within 30 working days of issuance of the advisory guidelines required by §724.403, each agency must prepare a written statement describing in detail:

(1) Whether it has adopted the guidelines and if it will fully follow the guidelines;

(2) If such agency has not adopted the guidelines, the reasons for non-adoption; and

(3) If such agency will not fully follow the guidelines, the reasons for the decision not to do so and an explanation of the extent to which the agency will not follow the guidelines.

(b) Each agency's written statement must be provided within the time limit stated in paragraph (a) of this section to the following:

(1) Speaker of the U.S. House of Representatives;

(2) President Pro Tempore of the U.S. Senate;

(3) Chair, Equal Employment Opportunity Commission;

(4) Attorney General; and

(5) Director, U.S. Office of Personnel Management.

Back to Top

U.S. Equal Employment Opportunity Commission

Title VII of the Civil Rights Act of 1964

EDITOR'S NOTE: The following is the text of Title VII of the Civil Rights Act of 1964 (Pub. L. 88-352) (Title VII), as amended, as it appears in volume 42 of the United States Code, beginning at section 2000e. Title VII prohibits employment discrimination based on race, color, religion, sex and national origin. The Civil Rights Act of 1991 (Pub. L. 102-166) (CRA) and the Lily Ledbetter Fair Pay Act of 2009 (Pub. L. 111-2) amend several sections of Title VII. In addition, section 102 of the CRA (which is printed elsewhere in this publication) amends the Revised Statutes by adding a new section following section 1977 (42 U.S.C. 1981), to provide for the recovery of compensatory and punitive damages in cases of intentional violations of Title VII, the Americans with Disabilities Act of 1990, and section 501 of the Rehabilitation Act of 1973. Cross references to Title VII as enacted appear in italics following each section heading. Editor's notes also appear in italics.

An Act

To enforce the constitutional right to vote, to confer jurisdiction upon the district courts of the United States to provide injunctive relief against discrimination in public accommodations, to authorize the attorney General to institute suits to protect constitutional rights in public facilities and public education, to extend the Commission on Civil Rights, to prevent discrimination in federally assisted programs, to establish a Commission on Equal Employment Opportunity, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the “Civil Rights Act of 1964”.

* * *

DEFINITIONS

SEC. 2000e. *[Section 701]*

For the purposes of this subchapter-

(a) The term “person” includes one or more individuals, governments, governmental agencies, political subdivisions, labor unions, partnerships, associations, corporations, legal representatives, mutual companies, joint-stock companies, trusts, unincorporated organizations, trustees, trustees in cases under Title 11 *[originally, bankruptcy],* or receivers.

(b) The term “employer” means a person engaged in an industry affecting commerce who has fifteen or more employees for each working day in each of twenty or more calendar weeks in the current or preceding calendar year, and any agent of such a person, but such term does not include (1) the United States, a corporation wholly owned by the Government of the United States, an Indian tribe, or any department or agency of the District of Columbia subject by statute to procedures of the competitive service (as defined in section 2102 of Title 5 *[United States Code]*), or

(2) a bona fide private membership club (other than a labor organization) which is exempt from taxation under section 501(c) of Title 26 *[the Internal Revenue Code of 1986]*, except that during the first year after March 24, 1972 *[the date of enactment of the Equal Employment Opportunity Act of 1972]*, persons having fewer than twenty-five employees (and their agents) shall not be considered employers.

(c) The term “employment agency” means any person regularly undertaking with or without compensation to procure employees for an employer or to procure for employees opportunities to work for an employer and includes an agent of such a person.

(d) The term “labor organization” means a labor organization engaged in an industry affecting commerce, and any agent of such an organization, and includes any organization of any kind, any agency, or employee representation committee, group, association, or plan so engaged in which employees participate and which exists for the purpose, in whole or in part, of dealing with employers concerning grievances, labor disputes, wages, rates of pay, hours, or other terms or conditions of employment, and any conference, general committee, joint or system board, or joint council so engaged which is subordinate to a national or international labor organization.

(e) A labor organization shall be deemed to be engaged in an industry affecting commerce if (1) it maintains or operates

a hiring hall or hiring office which procures employees for an employer or procures for employees opportunities to work for an employer, or (2) the number of its members (or, where it is a labor organization composed of other labor organizations or their representatives, if the aggregate number of the members of such other labor organization) is (A) twenty-five or more during the first year after March 24, 1972 *[the date of enactment of the Equal Employment Opportunity Act of 1972]*, or (B) fifteen or more thereafter, and such labor organization-

(1) is the certified representative of employees under the provisions of the National Labor Relations Act, as amended *[29 U.S.C. 151 et seq.]*, or the Railway Labor Act, as amended *[45 U.S.C. 151 et seq.]*;

(2) although not certified, is a national or international labor organization or a local labor organization recognized or acting as the representative of employees of an employer or employers engaged in an industry affecting commerce; or

(3) has chartered a local labor organization or subsidiary body which is representing or actively seeking to represent employees of employers within the meaning of paragraph (1) or (2); or

(4) has been chartered by a labor organization representing or actively seeking to represent employees within the meaning of paragraph (1) or (2) as the local or subordinate body through which such employees may enjoy membership or become affiliated with such labor organization; or

(5) is a conference, general committee, joint or system board, or joint council subordinate to a national or international labor organization, which includes a labor organization engaged in an industry affecting commerce within the meaning of any of the preceding paragraphs of this subsection.

(f) The term “employee” means an individual employed by an employer, except that the term “employee” shall not include any person elected to public office in any State or political subdivision of any State by the qualified voters thereof, or any person chosen by such officer to be on such officer’s personal staff, or an appointee on the policy making level or an immediate adviser with respect to the exercise of the constitutional or legal powers of the office. The exemption set forth in the preceding sentence shall not include employees subject to the civil service laws of a State government, governmental agency or political subdivision. With respect to employment in a foreign country, such term includes an individual who is a citizen of the United States.

(g) The term “commerce” means trade, traffic, commerce, transportation, transmission, or communication among the several States; or between a State and any place outside thereof; or within the District of Columbia, or a possession of the United States; or between points in the same State but through a point outside thereof.

(h) The term “industry affecting commerce” means any activity, business, or industry in commerce or in which a labor dispute would hinder or obstruct commerce or the free flow of commerce and includes any activity or industry “affecting commerce” within the meaning of the Labor-Management Reporting and Disclosure Act of 1959 *[29 U.S.C. 401 et seq.]*, and further includes any governmental industry, business, or activity.

(i) The term “State” includes a State of the United States, the District of Columbia, Puerto Rico, the Virgin Islands, American Samoa, Guam, Wake Island, the Canal Zone, and Outer Continental Shelf lands defined in the Outer Continental Shelf Lands Act *[43 U.S.C. 1331 et seq.]*.

(j) The term “religion” includes all aspects of religious observance and practice, as well as belief, unless an employer demonstrates that he is unable to reasonably accommodate to an employee’s or prospective employee’s religious observance or practice without undue hardship on the conduct of the employer’s business.

(k) The terms “because of sex” or “on the basis of sex” include, but are not limited to, because of or on the basis of pregnancy, childbirth, or related medical conditions; and women affected by pregnancy, childbirth, or related medical conditions shall be treated the same for all employment-related purposes, including receipt of benefits under fringe benefit programs, as other persons not so affected but similar in their ability or inability to work, and nothing in section 2000e-2(h) of this title *[section 703(h)]* shall be interpreted to permit otherwise. This subsection shall not require an employer to pay for health insurance benefits for abortion, except where the life of the mother would be endangered if the fetus were carried to term, or except where medical complications have arisen from an abortion: Provided, That nothing herein shall preclude an employer from providing abortion benefits or otherwise affect bargaining agreements in regard to abortion.

(l) The term “complaining party” means the Commission, the Attorney General, or a person who may bring an action or proceeding under this subchapter.

(m) The term “demonstrates” means meets the burdens of production and persuasion.

(n) The term “respondent” means an employer, employment agency, labor organization, joint labor management committee controlling apprenticeship or other training or retraining program, including an on-the-job training program, or Federal entity subject to section 2000e-16 of this title.

APPLICABILITY TO FOREIGN AND RELIGIOUS EMPLOYMENT

SEC. 2000e-1. *[Section 702]*

(a) Inapplicability of subchapter to certain aliens and employees of religious entities

This subchapter shall not apply to an employer with respect to the employment of aliens outside any State, or to a religious corporation, association, educational institution, or society with respect to the employment of individuals of a particular religion to perform work connected with the carrying on by such corporation, association, educational institution, or society of its activities.

(b) Compliance with statute as violative of foreign law

It shall not be unlawful under section 2000e-2 or 2000e-3 of this title *[section 703 or 704]* for an employer (or a corporation controlled by an employer), labor organization, employment agency, or joint labor-management committee controlling apprenticeship or other training or retraining (including on-the-job training programs) to take any action otherwise prohibited by such section, with respect to an employee in a workplace in a foreign country if compliance with such section would cause such employer (or such corporation), such organization, such agency, or such committee to violate the law of the foreign country in which such workplace is located.

(c) Control of corporation incorporated in foreign country

> (1) If an employer controls a corporation whose place of incorporation is a foreign country, any practice prohibited by section 2000e-2 or 2000e-3 of this title *[section 703 or 704]* engaged in by such corporation shall be presumed to be engaged in by such employer.
>
> (2) Sections 2000e-2 and 2000e-3 of this title *[sections 703 and 704]* shall not apply with respect to the foreign operations of an employer that is a foreign person not controlled by an American employer.
>
> (3) For purposes of this subsection, the determination of whether an employer controls a corporation shall be based on-
>
> > (A) the interrelation of operations;
> >
> > (B) the common management;
> >
> > (C) the centralized control of labor relations; and
> >
> > (D) the common ownership or financial control, of the employer and the corporation.

UNLAWFUL EMPLOYMENT PRACTICES

SEC. 2000e-2. *[Section 703]*

(a) Employer practices

It shall be an unlawful employment practice for an employer -

> (1) to fail or refuse to hire or to discharge any individual, or otherwise to discriminate against any individual with respect to his compensation, terms, conditions, or privileges of employment, because of such individual's race, color, religion, sex, or national origin; or
>
> (2) to limit, segregate, or classify his employees or applicants for employment in any way which would deprive or tend to deprive any individual of employment opportunities or otherwise adversely affect his status as an employee, because of such individual's race, color, religion, sex, or national origin.

(b) Employment agency practices

It shall be an unlawful employment practice for an employment agency to fail or refuse to refer for employment, or otherwise to discriminate against, any individual because of his race, color, religion, sex, or national origin, or to classify or refer for employment any individual on the basis of his race, color, religion, sex, or national origin.

(c) Labor organization practices

It shall be an unlawful employment practice for a labor organization-

> (1) to exclude or to expel from its membership, or otherwise to discriminate against, any individual because of his race, color, religion, sex, or national origin;
>
> (2) to limit, segregate, or classify its membership or applicants for membership, or to classify or fail or refuse to refer for employment any individual, in any way which would deprive or tend to deprive any individual of employment opportunities, or would limit such employment opportunities or otherwise adversely affect his status as an employee or as an applicant for employment, because of such individual's race, color, religion, sex, or national origin; or

(3) to cause or attempt to cause an employer to discriminate against an individual in violation of this section.

(d) Training programs

It shall be an unlawful employment practice for any employer, labor organization, or joint labor-management committee controlling apprenticeship or other training or retraining, including on-the-job training programs to discriminate against any individual because of his race, color, religion, sex, or national origin in admission to, or employment in, any program established to provide apprenticeship or other training.

(e) Businesses or enterprises with personnel qualified on basis of religion, sex, or national origin; educational institutions with personnel of particular religion

Notwithstanding any other provision of this subchapter, (1) it shall not be an unlawful employment practice for an employer to hire and employ employees, for an employment agency to classify, or refer for employment any individual, for a labor organization to classify its membership or to classify or refer for employment any individual, or for an employer, labor organization, or joint labor management committee controlling apprenticeship or other training or retraining programs to admit or employ any individual in any such program, on the basis of his religion, sex, or national origin in those certain instances where religion, sex, or national origin is a bona fide occupational qualification reasonably necessary to the normal operation of that particular business or enterprise, and (2) it shall not be an unlawful employment practice for a school, college, university, or other educational institution or institution of learning to hire and employ employees of a particular religion if such school, college, university, or other educational institution or institution of learning is, in whole or in substantial part, owned, supported, controlled, or managed by a particular religion or by a particular religious corporation, association, or society, or if the curriculum of such school, college, university, or other educational institution or institution of learning is directed toward the propagation of a particular religion.

(f) Members of Communist Party or Communist-action or Communist-front organizations

As used in this subchapter, the phrase “unlawful employment practice” shall not be deemed to include any action or measure taken by an employer, labor organization, joint labor management committee, or employment agency with respect to an individual who is a member of the Communist Party of the United States or of any other organization required to register as a Communist-action or Communist-front organization by final order of the Subversive Activities Control Board pursuant to the Subversive Activities Control Act of 1950 *[50 U.S.C. 781 et seq.]*.

(g) National security

Notwithstanding any other provision of this subchapter, it shall not be an unlawful employment practice for an employer to fail or refuse to hire and employ any individual for any position, for an employer to discharge any individual from any position, or for an employment agency to fail or refuse to refer any individual for employment in any position, or for a labor organization to fail or refuse to refer any individual for employment in any position, if-

(1) the occupancy of such position, or access to the premises in or upon which any part of the duties of such position is performed or is to be performed, is subject to any requirement imposed in the interest of the national security of the United States under any security program in effect pursuant to or administered under any statute of the United States or any Executive order of the President; and

(2) such individual has not fulfilled or has ceased to fulfill that requirement.

(h) Seniority or merit system; quantity or quality of production; ability tests; compensation based on sex and authorized by minimum wage provisions

Notwithstanding any other provision of this subchapter, it shall not be an unlawful employment practice for an employer to apply different standards of compensation, or different terms, conditions, or privileges of employment pursuant to a bona fide seniority or merit system, or a system which measures earnings by quantity or quality of production or to employees who work in different locations, provided that such differences are not the result of an intention to discriminate because of race, color, religion, sex, or national origin, nor shall it be an unlawful employment practice for an employer to give and to act upon the results of any professionally developed ability test provided that such test, its administration or action upon the results is not designed, intended or used to discriminate because of race, color, religion, sex or national origin. It shall not be an unlawful employment practice under this subchapter for any employer to differentiate upon the basis of sex in determining the amount of the wages or compensation paid or to be paid to employees of such employer if such differentiation is authorized by the provisions of section 206(d) of Title 29 *[section 6(d) of the Labor Standards Act of 1938, as amended]*.

(i) Businesses or enterprises extending preferential treatment to Indians

Nothing contained in this subchapter shall apply to any business or enterprise on or near an Indian reservation with respect to any publicly announced employment practice of such business or enterprise under which a preferential treatment is given to any individual because he is an Indian living on or near a reservation.

(j) Preferential treatment not to be granted on account of existing number or percentage imbalance

Nothing contained in this subchapter shall be interpreted to require any employer, employment agency, labor organization, or joint labor-management committee subject to this subchapter to grant preferential treatment to any individual or to any group because of the race, color, religion, sex, or national origin of such individual or group on account of an imbalance which may exist with respect to the total number or percentage of persons of any race, color, religion, sex, or national origin employed by any employer, referred or classified for employment by any employment agency or labor organization, admitted to membership or classified by any labor organization, or admitted to, or employed in, any apprenticeship or other training program, in comparison with the total number or percentage of persons of such race, color, religion, sex, or national origin in any community, State, section, or other area, or in the available work force in any community, State, section, or other area.

(k) Burden of proof in disparate impact cases

(1) (A) An unlawful employment practice based on disparate impact is established under this subchapter only if-

> (i) a complaining party demonstrates that a respondent uses a particular employment practice that causes a disparate impact on the basis of race, color, religion, sex, or national origin and the respondent fails to demonstrate that the challenged practice is job related for the position in question and consistent with business necessity; or
>
> (ii) the complaining party makes the demonstration described in subparagraph (C) with respect to an alternative employment practice and the respondent refuses to adopt such alternative employment practice.
>
> (B) (i) With respect to demonstrating that a particular employment practice causes a disparate impact as described in subparagraph (A)(i), the complaining party shall demonstrate that each particular challenged employment practice causes a disparate impact, except that if the complaining party can demonstrate to the court that the elements of a respondent's decisionmaking process are not capable of separation for analysis, the decisionmaking process may be analyzed as one employment practice.
>
> (ii) If the respondent demonstrates that a specific employment practice does not cause the disparate impact, the respondent shall not be required to demonstrate that such practice is required by business necessity.
>
> (C) The demonstration referred to by subparagraph (A)(ii) shall be in accordance with the law as it existed on June 4, 1989, with respect to the concept of "alternative employment practice".
>
> (2) A demonstration that an employment practice is required by business necessity may not be used as a defense against a claim of intentional discrimination under this subchapter.
>
> (3) Notwithstanding any other provision of this subchapter, a rule barring the employment of an individual who currently and knowingly uses or possesses a controlled substance, as defined in schedules I and II of section 102(6) of the Controlled Substances Act (21 U.S.C. 802(6)), other than the use or possession of a drug taken under the supervision of a licensed health care professional, or any other use or possession authorized by the Controlled Substances Act *[21 U.S.C. 801 et seq.]* or any other provision of Federal law, shall be considered an unlawful employment practice under this subchapter only if such rule is adopted or applied with an intent to discriminate because of race, color, religion, sex, or national origin.

(l) Prohibition of discriminatory use of test scores

It shall be an unlawful employment practice for a respondent, in connection with the selection or referral of applicants or candidates for employment or promotion, to adjust the scores of, use different cutoff scores for, or otherwise alter the results of, employment related tests on the basis of race, color, religion, sex, or national origin.

(m) Impermissible consideration of race, color, religion, sex, or national origin in employment practices

Except as otherwise provided in this subchapter, an unlawful employment practice is established when the complaining party demonstrates that race, color, religion, sex, or national origin was a motivating factor for any employment practice, even though other factors also motivated the practice.

(n) Resolution of challenges to employment practices implementing litigated or consent judgments or orders

(1) (A) Notwithstanding any other provision of law, and except as provided in paragraph (2), an employment practice that implements and is within the scope of a litigated or consent judgment or order that resolves a claim of employment discrimination under the Constitution or Federal civil rights laws may not be challenged under the circumstances described in subparagraph (B).

> (B) A practice described in subparagraph (A) may not be challenged in a claim under the Constitution or Federal civil rights laws-
>
> (i) by a person who, prior to the entry of the judgment or order described in subparagraph

(A), had-

(I) actual notice of the proposed judgment or order sufficient to apprise such person that such judgment or order might adversely affect the interests and legal rights of such person and that an opportunity was available to present objections to such judgment or order by a future date certain; and

(II) a reasonable opportunity to present objections to such judgment or order; or

(ii) by a person whose interests were adequately represented by another person who had previously challenged the judgment or order on the same legal grounds and with a similar factual situation, unless there has been an intervening change in law or fact.

(2) Nothing in this subsection shall be construed to-

(A) alter the standards for intervention under rule 24 of the Federal Rules of Civil Procedure or apply to the rights of parties who have successfully intervened pursuant to such rule in the proceeding in which the parties intervened;

(B) apply to the rights of parties to the action in which a litigated or consent judgment or order was entered, or of members of a class represented or sought to be represented in such action, or of members of a group on whose behalf relief was sought in such action by the Federal Government;

(C) prevent challenges to a litigated or consent judgment or order on the ground that such judgment or order was obtained through collusion or fraud, or is transparently invalid or was entered by a court lacking subject matter jurisdiction; or

(D) authorize or permit the denial to any person of the due process of law required by the Constitution.

(3) Any action not precluded under this subsection that challenges an employment consent judgment or order described in paragraph (1) shall be brought in the court, and if possible before the judge, that entered such judgment or order. Nothing in this subsection shall preclude a transfer of such action pursuant to section 1404 of Title 28 [*United States Code]*.

OTHER UNLAWFUL EMPLOYMENT PRACTICES

SEC. 2000e-3. *[Section 704]*

(a) Discrimination for making charges, testifying, assisting, or participating in enforcement proceedings

It shall be an unlawful employment practice for an employer to discriminate against any of his employees or applicants for employment, for an employment agency, or joint labor-management committee controlling apprenticeship or other training or retraining, including on—the-job training programs, to discriminate against any individual, or for a labor organization to discriminate against any member thereof or applicant for membership, because he has opposed any practice made an unlawful employment practice by this subchapter, or because he has made a charge, testified, assisted, or participated in any manner in an investigation, proceeding, or hearing under this subchapter.

(b) Printing or publication of notices or advertisements indicating prohibited preference, limitation, specification, or discrimination; occupational qualification exception

It shall be an unlawful employment practice for an employer, labor organization, employment agency, or joint labor-management committee controlling apprenticeship or other training or retraining, including on-the-job training programs, to print or publish or cause to be printed or published any notice or advertisement relating to employment by such an employer or membership in or any classification or referral for employment by such a labor organization, or relating to any classification or referral for employment by such an employment agency, or relating to admission to, or employment in, any program established to provide apprenticeship or other training by such a joint labor-management committee, indicating any preference, limitation, specification, or discrimination, based on race, color, religion, sex, or national origin, except that such a notice or advertisement may indicate a preference, limitation, specification, or discrimination based on religion, sex, or national origin when religion, sex, or national origin is a bona fide occupational qualification for employment.

EQUAL EMPLOYMENT OPPORTUNITY COMMISSION

SEC. 2000e-4. *[Section 705]*

(a) Creation; composition; political representation; appointment; term; vacancies; Chairman and Vice Chairman; duties of Chairman; appointment of personnel; compensation of personnel

There is hereby created a Commission to be known as the Equal Employment Opportunity Commission, which shall be

composed of five members, not more than three of whom shall be members of the same political party. Members of the Commission shall be appointed by the President by and with the advice and consent of the Senate for a term of five years. Any individual chosen to fill a vacancy shall be appointed only for the unexpired term of the member whom he shall succeed, and all members of the Commission shall continue to serve until their successors are appointed and qualified, except that no such member of the Commission shall continue to serve (1) for more than sixty days when the Congress is in session unless a nomination to fill such vacancy shall have been submitted to the Senate, or (2) after the adjournment sine die of the session of the Senate in which such nomination was submitted. The President shall designate one member to serve as Chairman of the Commission, and one member to serve as Vice Chairman. The Chairman shall be responsible on behalf of the Commission for the administrative operations of the Commission, and, except as provided in subsection (b) of this section, shall appoint, in accordance with the provisions of Title 5 *[United States Code]* governing appointments in the competitive service, such officers, agents, attorneys, administrative law judges *[originally, hearing examiners]*, and employees as he deems necessary to assist it in the performance of its functions and to fix their compensation in accordance with the provisions of chapter 51 and subchapter III of chapter 53 of Title 5 *[United States Code]*, relating to classification and General Schedule pay rates: Provided, That assignment, removal, and compensation of administrative law judges *[originally, hearing examiners]* shall be in accordance with sections 3105, 3344, 5372, and 7521 of Title 5 *[United States Code]*.

(b) General Counsel; appointment; term; duties; representation by attorneys and Attorney General

> (1) There shall be a General Counsel of the Commission appointed by the President, by and with the advice and consent of the Senate, for a term of four years. The General Counsel shall have responsibility for the conduct of litigation as provided in sections 2000e-5 and 2000e-6 of this title *[sections 706 and 707]*. The General Counsel shall have such other duties as the Commission may prescribe or as may be provided by law and shall concur with the Chairman of the Commission on the appointment and supervision of regional attorneys. The General Counsel of the Commission on the effective date of this Act shall continue in such position and perform the functions specified in this subsection until a successor is appointed and qualified.
>
> (2) Attorneys appointed under this section may, at the direction of the Commission, appear for and represent the Commission in any case in court, provided that the Attorney General shall conduct all litigation to which the Commission is a party in the Supreme Court pursuant to this subchapter.

(c) Exercise of powers during vacancy; quorum

A vacancy in the Commission shall not impair the right of the remaining members to exercise all the powers of the Commission and three members thereof shall constitute a quorum.

(d) Seal; judicial notice

The Commission shall have an official seal which shall be judicially noticed.

(e) Reports to Congress and the President

The Commission shall at the close of each fiscal year report to the Congress and to the President concerning the action it has taken *[originally, the names, salaries, and duties of all individuals in its employ]* and the moneys it has disbursed. It shall make such further reports on the cause of and means of eliminating discrimination and such recommendations for further legislation as may appear desirable.

(f) Principal and other offices

The principal office of the Commission shall be in or near the District of Columbia, but it may meet or exercise any or all its powers at any other place. The Commission may establish such regional or State offices as it deems necessary to accomplish the purpose of this subchapter.

(g) Powers of Commission

The Commission shall have power-

> (1) to cooperate with and, with their consent, utilize regional, State, local, and other agencies, both public and private, and individuals;
>
> (2) to pay to witnesses whose depositions are taken or who are summoned before the Commission or any of its agents the same witness and mileage fees as are paid to witnesses in the courts of the United States;
>
> (3) to furnish to persons subject to this subchapter such technical assistance as they may request to further their compliance with this subchapter or an order issued thereunder;
>
> (4) upon the request of (i) any employer, whose employees or some of them, or (ii) any labor organization, whose members or some of them, refuse or threaten to refuse to cooperate in effectuating

the provisions of this subchapter, to assist in such effectuation by conciliation or such other remedial action as is provided by this subchapter;

(5) to make such technical studies as are appropriate to effectuate the purposes and policies of this subchapter and to make the results of such studies available to the public;

(6) to intervene in a civil action brought under section 2000e-5 of this title *[section 706]* by an aggrieved party against a respondent other than a government, governmental agency or political subdivision.

(h) Cooperation with other departments and agencies in performance of educational or promotional activities; outreach activities

(1) The Commission shall, in any of its educational or promotional activities, cooperate with other departments and agencies in the performance of such educational and promotional activities.

(2) In exercising its powers under this subchapter, the Commission shall carry out educational and outreach activities (including dissemination of information in languages other than English) targeted to-

(A) individuals who historically have been victims of employment discrimination and have not been equitably served by the Commission; and

(B) individuals on whose behalf the Commission has authority to enforce any other law prohibiting employment discrimination, concerning rights and obligations under this subchapter or such law, as the case may be.

(i) Personnel subject to political activity restrictions

All officers, agents, attorneys, and employees of the Commission shall be subject to the provisions of section 7324 of Title 5 *[originally, section 9 of the Act of August 2, 1939, as amended (the Hatch Act)]*, notwithstanding any exemption contained in such section.

(j) Technical Assistance Training Institute

(1) The Commission shall establish a Technical Assistance Training Institute, through which the Commission shall provide technical assistance and training regarding the laws and regulations enforced by the Commission.

(2) An employer or other entity covered under this subchapter shall not be excused from compliance with the requirements of this subchapter because of any failure to receive technical assistance under this subsection.

(3) There are authorized to be appropriated to carry out this subsection such sums as may be necessary for fiscal year 1992.

(k) EEOC Education, Technical Assistance, and Training Revolving Fund

(1) There is hereby established in the Treasury of the United States a revolving fund to be known as the “EEOC Education, Technical Assistance, and Training Revolving Fund” (hereinafter in this subsection referred to as the “Fund”) and to pay the cost (including administrative and personnel expenses) of providing education, technical assistance, and training relating to laws administered by the Commission. Monies in the Fund shall be available without fiscal year limitation to the Commission for such purposes.

(2)(A) The Commission shall charge fees in accordance with the provisions of this paragraph to offset the costs of education, technical assistance, and training provided with monies in the Fund. Such fees for any education, technical assistance, or training--

(i) shall be imposed on a uniform basis on persons and entities receiving such education, assistance, or training,

(ii) shall not exceed the cost of providing such education, assistance, and training, and

(iii) with respect to each person or entity receiving such education, assistance, or training, shall bear a reasonable relationship to the cost of providing such education, assistance, or training to such person or entity.

(B) Fees received under subparagraph (A) shall be deposited in the Fund by the Commission.

(C) The Commission shall include in each report made under subsection (e) of this section information with respect to the operation of the Fund, including information, presented in the aggregate, relating to--

(i) the number of persons and entities to which the Commission provided education, technical assistance,

or training with monies in the Fund, in the fiscal year for which such report is prepared,

(ii) the cost to the Commission to provide such education, technical assistance, or training to such persons and entities, and

(iii) the amount of any fees received by the Commission from such persons and entities for such education, technical assistance, or training.

(3) The Secretary of the Treasury shall invest the portion of the Fund not required to satisfy current expenditures from the Fund, as determined by the Commission, in obligations of the United States or obligations guaranteed as to principal by the United States. Investment proceeds shall be deposited in the Fund.

(4) There is hereby transferred to the Fund $1,000,000 from the Salaries and Expenses appropriation of the Commission.

ENFORCEMENT PROVISIONS

SEC. 2000e-5. *[Section 706]*

(a) Power of Commission to prevent unlawful employment practices

The Commission is empowered, as hereinafter provided, to prevent any person from engaging in any unlawful employment practice as set forth in section 2000e-2 or 2000e-3 of this title *[section 703 or 704]*.

(b) Charges by persons aggrieved or member of Commission of unlawful employment practices by employers, etc.; filing; allegations; notice to respondent; contents of notice; investigation by Commission; contents of charges; prohibition on disclosure of charges; determination of reasonable cause; conference, conciliation, and persuasion for elimination of unlawful practices; prohibition on disclosure of informal endeavors to end unlawful practices; use of evidence in subsequent proceedings; penalties for disclosure of information; time for determination of reasonable cause

Whenever a charge is filed by or on behalf of a person claiming to be aggrieved, or by a member of the Commission, alleging that an employer, employment agency, labor organization, or joint labormanagement committee controlling apprenticeship or other training or retraining, including on-the-job training programs, has engaged in an unlawful employment practice, the Commission shall serve a notice of the charge (including the date, place and circumstances of the alleged unlawful employment practice) on such employer, employment agency, labor organization, or joint labor-management committee (hereinafter referred to as the “respondent”) within ten days, and shall make an investigation thereof. Charges shall be in writing under oath or affirmation and shall contain such information and be in such form as the Commission requires. Charges shall not be made public by the Commission. If the Commission determines after such investigation that there is not reasonable cause to believe that the charge is true, it shall dismiss the charge and promptly notify the person claiming to be aggrieved and the respondent of its action. In determining whether reasonable cause exists, the Commission shall accord substantial weight to final findings and orders made by State or local authorities in proceedings commenced under State or local law pursuant to the requirements of subsections (c) and (d) of this section. If the Commission determines after such investigation that there is reasonable cause to believe that the charge is true, the Commission shall endeavor to eliminate any such alleged unlawful employment practice by informal methods of conference, conciliation, and persuasion. Nothing said or done during and as a part of such informal endeavors may be made public by the Commission, its officers or employees, or used as evidence in a subsequent proceeding without the written consent of the persons concerned. Any person who makes public information in violation of this subsection shall be fined not more than $1,000 or imprisoned for not more than one year, or both. The Commission shall make its determination on reasonable cause as promptly as possible and, so far as practicable, not later than one hundred and twenty days from the filing of the charge or, where applicable under subsection (c) or (d) of this section, from the date upon which the Commission is authorized to take action with respect to the charge.

(c) State or local enforcement proceedings; notification of State or local authority; time for filing charges with Commission; commencement of proceedings

In the case of an alleged unlawful employment practice occurring in a State, or political subdivision of a State, which has a State or local law prohibiting the unlawful employment practice alleged and establishing or authorizing a State or local authority to grant or seek relief from such practice or to institute criminal proceedings with respect thereto upon receiving notice thereof, no charge may be filed under subsection (a) of this section by the person aggrieved before the expiration of sixty days after proceedings have been commenced under the State or local law, unless such proceedings have been earlier terminated, provided that such sixty- day period shall be extended to one hundred and twenty days during the first year after the effective date of such State or local law. If any requirement for the commencement of such proceedings is imposed by a State or local authority other than a requirement of the filing of a written and signed statement of the facts upon which the proceeding is based, the proceeding shall be deemed to have been commenced for the purposes of this subsection at the time such statement is sent by registered mail to the appropriate State or local authority.

(d) State or local enforcement proceedings; notification of State or local authority; time for action on charges by Commission

In the case of any charge filed by a member of the Commission alleging an unlawful employment practice occurring in a State or political subdivision of a State which has a State or local law prohibiting the practice alleged and establishing or authorizing a State or local authority to grant or seek relief from such practice or to institute criminal proceedings with respect thereto upon receiving notice thereof, the Commission shall, before taking any action with respect to such charge, notify the appropriate State or local officials and, upon request, afford them a reasonable time, but not less than sixty days (provided that such sixty-day period shall be extended to one hundred and twenty days during the first year after the effective day of such State or local law), unless a shorter period is requested, to act under such State or local law to remedy the practice alleged.

(e) Time for filing charges; time for service of notice of charge on respondent; filing of charge by Commission with State or local agency; seniority system

(1) A charge under this section shall be filed within one hundred and eighty days after the alleged unlawful employment practice occurred and notice of the charge (including the date, place and circumstances of the alleged unlawful employment practice) shall be served upon the person against whom such charge is made within ten days thereafter, except that in a case of an unlawful employment practice with respect to which the person aggrieved has initially instituted proceedings with a State or local agency with authority to grant or seek relief from such practice or to institute criminal proceedings with respect thereto upon receiving notice thereof, such charge shall be filed by or on behalf of the person aggrieved within three hundred days after the alleged unlawful employment practice occurred, or within thirty days after receiving notice that the State or local agency has terminated the proceedings under the State or local law, whichever is earlier, and a copy of such charge shall be filed by the Commission with the State or local agency.

(2) For purposes of this section, an unlawful employment practice occurs, with respect to a seniority system that has been adopted for an intentionally discriminatory purpose in violation of this subchapter (whether or not that discriminatory purpose is apparent on the face of the seniority provision), when the seniority system is adopted, when an individual becomes subject to the seniority system, or when a person aggrieved is injured by the application of the seniority system or provision of the system.

(3)(A) For purposes of this section, an unlawful employment practice occurs, with respect to discrimination in compensation in violation of this title, when a discriminatory compensation decision or other practice is adopted, when an individual becomes subject to a discriminatory compensation decision or other practice, or when an individual is affected by application of a discriminatory compensation decision or other practice, including each time wages, benefits, or other compensation is paid, resulting in whole or in part from such a decision or other practice.

(B) In addition to any relief authorized by section 1977A of the Revised Statutes (42 U.S.C. 1981a), liability may accrue and an aggrieved person may obtain relief as provided in subsection (g)(1), including recovery of back pay for up to two years preceding the filing of the charge, where the unlawful employment practices that have occurred during the charge filing period are similar or related to unlawful employment practices with regard to discrimination in compensation that occurred outside the time for filing a charge.

(f) Civil action by Commission, Attorney General, or person aggrieved; preconditions; procedure; appointment of attorney; payment of fees, costs, or security; intervention; stay of Federal proceedings; action for appropriate temporary or preliminary relief pending final disposition of charge; jurisdiction and venue of United States courts; designation of judge to hear and determine case; assignment of case for hearing; expedition of case; appointment of master

(1) If within thirty days after a charge is filed with the Commission or within thirty days after expiration of any period of reference under subsection (c) or (d) of this section, the Commission has been unable to secure from the respondent a conciliation agreement acceptable to the Commission, the Commission may bring a civil action against any respondent not a government, governmental agency, or political subdivision named in the charge. In the case of a respondent which is a government, governmental agency, or political subdivision, if the Commission has been unable to secure from the respondent a conciliation agreement acceptable to the Commission, the Commission shall take no further action and shall refer the case to the Attorney General who may bring a civil action against such respondent in the appropriate United States district court. The person or persons aggrieved shall have the right to intervene in a civil action brought by the Commission or the Attorney General in a case involving a government, governmental agency, or political subdivision. If a charge filed with the Commission pursuant to subsection (b) of this section is dismissed by the Commission, or if within one hundred and eighty days from the filing of such charge or the expiration of any period of reference under subsection (c) or (d) of this section, whichever is later, the Commission has not filed a civil action under this section or the Attorney General has not filed a civil action in a case involving a government, governmental agency, or political subdivision, or the Commission has not entered into a conciliation agreement to which the person aggrieved is a party, the Commission, or the Attorney General in a case involving a government, governmental agency, or political subdivision, shall so notify the person aggrieved and within ninety days

after the giving of such notice a civil action may be brought against the respondent named in the charge (A) by the person claiming to be aggrieved or (B) if such charge was filed by a member of the Commission, by any person whom the charge alleges was aggrieved by the alleged unlawful employment practice. Upon application by the complainant and in such circumstances as the court may deem just, the court may appoint an attorney for such complainant and may authorize the commencement of the action without the payment of fees, costs, or security. Upon timely application, the court may, in its discretion, permit the Commission, or the Attorney General in a case involving a government, governmental agency, or political subdivision, to intervene in such civil action upon certification that the case is of general public importance. Upon request, the court may, in its discretion, stay further proceedings for not more than sixty days pending the termination of State or local proceedings described in subsection (c) or (d) of this section or further efforts of the Commission to obtain voluntary compliance.

(2) Whenever a charge is filed with the Commission and the Commission concludes on the basis of a preliminary investigation that prompt judicial action is necessary to carry out the purposes of this Act, the Commission, or the Attorney General in a case involving a government, governmental agency, or political subdivision, may bring an action for appropriate temporary or preliminary relief pending final disposition of such charge. Any temporary restraining order or other order granting preliminary or temporary relief shall be issued in accordance with rule 65 of the Federal Rules of Civil Procedure. It shall be the duty of a court having jurisdiction over proceedings under this section to assign cases for hearing at the earliest practicable date and to cause such cases to be in every way expedited.

(3) Each United States district court and each United States court of a place subject to the jurisdiction of the United States shall have jurisdiction of actions brought under this subchapter. Such an action may be brought in any judicial district in the State in which the unlawful employment practice is alleged to have been committed, in the judicial district in which the employment records relevant to such practice are maintained and administered, or in the judicial district in which the aggrieved person would have worked but for the alleged unlawful employment practice, but if the respondent is not found within any such district, such an action may be brought within the judicial district in which the respondent has his principal office. For purposes of sections 1404 and 1406 of Title 28 *[United States Code]*, the judicial district in which the respondent has his principal office shall in all cases be considered a district in which the action might have been brought.

(4) It shall be the duty of the chief judge of the district (or in his absence, the acting chief judge) in which the case is pending immediately to designate a judge in such district to hear and determine the case. In the event that no judge in the district is available to hear and determine the case, the chief judge of the district, or the acting chief judge, as the case may be, shall certify this fact to the chief judge of the circuit (or in his absence, the acting chief judge) who shall then designate a district or circuit judge of the circuit to hear and determine the case.

(5) It shall be the duty of the judge designated pursuant to this subsection to assign the case for hearing at the earliest practicable date and to cause the case to be in every way expedited. If such judge has not scheduled the case for trial within one hundred and twenty days after issue has been joined, that judge may appoint a master pursuant to rule 53 of the Federal Rules of Civil Procedure.

(g) Injunctions; appropriate affirmative action; equitable relief; accrual of back pay; reduction of back pay; limitations on judicial orders

(1) If the court finds that the respondent has intentionally engaged in or is intentionally engaging in an unlawful employment practice charged in the complaint, the court may enjoin the respondent from engaging in such unlawful employment practice, and order such affirmative action as may be appropriate, which may include, but is not limited to, reinstatement or hiring of employees, with or without back pay (payable by the employer, employment agency, or labor organization, as the case may be, responsible for the unlawful employment practice), or any other equitable relief as the court deems appropriate. Back pay liability shall not accrue from a date more than two years prior to the filing of a charge with the Commission. Interim earnings or amounts earnable with reasonable diligence by the person or persons discriminated against shall operate to reduce the back pay otherwise allowable.

(2) (A) No order of the court shall require the admission or reinstatement of an individual as a member of a union, or the hiring, reinstatement, or promotion of an individual as an employee, or the payment to him of any back pay, if such individual was refused admission, suspended, or expelled, or was refused employment or advancement or was suspended or discharged for any reason other than discrimination on account of race, color, religion, sex, or national origin or in violation of section 2000e-3(a) of this Title *[section 704(a)]*.

(B) On a claim in which an individual proves a violation under section 2000e-2(m) of this title *[section 703(m)]* and a respondent demonstrates that the respondent would have taken the same action in the absence of the impermissible motivating factor, the court-

(i) may grant declaratory relief, injunctive relief (except as provided in clause (ii)), and attorney's fees and costs demonstrated to be directly attributable only to the pursuit of a claim under section 2000e-2(m) of this title *[section 703(m)]*; and

(ii) shall not award damages or issue an order requiring any admission, reinstatement, hiring, promotion, or payment, described in subparagraph (A).

(h) Provisions of chapter 6 of Title 29 not applicable to civil actions for prevention of unlawful practices

The provisions of chapter 6 of title 29 *[the Act entitled"An Act to amend the Judicial Code and to define and limit the jurisdiction of courts sitting in equity, and for other purposes," approved March 23, 1932 (29 U.S.C. 105-115)]* shall not apply with respect to civil actions brought under this section.

(i) Proceedings by Commission to compel compliance with judicial orders In any case in which an employer, employment agency, or labor organization fails to comply with an order of a court issued in a civil action brought under this section, the Commission may commence proceedings to compel compliance with such order.

(j) Appeals

Any civil action brought under this section and any proceedings brought under subsection (i) of this section shall be subject to appeal as provided in sections 1291 and 1292, Title 28 *[United States Code]*.

(k) Attorney's fee; liability of Commission and United States for costs

In any action or proceeding under this subchapter the court, in its discretion, may allow the prevailing party, other than the Commission or the United States, a reasonable attorney's fee (including expert fees) as part of the costs, and the Commission and the United States shall be liable for costs the same as a private person.

CIVIL ACTIONS BY THE ATTORNEY GENERAL

SEC. 2000e-6. *[Section 707]*

(a) Complaint

Whenever the Attorney General has reasonable cause to believe that any person or group of persons is engaged in a pattern or practice of resistance to the full enjoyment of any of the rights secured by this subchapter, and that the pattern or practice is of such a nature and is intended to deny the full exercise of the rights herein described, the Attorney General may bring a civil action in the appropriate district court of the United States by filing with it a complaint (1) signed by him (or in his absence the Acting Attorney General), (2) setting forth facts pertaining to such pattern or practice, and (3) requesting such relief, including an application for a permanent or temporary injunction, restraining order or other order against the person or persons responsible for such pattern or practice, as he deems necessary to insure the full enjoyment of the rights herein described.

(b) Jurisdiction; three-judge district court for cases of general public importance: hearing, determination, expedition of action, review by Supreme Court; single judge district court: hearing, determination, expedition of action

The district courts of the United States shall have and shall exercise jurisdiction of proceedings instituted pursuant to this section, and in any such proceeding the Attorney General may file with the clerk of such court a request that a court of three judges be convened to hear and determine the case. Such request by the Attorney General shall be accompanied by a certificate that, in his opinion, the case is of general public importance. A copy of the certificate and request for a three-judge court shall be immediately furnished by such clerk to the chief judge of the circuit (or in his absence, the presiding circuit judge of the circuit) in which the case is pending. Upon receipt of such request it shall be the duty of the chief judge of the circuit or the presiding circuit judge, as the case may be, to designate immediately three judges in such circuit, of whom at least one shall be a circuit judge and another of whom shall be a district judge of the court in which the proceeding was instituted, to hear and determine such case, and it shall be the duty of the judges so designated to assign the case for hearing at the earliest practicable date, to participate in the hearing and determination thereof, and to cause the case to be in every way expedited. An appeal from the final judgment of such court will lie to the Supreme Court.

In the event the Attorney General fails to file such a request in any such proceeding, it shall be the duty of the chief judge of the district (or in his absence, the acting chief judge) in which the case is pending immediately to designate a judge in such district to hear and determine the case. In the event that no judge in the district is available to hear and determine the case, the chief judge of the district, or the acting chief judge, as the case may be, shall certify this fact to the chief judge of the circuit (or in his absence, the acting chief judge) who shall then designate a district or circuit judge of the circuit to hear and determine the case.

It shall be the duty of the judge designated pursuant to this section to assign the case for hearing at the earliest practicable date and to cause the case to be in every way expedited.

(c) Transfer offunctions, etc., to Commission; effective date; prerequisite to transfer; execution of functions by

Commission

Effective two years after March 24, 1972 *[the date of enactment of the Equal Employment Opportunity Act of 1972]*, the functions of theAttorney General under this section shall be transferred to the Commission, together with such personnel, property, records, and unexpended balances of appropriations, allocations, and other funds employed, used, held, available, or to be made available in connection with such functions unless the President submits, and neither House of Congress vetoes, a reorganization plan pursuant to chapter 9 of Title 5 *[United States Code]*, inconsistent with the provisions of this subsection. The Commission shall carry out such functions in accordance with subsections (d) and (e) of this section.

(d) Transfer of functions, etc., not to affect suits commenced pursuant to this section prior to date of transfer

Upon the transfer of functions provided for in subsection (c) of this section, in all suits commenced pursuant to this section prior to the date of such transfer, proceedings shall continue without abatement, all court orders and decrees shall remain in effect, and the Commission shall be substituted as a party for the United States of America, the Attorney General, or the Acting Attorney General, as appropriate.

(e) Investigation and action by Commission pursuant to filing of charge of discrimination; procedure

Subsequent to March 24, 1972 *[the date of enactment of the Equal Employment Opportunity Act of 1972]*, the Commission shall haveauthority to investigate and act on a charge of a pattern or practice ofdiscrimination, whether filed by or on behalf of a person claiming to beaggrieved or by a member of the Commission. All such actions shall beconducted in accordance with the procedures set forth in section 2000e-5of this title *[section 706]*.

EFFECT ON STATE LAWS

SEC. 2000e-7. *[Section 708]*

Nothing in this subchapter shall be deemed to exempt or relieve any person from any liability, duty, penalty, or punishment provided by any present or future law of any State or political subdivision of a State, other than any such law which purports to require or permit the doing of any act which would be an unlawful employment practice under this subchapter.

INVESTIGATIONS

SEC. 2000e-8. *[Section 709]*

(a) Examination and copying of evidence related to unlawful employment practices

In connection with any investigation of a charge filed under section 2000e-5 of this title *[section 706]*, the Commission or its designated representative shall at all reasonable times have access to, for the purposes of examination, and the right to copy any evidence of any person being investigated or proceeded against that relates to unlawful employment practices covered by this subchapter and is relevant to the charge under investigation.

(b) Cooperation with State and local agencies administering State fair employment practices laws; participation in and contribution to research and other projects; utilization of services; payment in advance or reimbursement; agreements and rescission of agreements

The Commission may cooperate with State and local agencies charged with the administration of State fair employment practices laws and, with the consent of such agencies, may, for the purpose of carrying out its functions and duties under this subchapter and within the limitation of funds appropriated specifically for such purpose, engage in and contribute to the cost of research and other projects of mutual interest undertaken by such agencies, and utilize the services of such agencies and their employees, and, notwithstanding any other provision of law, pay by advance or reimbursement such agencies and their employees for services rendered to assist the Commission in carrying out this subchapter. In furtherance of such cooperative efforts, the Commission may enter into written agreements with such State or local agencies and such agreements may include provisions under which the Commission shall refrain from processing a charge in any cases or class of cases specified in such agreements or under which the Commission shall relieve any person or class of persons in such State or locality from requirements imposed under this section. The Commission shall rescind any such agreement whenever it determines that the agreement no longer serves the interest of effective enforcement of this subchapter.

(c) Execution, retention, and preservation of records; reports to Commission; training program records; appropriate relief from regulation or order for undue hardship; procedure for exemption; judicial action to compel compliance

Every employer, employment agency, and labor organization subject to this subchapter shall (1) make and keep such records relevant to the determinations of whether unlawful employment practices have been or are being committed, (2) preserve such records for such periods, and (3) make such reports therefrom as the Commission shall prescribe by regulation or order, after public hearing, as reasonable, necessary, or appropriate for the enforcement of this subchapter or the regulations or orders thereunder. The Commission shall, by regulation, require each employer, labor organization, and joint labor-management committee subject to this subchapter which controls an apprenticeship or other training

program to maintain such records as are reasonably necessary to carry out the purposes of this subchapter, including, but not limited to, a list of applicants who wish to participate in such program, including the chronological order in which applications were received, and to furnish to the Commission upon request, a detailed description of the manner in which persons are selected to participate in the apprenticeship or other training program. Any employer, employment agency, labor organization, or joint labor-management committee which believes that the application to it of any regulation or order issued under this section would result in undue hardship may apply to the Commission for an exemption from the application of such regulation or order, and, if such application for an exemption is denied, bring a civil action in the United States district court for the district where such records are kept. If the Commission or the court, as the case may be, finds that the application of the regulation or order to the employer, employment agency, or labor organization in question would impose an undue hardship, the Commission or the court, as the case may be, may grant appropriate relief. If any person required to comply with the provisions of this subsection fails or refuses to do so, the United States district court for the district in which such person is found, resides, or transacts business, shall, upon application of the Commission, or the Attorney General in a case involving a government, governmental agency or political subdivision, have jurisdiction to issue to such person an order requiring him to comply.

(d) Consultation and coordination between Commission and interested State and Federal agencies in prescribing recordkeeping and reporting requirements; availability of information furnished pursuant to recordkeeping and reporting requirements; conditions on availability

In prescribing requirements pursuant to subsection (c) of this section, the Commission shall consult with other interested State and Federal agencies and shall endeavor to coordinate its requirements with those adopted by such agencies. The Commission shall furnish upon request and without cost to any State or local agency charged with the administration of a fair employment practice law information obtained pursuant to subsection (c) of this section from any employer, employment agency, labor organization, or joint labor-management committee subject to the jurisdiction of such agency. Such information shall be furnished on condition that it not be made public by the recipient agency prior to the institution of a proceeding under State or local law involving such information. If this condition is violated by a recipient agency, the Commission may decline to honor subsequent requests pursuant to this subsection.

(e) Prohibited disclosures; penalties

It shall be unlawful for any officer or employee of the Commission to make public in any manner whatever any information obtained by the Commission pursuant to its authority under this section prior to the institution of any proceeding under this subchapter involving such information. Any officer or employee of the Commission who shall make public in any manner whatever any information in violation of this subsection shall be guilty of a misdemeanor and upon conviction thereof, shall be fined not more than $1,000, or imprisoned not more than one year.

CONDUCT OF HEARINGS AND INVESTIGATIONS PURSUANT TO SECTION 161 OF Title 29

SEC. 2000e-9. *[Section 710]*

For the purpose of all hearings and investigations conducted by the Commission or its duly authorized agents or agencies, section 161 of Title 29 *[section 11 of the National Labor Relations Act]* shall apply.

POSTING OF NOTICES; PENALTIES

SEC. 2000e-10. *[Section 711]*

(a) Every employer, employment agency, and labor organization, as the case may be, shall post and keep posted in conspicuous places upon its premises where notices to employees, applicants for employment, and members are customarily posted a notice to be prepared or approved by the Commission setting forth excerpts from or, summaries of, the pertinent provisions of this subchapter and information pertinent to the filing of a complaint.

(b) A willful violation of this section shall be punishable by a fine of not more than $100 for each separate offense.

VETERANS' SPECIAL RIGHTS OR PREFERENCE

SEC. 2000e-11. *[Section 712]*

Nothing contained in this subchapter shall be construed to repeal or modify any Federal, State, territorial, or local law creating special rights or preference for veterans.

REGULATIONS; CONFORMITY OF REGULATIONS WITH ADMINISTRATIVE PROCEDURE PROVISIONS; RELIANCE ON INTERPRETATIONS AND INSTRUCTIONS OF COMMISSION

SEC. 2000e-12. *[Section 713]*

(a) The Commission shall have authority from time to time to issue, amend, or rescind suitable procedural regulations to carry out the provisions of this subchapter. Regulations issued under this section shall be in conformity with the standards and limitations of subchapter II of chapter 5 of Title 5 *[originally, the Administrative Procedure Act]*.

(b) In any action or proceeding based on any alleged unlawful employment practice, no person shall be subject to any liability or punishment for or on account of (1) the commission by such person of an unlawful employment practice if he pleads and proves that the act or omission complained of was in good faith, in conformity with, and in reliance on any written interpretation or opinion of the Commission, or (2) the failure of such person to publish and file any information required by any provision of this subchapter if he pleads and proves that he failed to publish and file such information in good faith, in conformity with the instructions of the Commission issued under this subchapter regarding the filing of such information. Such a defense, if established, shall be a bar to the action or proceeding, notwithstanding that (A) after such act or omission, such interpretation or opinion is modified or rescinded or is determined by judicial authority to be invalid or of no legal effect, or (B) after publishing or filing the description and annual reports, such publication or filing is determined by judicial authority not to be in conformity with the requirements of this subchapter.

APPLICATION TO PERSONNEL OF COMMISSION OF SECTIONS 111 AND 1114 OF TITLE 18; PUNISHMENT FOR VIOLATION OF SECTION 1114 OF TITLE 18

SEC. 2000e-13. *[Section 714]*

The provisions of sections 111 and 1114, Title 18 *[United States Code]*, shall apply to officers, agents, and employees of the Commission in the performance of their official duties. Notwithstanding the provisions of sections 111 and 1114 of Title 18 *[United States Code]*, whoever in violation of the provisions of section 1114 of such title kills a person while engaged in or on account of the performance of his official functions under this Act shall be punished by imprisonment for any term of years or for life.

TRANSFER OF AUTHORITY

[Administration of the duties of the Equal Employment Opportunity Coordinating Council was transferred to the Equal Employment Opportunity Commission effective July 1, 1978, under the President's Reorganization Plan of 1978.]

EQUAL EMPLOYMENT OPPORTUNITY COORDINATING COUNCIL; ESTABLISHMENT; COMPOSITION; DUTIES; REPORT TO PRESIDENT AND CONGRESS

SEC. 2000e-14. *[Section 715]*

[Original introductory text: There shall be established an Equal Employment Opportunity Coordinating Council (hereinafter referred to in this section as the Council) composed of the Secretary of Labor, the Chairman of the Equal Employment Opportunity Commission, the Attorney General, the Chairman of the United States Civil Service Commission, and the Chairman of the United States Civil Rights Commission, or their respective delegates.]

The Equal Employment Opportunity Commission *[originally, Council]* shall have the responsibility for developing and implementing agreements, policies and practices designed to maximize effort, promote efficiency, and eliminate conflict, competition, duplication and inconsistency among the operations, functions and jurisdictions of the various departments, agencies and branches of the Federal Government responsible for the implementation and enforcement of equal employment opportunity legislation, orders, and policies. On or before October 1 *[originally, July 1]* of each year, the Equal Employment Opportunity Commission *[originally, Council]* shall transmit to the President and to the Congress a report of its activities, together with such recommendations for legislative or administrative changes as it concludes are desirable to further promote the purposes of this section.

PRESIDENTIAL CONFERENCES; ACQUAINTANCE OF LEADERSHIP WITH PROVISIONS FOR EMPLOYMENT RIGHTS AND OBLIGATIONS; PLANS FOR FAIR ADMINISTRATION; MEMBERSHIP

SEC. 2000e-15. *[Section 716]*

[Original text: (a) This title shall become effective one year after the date of its enactment.

(b) Notwithstanding subsection (a), sections of this title other than sections 703, 704, 706, and 707 shall become effective immediately.

(c)] The President shall, as soon as feasible after July 2, 1964 *[the date of enactment of this title]*, convene one or more conferences for the purpose of enabling the leaders of groups whose members will be affected by this subchapter to become familiar with the rights afforded and obligations imposed by its provisions, and for the purpose of making plans which will result in the fair and effective administration of this subchapter when all of its provisions become effective. The President shall invite the participation in such conference or conferences of (1) the members of the President's

Committee on Equal Employment Opportunity, (2) the members of the Commission on Civil Rights, (3) representatives of State and local agencies engaged in furthering equal employment opportunity, (4) representatives of private agencies engaged in furthering equal employment opportunity, and (5) representatives of employers, labor organizations, and employment agencies who will be subject to this subchapter.

TRANSFER OF AUTHORITY

[Enforcement of Section 717 was transferred to the Equal Employment Opportunity Commission from the Civil Service Commission (Office of Personnel Management) effective January 1, 1979 under the President's Reorganization Plan No. 1 of 1978.]

EMPLOYMENT BY FEDERAL GOVERNMENT

SEC. 2000e-16. *[Section 717]*

(a) Discriminatory practices prohibited; employees or applicants for employment subject to coverage

All personnel actions affecting employees or applicants for employment (except with regard to aliens employed outside the limits of the United States) in military departments as defined in section 102 of Title 5 *[United States Code]*, in executive agencies *[originally, other than the General Accounting Office]* as defined in section 105 of Title 5 *[United States Code]* (including employees and applicants for employment who are paid from nonappropriated funds), in the United States Postal Service and the Postal Regulatory Commission, in those units of the Government of the District of Columbia having positions in the competitive service, and in those units of the judicial branch of the Federal Government having positions in the competitive service, in the Smithsonian Institution, and in the Government Printing Office, the Government Accountability Office, and the Library of Congress shall be made free from any discrimination based on race, color, religion, sex, or national origin.

(b) Equal Employment Opportunity Commission; enforcement powers; issuance of rules, regulations, etc.; annual review and approval of national and regional equal employment opportunity plans; review and evaluation of equal employment opportunity programs and publication of progress reports; consultations with interested parties; compliance with rules, regulations, etc.; contents of national and regional equal employment opportunity plans; authority of Librarian of Congress

Except as otherwise provided in this subsection, the Equal Employment Opportunity Commission *[originally, Civil Service Commission]* shall have authority to enforce the provisions of subsection (a) of this section through appropriate remedies, including reinstatement or hiring of employees with or without back pay, as will effectuate the policies of this section, and shall issue such rules, regulations, orders and instructions as it deems necessary and appropriate to carry out its responsibilities under this section. The Equal Employment Opportunity Commission *[originally, Civil Service Commission]* shall-

> (1) be responsible for the annual review and approval of a national and regional equal employment opportunity plan which each department and agency and each appropriate unit referred to in subsection (a) of this section shall submit in order to maintain an affirmative program of equal employment opportunity for all such employees and applicants for employment;
>
> (2) be responsible for the review and evaluation of the operation of all agency equal employment opportunity programs, periodically obtaining and publishing (on at least a semiannual basis) progress reports from each such department, agency, or unit; and
>
> (3) consult with and solicit the recommendations of interested individuals, groups, and organizations relating to equal employment opportunity.

The head of each such department, agency, or unit shall comply with such rules, regulations, orders, and instructions which shall include a provision that an employee or applicant for employment shall be notified of any final action taken on any complaint of discrimination filed by him thereunder. The plan submitted by each department, agency, and unit shall include, but not be limited to-

> (1) provision for the establishment of training and education programs designed to provide a maximum opportunity for employees to advance so as to perform at their highest potential; and
>
> (2) a description of the qualifications in terms of training and experience relating to equal employment opportunity for the principal and operating officials of each such department, agency, or unit responsible for carrying out the equal employment opportunity program and of the allocation of personnel and resources proposed by such department, agency, or unit to carry out its equal employment opportunity program.

With respect to employment in the Library of Congress, authorities granted in this subsection to the Equal Employment Opportunity Commission *[originally, Civil Service Commission]* shall be exercised by the Librarian of Congress.

(c) Civil action by employee or applicant for employment for redress of grievances; time for bringing of action; head of department, agency, or unit as defendant

Within 90 days of receipt of notice of final action taken by a department, agency, or unit referred to in subsection (a) of this section, or by the Equal Employment Opportunity Commission *[originally, Civil Service Commission]* upon an appeal from a decision or order of such department, agency, or unit on a complaint of discrimination based on race, color, religion, sex or national origin, brought pursuant to subsection (a) of this section, Executive Order 11478 or any succeeding Executive orders, or after one hundred and eighty days from the filing of the initial charge with the department, agency, or unit or with the Equal Employment Opportunity Commission *[originally, Civil Service Commission]* on appeal from a decision or order of such department, agency, or unit until such time as final action may be taken by a department, agency, or unit, an employee or applicant for employment, if aggrieved by the final disposition of his complaint, or by the failure to take final action on his complaint, may file a civil action as provided in section 2000e-5 of this title *[section 706]*, in which civil action the head of the department, agency, or unit, as appropriate, shall be the defendant.

(d) Section 2000e-5(f) through (k) of this title applicable to civil actions

The provisions of section 2000e-5(f) through (k) of this title *[section 706(f) through (k)]*, as applicable, shall govern civil actions brought hereunder, and the same interest to compensate for delay in payment shall be available as in cases involving nonpublic parties.

(e) Government agency or official not relieved of responsibility to assure nondiscrimination in employment or equal employment opportunity

Nothing contained in this Act shall relieve any Government agency or official of its or his primary responsibility to assure nondiscrimination in employment as required by the Constitution and statutes or of its or his responsibilities under Executive Order 11478 relating to equal employment opportunity in the Federal Government.

(f) Section 2000e-5(e)(3) *[Section 706(e)(3)]* shall apply to complaints of discrimination in compensation under this section.

PROCEDURE FOR DENIAL, WITHHOLDING, TERMINATION, OR SUSPENSION OF GOVERNMENT CONTRACT SUBSEQUENT TO ACCEPTANCE BY GOVERNMENT OF AFFIRMATIVE ACTION PLAN OF EMPLOYER; TIME OF ACCEPTANCE OF PLAN

SEC. 2000e-17. *[Section 718]*

No Government contract, or portion thereof, with any employer, shall be denied, withheld, terminated, or suspended, by any agency or officer of the United States under any equal employment opportunity law or order, where such employer has an affirmative action plan which has previously been accepted by the Government for the same facility within the past twelve months without first according such employer full hearing and adjudication under the provisions of section 554 of Title 5 *[United States Code]*, and the following pertinent sections: Provided, That if such employer has deviated substantially from such previously agreed to affirmative action plan, this section shall not apply: Provided further, That for the purposes of this section an affirmative action plan shall be deemed to have been accepted by the Government at the time the appropriate compliance agency has accepted such plan unless within forty-five days thereafter the Office of Federal Contract Compliance has disapproved such plan.

United States Government Accountability Office

GAO

Report to Congressional Requesters

November 2008

HUMAN CAPITAL

Diversity in the Federal SES and Processes for Selecting New Executives

GAO-09-110

November 2008

HUMAN CAPITAL

Diversity in the Federal SES and Processes for Selecting New Executives

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-09-110, a report to congressional requesters

Why GAO Did This Study

A diverse Senior Executive Service (SES), which generally represents the most experienced segment of the federal workforce, can be an organizational strength by bringing a wider variety of perspectives and approaches to policy development and implementation, strategic planning, problem solving, and decision making. In a January 2003 report (GAO-03-34), GAO provided data on career SES members by race, ethnicity, and gender as of October 2000 and a statistically estimated projection of what the profile of the SES would be in October 2007 if appointment and separation trends did not change.

In response to a request for updated information on the diversity in the SES, GAO is providing information from the Office of Personnel Management's (OPM) Central Personnel Data File (1) on the representation of women and minorities in the SES and the SES developmental pool (i.e., GS-15 and GS-14 positions) for the executive branch as of fiscal year 2007 and comparing this representation to fiscal year 2000 levels and to levels GAO projected for October 2007 in its 2003 report; (2) for fiscal years 2000 and 2007, the average age at which women and minorities were appointed to and retired from the SES as well as information on those in the SES reporting targeted disabilities; and (3) on the overall processes used in executive branch agencies for selecting and certifying members into the SES.

GAO is making no recommendations in this report.

To view the full product, including the scope and methodology, click on GAO-09-110. For more information, contact George H. Stalcup at (202) 512-6806 or stalcupg@gao.gov.

What GAO Found

The representation of women and minorities in the SES and the SES developmental pool increased governmentwide from October 2000 through September 2007, but increases did not occur in all agencies. Over these 7 years, increases occurred in more than half of the 24 major executive branch agencies, but in both 2000 and 2007 the representation of women and minorities continued to vary significantly at those agencies. In 2003, we projected that increases would occur in the representation of women and minorities in the SES and SES developmental pool by 2007. These increases generally did occur.

	October 2000			September 2007		
		Percent			Percent	
Governmentwide	Number	Women	Minorities	Number	Women	Minorities
SES	6, 296	23.2	13.9	6,555	29.1	15.8
SES developmental pool (GS-15s and GS-14s)	137,785	28.0	17.0	149,149	34.3	22.5

Source: GAO analysis of OPM's Central Personnel Data File.

Looking beyond racial, ethnic, and gender profiles, GAO also reviewed the average age at appointment to and retirement from the career SES as well as the disability status reported by career SES employees for fiscal years 2000 and 2007. For the most part, career SES members were, on average, about age 50 at the time of their appointment to the SES and about age 60 at the time of their retirement. The average age at appointment to and retirement from the career SES generally did not vary much by race, ethnicity, or gender. GAO also calculated how long, on average, individuals served in the SES, and found that the length of their stay in the SES did vary. For example, women stayed in the SES longer than men; women who voluntarily retired stayed, on average, for 11.4 years, and men who voluntarily retired stayed, on average, for 8.8 years. The average length of service among minorities ranged from 4.1 years for Asian/Pacific Islander women to 12 years for American Indian/Alaska Native men. Governmentwide less than 1 percent of the career SES in 2000 and 2007 had self-reported targeted disabilities, and their representation declined slightly over this time.

Executive branch agencies have established processes for selecting members into the SES and have developmental programs that are designed to create pools of candidates from which new members can be selected. These agencies use Executive Resources Boards to review the executive and technical qualifications of eligible candidates for initial SES career appointments and make recommendations based on the best qualified. An OPM-administered board reviews candidates' qualifications before appointment to the SES.

Contents

Tables

Abbreviations

AID	Agency for International Development
CFO	Chief Financial Officer
CPDF	Central Personnel Data File
DHS	Department of Homeland Security
EEO	equal employment opportunity
EEOC	Equal Employment Opportunity Commission
EPA	Environmental Protection Agency
ERB	Executive Resources Board
FEMA	Federal Emergency Management Agency
FEORP	Federal Equal Opportunity Recruitment Program
GS	General Schedule
GSA	General Services Administration
HHS	Department of Health and Human Services
HUD	Department of Housing and Urban Development
NASA	National Aeronautics and Space Administration
NRC	Nuclear Regulatory Commission
NSF	National Science Foundation
OPM	Office of Personnel Management
QRB	Qualifications Review Board
SBA	Small Business Administration
SES	Senior Executive Service
SSA	Social Security Administration
VA	Department of Veterans Affairs

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

November 26, 2008

The Honorable Danny K. Davis
Chairman
Subcommittee on Federal Workforce, Postal Service,
and the District of Columbia
Committee on Oversight and Government Reform
House of Representatives

The Honorable Daniel K. Akaka
Chairman
Subcommittee on Oversight of Government Management,
the Federal Workforce and the District of Columbia
Committee on Homeland Security and Governmental Affairs
United States Senate

The federal government continues to face new and more complex challenges in the 21st century resulting from long-term fiscal constraints, changing demographics, and other factors. Leadership in agencies across the federal government, especially at senior executive levels, is essential to providing accountable, committed, consistent, and sustained attention to human capital and related organizational transformation issues. The federal government's senior corps generally represents the most experienced segment of the federal career workforce. Having a diverse senior corps can be an organizational strength that can bring a wider variety of perspectives and approaches to bear on policy development and implementation, strategic planning, problem solving, and decision making.

Over the past several years, we have reported on the diversity of the Senior Executive Service (SES). For example, we issued a January 2003 report that included both a comprehensive review of career SES[1] by race, ethnicity, and gender governmentwide as of October 2000 and a statistically estimated projection of what the profile of the SES would be

[1]Career SES members are those with civil service status who are appointed competitively to SES positions and serve in positions below the top political appointees in the executive branch of government. These individuals are in executive positions classified above GS-15 or equivalent. We excluded those in SES-type positions authorized by law, such as in the Foreign Service, and some law enforcement and intelligence programs as well as positions in the Senior Level and Science and Professional systems.

in October 2007 if appointment and separation trends did not change.[2] Earlier this year, we testified on the diversity of the SES again by race, ethnicity, and gender governmentwide, comparing the results of our 2003 report with the representation of the SES in September 2007.[3] This report goes beyond the representation of the SES in 2007 to include other characteristics of the diversity of the SES, specifically age of SES members and disability status.

As requested, this report updates our January 2003 report and provides information (1) on the representation of women and minorities[4] in the SES and the SES developmental pool (i.e., GS-15 and GS-14 positions)[5] for the executive branch as of fiscal year 2007 and compares this representation to fiscal year 2000 levels and to levels we projected for the end of fiscal year 2007 in our 2003 report; (2) for fiscal years 2000 and 2007, the average age at which women and minorities were appointed to and retired from the SES, the average length of service among those appointed to the SES in fiscal year 1990, as well as information for 2000 and 2007 on the representation of individuals with targeted disabilities among the SES;[6] and (3) on the overall processes used in executive branch agencies for selecting and certifying members into the SES. The information provided for objectives (1) and (3) was reported earlier this year in testimony.[7]

[2]GAO, *Senior Executive Service: Enhanced Agency Efforts Needed to Improve Diversity as the Senior Corps Turns Over*, GAO-03-34 (Washington, D.C.: Jan. 17, 2003).

[3]GAO, *Human Capital: Diversity in the Federal SES and Senior Levels of the U.S. Postal Service and Processes for Selecting New Executives*, GAO-08-609T (Washington, D.C.: Apr. 3, 2008).

[4]By minorities, we are referring to people in the following racial and ethnic groups: African American, American Indian/Alaska Native, Asian/Pacific Islander, and Hispanic.

[5]The vast majority of potential successors for career SES positions come from the general schedule (GS) pay plan for grades GS-15 and GS-14. We included GS-15, GS-14, and equivalent employees. GS-equivalent employees are those in equivalent grades under other pay plans that follow the GS grade structure and job evaluation methodology or are equivalent by statute.

[6]Targeted disabilities are those disabilities the federal government, as a matter of policy, has identified for special emphasis. The targeted disabilities are deafness, blindness, missing extremities, partial paralysis, complete paralysis, convulsive disorders, mental retardation, mental illness, and distortion of limbs and/or spine.

[7]GAO-08-609T.

For this report, we extracted representation data for the SES and the SES developmental pool governmentwide[8] and by Chief Financial Officers Act (CFO)[9] agencies for October 2000 and September 2007 from the Office of Personnel Management's (OPM) Central Personnel Data File (CPDF). We also extracted data from the CPDF to identify average age at appointment and retirement and using those data calculated the mean and median ages of those appointed to or retired from the SES in fiscal years 2000 and 2007. We also calculated how long individuals, on average, served in the SES. To do so, we analyzed data from the CPDF on those appointed to the SES in fiscal year 1990 and followed those individuals through fiscal year 2007 to determine how many were still in the SES. Finally, we identified from the CPDF the representation of individuals in the SES who reported that they had targeted disabilities. We believe the CPDF is sufficiently reliable for the informational purpose of this report because we previously reported that governmentwide data from the CPDF for the key variables in this report—agency, gender, race or national origin, pay plan or grade, and disability status—were 96 percent or more accurate.[10] Some data on the SES and the SES developmental pool for 2000 in this report differ from data in our prior products.[11]

We conducted this performance audit from January 2008 through November 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the

[8]Governmentwide includes civilian employees of all cabinet-level departments, independent agencies, commissions, councils, and boards in the executive branch except the intelligence agencies, the Postal Service, and the Foreign Service (as of 2007).

[9]The CFO Act agencies are 24 major executive agencies that are subject to the CFO Act. In 2007, the CFO Act agencies employed 98 percent of federal employees. See 31 U.S.C. § 901.

[10]GAO, *OPM's Central Personnel Data File: Data Appear Sufficiently Reliable to Meet Most Customer Needs*, GAO/GGD-98-199 (Washington, D.C.: Sept. 30, 1998). Also, in a document dated February 28, 2008, an OPM official confirmed that OPM continues to follow the CPDF data quality standards and procedures contained in our 1998 report.

[11]We first identified SES and SES developmental pool data for 2000 in our 2003 report (GAO-03-34), in which we excluded the Federal Bureau of Investigation (FBI) from the SES and the SES developmental pool because that report contained projected SES and the SES developmental pool levels for the end of fiscal year 2007 based on separation and appointment data, and the FBI did not submit separation and appointment data to the CPDF for 2000. We subsequently cited data on the SES and SES developmental pool for 2000 from our 2003 report in four additional products (GAO-04-123T, GAO-07-838T, GAO-08-609T, and GAO-08-725T). The FBI began submitting such data to the CPDF in fiscal year 2005; therefore data in this report on the SES and the SES developmental pool governmentwide include data on the FBI.

audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Results in Brief

The representation of women and minorities in the SES and the SES developmental pool increased governmentwide from October 2000 through September 2007, but increases did not occur in all agencies. Over these 7 years, increases occurred in more than half of the 24 major executive branch agencies, but in both 2000 and 2007 the representation of women and minorities continued to vary significantly at the 24 major executive branch agencies. In 2003, we projected that increases would occur in the representation of minorities and women in the SES and SES developmental pool by 2007. These increases generally did occur.

Looking beyond racial, ethnic, and gender profiles and as requested, we reviewed the average age at appointment to and retirement from the career SES as well as the disability status of career SES employees for fiscal years 2000 and 2007. We found that for the most part, career SES members were, on average, about age 50 at the time of their appointment to the SES and about age 60 at the time of their retirement. The average age at appointment to and retirement from the career SES generally did not vary much by race, ethnicity, or gender. We also calculated how long individuals, on average, served in the SES by analyzing data on those appointed to the SES in fiscal year 1990 and following those individuals through fiscal year 2007 to determine how many were still in the SES. We found that women stayed in the SES longer than men; women who voluntarily retired (as opposed to taking some other form of retirement, such as mandatory or disability retirement) stayed, on average, for 11.4 years, and men who voluntarily retired stayed, on average, for 8.8 years. The average length of service among minorities ranged from 4.1 years for Asian/Pacific Islander women to 12 years for American Indian men. As for disability status, governmentwide less than 1 percent of the career SES in 2000 and 2007 had self-reported targeted disabilities, and the representation of individuals with these reported disabilities declined slightly between 2000 and 2007.

Executive branch agencies have established processes for selecting members into the SES and have developmental programs that are designed to create pools of candidates from which new members can be selected. These agencies are required by OPM regulations to follow competitive merit staffing requirements when making initial appointments

to the career SES or to the formal candidate development programs, which are competitive programs that are designed to create pools of candidates for SES positions.

We provided the Acting Director of OPM and the Chair of EEOC with a draft of this report for their review and comment. OPM provided technical comments, which we incorporated as appropriate, but did not otherwise comment on the report. EEOC had no comments.

Background

OPM and the Equal Employment Opportunity Commission (EEOC) each play important roles in ensuring equal employment opportunity (EEO) in the federal workplace through their leadership and oversight of federal agencies. In their oversight roles, OPM and EEOC require federal agencies to analyze their workforces, and both agencies also report on governmentwide representation levels.[12] Under OPM's regulations implementing the Federal Equal Opportunity Recruitment Program (FEORP),[13] agencies are required to determine where representation levels for covered groups are lower than in the civilian labor force and take steps to address those differences.[14] Agencies are also required to submit annual FEORP reports to OPM in the form prescribed by OPM. EEOC's Management Directive 715 (MD-715) provides guidance and standards to federal agencies for establishing and maintaining effective equal employment opportunity programs,[15] including a framework for executive branch agencies to help ensure effective management, accountability, and self-analysis to determine whether barriers to equal employment opportunity exist and to identify and develop strategies to mitigate or eliminate the barriers to participation.[16] Specifically, EEOC's MD-715 states that agency personnel programs and policies should be evaluated

[12]OPM's most recent report is its January 2007 *Annual Report to the Congress: Federal Equal Opportunity Recruitment Program, Fiscal Year 2006*, and EEOC's most recent report is its *Fiscal Year 2007 Annual Report on the Federal Work Force.*

[13]5 U.S.C. §7201 and 5 C.F.R. Part 720, Subpart B.

[14]The civilian labor force is composed of those 16 and older who are employed or looking for work and not in the military or institutionalized.

[15]See section 717 of the Civil Rights Act of 1964 and section 501 of the Rehabilitation Act of 1973, codified as amended at 42 U.S.C. § 2000e-16 and 29 U.S.C. § 791, respectively.

[16]EEOC defines barriers as agency policies, principles, or practices that limit or tend to limit employment opportunities for members of a particular gender, race, or ethnic background or based on an individual's disability status.

regularly to ascertain whether such programs have any barriers that tend to limit or restrict equitable opportunities for open competition in the workplace. The initial step is for agencies to analyze their workforce data with designated benchmarks, including the civilian labor force. If analyses of their workforce profiles identify potential barriers, agencies are to examine all related policies, procedures, and practices to determine whether an actual barrier exists. EEOC requires agencies to report the results of their analyses annually. In addition, EEOC recently issued a report on the participation of individuals who reported targeted disabilities in the federal workforce.[17] Targeted disabilities are those disabilities that the federal government, as a matter of policy, has identified for special emphasis. The targeted disabilities are deafness, blindness, missing extremities, partial paralysis, complete paralysis, convulsive disorders, mental retardation, mental illness, and distortion of limb and/or spine.

Women and Minorities in the Career SES and the SES Developmental Pool Increased Governmentwide between 2000 and 2007, and Their Representation in the SES Increased in More Than Half of the Agencies

The data that we are reporting provide a demographic snapshot of the career SES as well as the levels that serve as the SES developmental pool for October 2000 and September 2007. Table 1 shows that governmentwide, the number and percentage of women and minorities in the career SES and SES developmental pool increased between October 2000 and September 2007.

[17]*EEOC, Improving the Participation Rate of People with Targeted Disabilities in the Federal Workforce* (Washington, D.C.: Jan. 2008). Federal employees or applicants for federal employment use OPM Form SF-256 to identify physical or mental impairments. According to EEOC, the information collected from this form is used to produce reports and to ensure that individuals with disabilities are not discriminated against.

Table 1: Career SES and the SES Developmental Pool Governmentwide for October 2000 and September 2007

	October 2000			September 2007		
		Percent			Percent	
Governmentwide	Number	Women	Minorities	Number	Women	Minorities
SES	6,296	23.2	13.9	6,555	29.1	15.8
SES developmental pool (GS-15s and GS-14s)	137,785	28.0	17.0	149,149	34.3	22.5

Source: GAO analysis of OPM's CPDF.

Note: Governmentwide includes civilian employees of all cabinet-level departments, independent agencies, commissions, councils, and boards in the executive branch except the intelligence agencies, the Postal Service, and the Foreign Service (as of 2007).

As shown in table 2, the percentage of both women and minorities in the SES increased in 15 of the 24 CFO Act agencies by 2007. For the remaining CFO Act agencies, most experienced an increase in either the percentage of women or minorities between October 2000 and September 2007.

Table 2: Career SES Members by CFO Act Agency for October 2000 and September 2007

	October 2000			September 2007		
		Percent			Percent	
CFO Act agency	Number of SES	Women	Minorities	Number of SES	Women	Minorities
Agriculture	283	25.4	20.1	318	28.3	18.9
AID	25	20.0	20.0	22	45.5	36.4
Commerce	296	23.3	12.5	317	28.4	14.5
Defense	1,143	16.3	6.1	1,123	22.6	8.3
Education	60	28.3	21.7	66	36.4	15.2
Energy	391	18.9	10.7	421	22.8	14.3
EPA	255	29.8	15.3	261	37.5	17.2
FEMA	32	21.9	3.1	[a]	[a]	[a]
GSA	84	28.6	14.3	80	28.8	15.0
HHS	399	36.1	21.3	356	44.1	20.5
DHS	[b]	[b]	[b]	325	26.2	13.2
HUD	73	28.8	35.6	89	38.2	43.8
Interior	191	31.9	22.0	221	31.7	25.8
Justice	594	18.4	15.2	645	22.2	17.8
Labor	132	28.0	21.2	133	33.1	21.1
NASA	394	19.5	13.2	431	23.4	14.6
NRC	139	13.7	11.5	146	19.9	13.7

	October 2000			September 2007		
		Percent			Percent	
CFO Act agency	Number of SES	Women	Minorities	Number of SES	Women	Minorities
NSF	79	30.4	13.9	79	44.3	16.5
OPM	36	41.7	19.4	42	38.1	16.7
SBA	39	33.3	33.3	36	27.8	38.9
SSA	118	35.6	33.1	134	41.8	27.6
State	101	28.7	5.0	114	32.5	6.1
Transportation	178	27.0	14.6	188	36.2	16.0
Treasury	537	23.3	12.8	386	36.8	18.4
VA	247	14.6	9.7	236	30.9	14.8

Source: GAO analysis of OPM's CPDF.

Note: AID is the Agency for International Development; EPA is the Environmental Protection Agency; GSA is the General Services Administration; HHS is the Department of Health and Human Services; HUD is the Department of Housing and Urban Development; NASA is the National Aeronautics and Space Administration; NRC is the Nuclear Regulatory Commission; NSF is the National Science Foundation; SBA is the Small Business Administration; SSA is the Social Security Administration; and VA is the Department of Veterans Affairs.

[a]The Federal Emergency Management Agency (FEMA) was an independent agency and 1 of the 24 CFO Act agencies until the formation of the Department of Homeland Security (DHS) in 2003.

[b]DHS did not exist before March 2003. It was created from 22 agencies or parts of agencies, including the U.S. Customs Service, which was formerly located in the Department of the Treasury; FEMA; and the Coast Guard.

As we reported in 2003, the gender, racial, and ethnic profiles of the career SES at the 24 CFO Act agencies varied significantly in October 2000. The representation of women ranged from 13.7 percent to 41.7 percent, with half of the agencies having 27 percent or fewer women in the career SES. For minority representation, rates varied even more and ranged from 3.1 percent to 35.6 percent, with half of the agencies having less than 15 percent minorities in the career SES. In 2007, the representation of women and minorities, both overall and in more than half of the individual agencies, was higher than it was in October 2000. The representation of women ranged from 19.9 percent to 45.5 percent with more than half of the agencies having 30 percent or more women. For minority representation, rates ranged from 6.1 percent to 43.8 percent, with more than half of the agencies having over 16 percent minority representation, and more than 90 percent of the agencies having more than 13 percent minority representation in the career SES.

For this report, we did not analyze the factors that contributed to the changes in representation from October 2000 through September 2007. As we said previously, OPM and EEOC, in their oversight roles, require

federal agencies to analyze their workforces and both agencies also report on governmentwide representation levels.

In our 2003 report, we (1) reviewed actual appointment trends from fiscal years 1995 to 2000 and actual separation experience from fiscal years 1996 to 2000; (2) estimated by race, ethnicity, and gender the number of career SES who would leave government service from October 1, 2000, through October 1, 2007; and (3) projected what the profile of the SES would be if appointment and separation trends did not change. We estimated that more than half of the career SES members employed on October 1, 2000, will have left service by October 1, 2007. Assuming then-current career SES appointment trends, we projected that (1) the only significant changes in diversity would be an increase in the number of white women with an essentially equal decrease in white men and (2) the proportions of minority women and men would remain virtually unchanged in the SES corps, although we projected slight increases among most racial and ethnic minorities.

Table 3 shows career SES representation as of October 1, 2000, our 2003 projections of what representation would be at the end of fiscal year 2007, and actual fiscal year 2007 data. We projected increases in representation among both minorities and women. Fiscal year 2007 data show that increases did take place among those groups and that those increases generally exceeded the increases we projected. The only decrease among minorities occurred in African American men, whose representation declined from 5.5 percent in 2000 to 5.0 percent at the end of fiscal year 2007.

Table 3: Fiscal Year 2007 Projections We Reported in 2003 Compared with Actual Fiscal Year 2007 Data for Career SES Governmentwide and Baseline 2000 Data

(Numbers in percent)

SES profile	October 1, 2000	October 2003 projections for October 1, 2007	Actual September 2007
African American men	5.5	5.7	5.0
African American women	2.9	3.4	3.5
American Indian/Alaska Native men	0.9	0.8	0.9
American Indian/Alaska Native women	0.3	0.3	0.4
Asian/Pacific Islander men	1.1	1.1	1.5
Asian/Pacific Islander women	0.5	0.6	0.9
Hispanic men	2.0	2.0	2.7
Hispanic women	0.7	0.7	0.9
White men	67.3	62.1	60.7
White women	18.7	23.1	23.3
Unspecified/other	0.1	0.4	0.2
Total[a]	**100.0**	**100.0**	**100.0**
Minorities	13.9	14.5	15.8
Men	76.8	71.6	70.9
Minority men	9.5	9.5	10.1
Women	23.2	28.1	29.1
Minority women	4.4	5.0	5.8

Source: GAO analysis of CPDF.

Note: Projections include replacements for departing SES members at appointment trends for fiscal years 1995 to 2000 (See GAO-03-34).

[a]Percentages may not add to 100 because of rounding.

Table 4 shows SES developmental pool representation as of October 1, 2000, our 2003 projections of what representation would be at the end of fiscal year 2007, and actual fiscal year 2007 data. We projected increases in representation among both minorities and women. Fiscal year 2007 data show that increases did generally take place among those groups. The representation of American Indian/Alaska Native men remained unchanged from the October 2000 baseline.

Table 4: Fiscal Year 2007 Projections We Reported in 2003 Compared with Actual Fiscal Year 2007 Data for the SES Developmental Pool Governmentwide and Baseline 2000 Data

(Numbers in percent)

Profile of developmental pool (GS-15s and GS-14s)	October 1, 2000	October 2003 projections for October 1, 2007	Actual September 2007
African American men	3.8	4.1	4.3
African American women	4.1	4.5	6.1
American Indian/Alaska Native men	0.6	0.7	0.6
American Indian/Alaska Native women	0.3	0.3	0.4
Asian/Pacific Islander men	3.3	3.1	4.2
Asian/Pacific Islander women	1.4	1.5	2.3
Hispanic men	2.5	2.8	3.0
Hispanic women	1.0	1.2	1.5
White men	61.7	58.6	53.4
White women	21.3	22.9	23.9
Unspecified/other	0.1	0.2	0.2
Total[a]	**100.0**	**100.0**	**100.0**
Minorities	17.0	18.2	22.5
Men	72.0	69.4	65.7
Minority men	10.2	10.7	12.1
Women	28.0	30.4	34.3
Minority women	6.7	7.5	10.3

Source: GAO analysis of CPDF.

Notes: We included GS-15, GS-14, and equivalent employees. GS-equivalent employees are those in equivalent grades under other pay plans that follow the GS grade structure and job evaluation methodology or are equivalent by statute.

Projections include replacements for departing GS-15, GS-14, and equivalent employees at appointment trends for fiscal years 1995-2000 (See GAO-03-34).

[a]Percentages may not add to 100 because of rounding.

As stated previously, we have not analyzed the factors contributing to changes in representation; therefore, care must be taken when comparing changes in demographic data since fiscal year 2000 to the projections we made in 2003, and to the 2007 actual data we present in both tables 3 and 4. For example, we have not determined whether estimated retirement trends materialized or appointment and separation trends used in our projections continued and the impact these factors may have had on the diversity of the SES and its developmental pool.

Considering retirement eligibility and actual retirement rates of the SES is important because individuals normally do not enter the SES until well into their careers; thus, SES retirement eligibility is much higher than the workforce in general. As we have said in previous reports, as part of a strategic human capital planning approach, agencies need to develop long-term strategies for acquiring, developing, motivating, and retaining staff.[18] An agency's human capital plan should address the demographic trends that the agency faces with its workforce, especially retirements. In 2006, OPM reported that approximately 60 percent of the executive branch's 1.6 million white-collar employees and 90 percent of about 6,000 federal executives will be eligible for retirement over the next 10 years. If a significant number of SES members were to retire, it could result in a loss of leadership continuity, institutional knowledge, and expertise among the SES corps, with the degree of loss varying among agencies and occupations. This has important implications for government management and emphasizes the need for good succession planning for this leadership group. Rather than simply recreating the existing organization, effective succession planning and management, linked to the strategic human capital plan, can help an organization become what it needs to be. Leading organizations go beyond a "replacement" approach that focuses on identifying particular individuals as possible successors for specific top-ranking positions. Rather, they typically engage in broad, integrated succession planning and management efforts that focus on strengthening both current and future capacity, anticipating the need for leaders and other key employees with the necessary competencies to successfully meet the complex challenges of the 21st century.

Succession planning also is tied to the federal government's opportunity to affect the diversity of the executive corps through new appointments. In September 2003,[19] we reported that agencies in other countries use succession planning and management to achieve a more diverse workforce, maintain their leadership capacity, and increase the retention of high-potential staff. Racial, ethnic, and gender diversity in the SES is an important component for the effective operation of the government.

[18]GAO, *Human Capital: Federal Workforce Challenges in the 21st Century*, GAO-07-556T (Washington, D.C.: Mar. 6, 2007).

[19]GAO, *Human Capital: Insights for U.S. Agencies from Other Countries' Succession Planning and Management Initiatives*, GAO-03-914 (Washington, D.C.: Sept. 15, 2003).

Minimal Changes Occurred in the Average Age at Appointment to and Retirement from the Career SES and in Targeted Disabilities among the Career SES between 2000 and 2007

Individuals do not typically enter the career SES until well into their careers. As of the end of fiscal years 2000 and 2007, the average age of women and minorities at the time of their appointment to the SES was about age 50 and did not change dramatically over this 7-year period except for certain groups, as shown in table 5. The average age at appointment for American Indian/Alaska Native women declined from age 48 in 2000 to age 42 in 2007 and increased during this time for both American Indian/Alaska Native men (from age 50 in 2000 to 53 in 2007) and white women (from age 47 in 2000 to 49 in 2007).

Table 5: Average Age at Appointment to the Career SES for 2000 and 2007

	Average age at appointment in	
SES profile	**Fiscal year 2000**	**Fiscal year 2007**
African American men	51	50
African American women	48	49
American Indian/Alaska Native men	50	53
American Indian/Alaska Native women	48[a]	42[a]
Asian/Pacific Islander men	52	48
Asian/Pacific Islander women	48[a]	47
Hispanic men	48	49
Hispanic women	50	49
White men	50	50
White women	47	49
Unspecified/other	[b]	52[a]
Governmentwide	**49**	**50**
Men	50	50
Minority men	50	49
Women	47	49
Minority women	48	49

Source: GAO analysis of OPM's CPDF.

Note: The average age is the statistical mean. We compared the average age to the median age for both fiscal years' data and found that the differences between the two were usually minimal and that the median age was less than the mean age in most instances.

[a]Ages of two to five individuals formed the basis for this average.

[b]One or no individuals were appointed in this year.

Similarly, the average age of women and minorities at the time of retirement from the career SES did not change much between 2000 and 2007. As shown in table 6, all of those who retired did so, on average, at

around age 60, with the exception of Asian/Pacific Islander men, whose average retirement age in 2007 was 64; Hispanic men, whose average retirement age in 2000 was 57 and in 2007 was 58; and African American men, whose average retirement age in 2000 was 62 and 59 in 2007.

Table 6: Average Age at Retirement from the Career SES in 2000 and 2007

	Average age at retirement	
SES profile	**Fiscal year 2000**	**Fiscal year 2007**
African American men	62	59
African American women	58[a]	61
American Indian/Alaska Native men	56[a]	59[a]
American Indian/Alaska Native women	[b]	60[a]
Asian/Pacific Islander men	60[a]	64
Asian/Pacific Islander women	[b]	56[a]
Hispanic men	57	58
Hispanic women	[b]	60
White men	60	60
White women	59	58
Unspecified/other	[b]	[b]
Governmentwide	**60**	**59**
Men	60	60
Minority men	60	60
Women	59	58
Minority women	59[a]	60

Source: GAO analysis of OPM's CPDF.

Note: The average age is the statistical mean. We compared the average age to the median age for both fiscal years' data and found that the differences between the two were usually minimal and that the median age was less than the mean age in most instances.

[a]Ages of two to five individuals formed the basis for this average.

[b]One or no individuals retired in this year.

In addition to examining the average age of individuals at the time of their appointment to and retirement from the career SES, we analyzed the length of time that a cohort of individuals served in the SES and differences in length of service. We reviewed data on the 625 individuals appointed to the career SES in fiscal year 1990. Because of questions with the records of 11 individuals, we excluded them from our analysis and analyzed the records of the remaining 614 individuals appointed to the SES in fiscal year 1990 and followed them through September 2007. We found

that 432 of the 614 had left the SES by that date—338 had retired voluntarily, 66 had resigned, and 28 had left for other reasons, such as disability or mandatory retirement. Those individuals who had voluntarily retired served in the SES an average of 9.2 years, as shown in table 7. Table 7 also shows that women stayed in the SES longer than men; women who voluntarily retired stayed, on average, for 11.4 years, and men who voluntarily retired stayed, on average, for 8.8 years. The average length of service among minorities ranged from 4.1 years for Asian/Pacific Islander women to 12 years for American Indian/Alaska Native men.

Table 7: Average Length of Stay of Career SES of Individuals Appointed to the Career SES in 1990 Who Retired or Resigned

SES profile	Number of SES appointed in fiscal year 1990	As of September 30, 2007, average length in SES (in years) among individuals appointed in 1990			
		Voluntary retirements		Resignations	
		Number	Years	Number	Years
African American men	32	22	9.5	0	0.0
African American women	9	5	10.3	0	0.0
American Indian/Alaska Native men	7	3	12.0	2	4.6
American Indian/Alaska Native women	1	0		0	0.0
Asian/Pacific Islander men	1	0	0.0	0	0.0
Asian/Pacific Islander women	2	1	4.1	0	0.0
Hispanic men	5	2	8.7	1	4.6
Hispanic women	1	0	0.0	1	5.6
White men	467	267	8.7	49	4.9
White women	88	38	11.7	13	5.9
Unspecified/other	1	0	0.0	0	0.0
Governmentwide	**614**	**338**	**9.2**	**66**	**5.1**
Men	512	294	8.8	52	4.9
Minority men	45	27	9.8	3	4.6
Women	101	44	11.4	14	5.9
Minority women	13	6	9.3	1	5.6

Source: GAO analysis of OPM's CPDF.

Note: The average number of years in the SES at retirement will increase as those who remained in the SES as of September 30, 2007, retire in the future. We also calculated the median length of service, which showed the same patterns.

The average number of years in the SES does not include those appointed to the SES in 1990 who, as of September 30, 2007, died (10); took other types of retirement, such as disability or mandatory retirement (17); or were terminated (1).

As shown in table 8, as of September 2007, about one-third of the 614 individuals we identified who were appointed to the career SES in 1990 remained in the SES. More women from the original cohort remained than men.

Table 8: Number and Percentage of Individuals Appointed to the Career SES in 1990 Remaining in the SES as of September 2007

SES profile	Number of SES appointed in fiscal year 1990	Those appointed to the SES in fiscal year 1990 remaining, as of September 30, 2007	
		Number	Percent
African American men	32	10	31.3
African American women	9	4	44.4
American Indian/Alaska Native men	7	1	14.3
American Indian/Alaska Native women	1	1	100.0
Asian/Pacific Islander men	1	1	100.0
Asian/Pacific Islander women	2	1	50.0
Hispanic men	5	1	20.0
Hispanic women	1	0	0.0
White men	467	134	28.7
White women	88	28	31.8
Unspecified/other	1	1	100.0
Governmentwide	**614**	**182**	**29.6**
Men	512	147	28.7
Minority men	45	13	28.9
Women	101	34	33.7
Minority women	13	6	46.2

Source: GAO analysis of OPM's CPDF.

We also reviewed the representation of career SES members who reported having targeted disabilities. EEOC reported that it first officially recognized the term targeted disabilities in its Management Directive 703,

which was approved on December 6, 1979.[20] In its report, EEOC stated that some individuals with disabilities are reluctant to self-identify their disability status because they are concerned that (1) such disclosure will preclude them from employment or advancement or subject them to discrimination and (2) their disability status will not remain confidential. It is not clear the extent to which individuals with disabilities do not identify or report them.

Governmentwide, the representation of career SES members reporting targeted disabilities declined from 0.52 in fiscal year 2000 to 0.44 in fiscal year 2007. Table 9 shows the representation of SES members with targeted disabilities governmentwide and within the CFO Act agencies.[21]

Table 9: Career SES Members with Targeted Disabilities Governmentwide and at CFO Act Agencies for 2000 and 2007

	September 2000			September 2007		
		SES with targeted disabilities			SES with targeted disabilities	
	Number of SES	Number	Percent	Number of SES	Number	Percent
Governmentwide	6,296	33	0.52	6,555	29	0.44
CFO Act agencies	5,826	30	0.51	6,169	26	0.42

Source: GAO analysis of OPM's CPDF.

In both 2000 and 2007, half of the CFO Act agencies (12) did not employ any SES members with targeted disabilities.

[20]EEOC recognizes that there are disabilities that are not designated as a "targeted disability," but may nevertheless be just as severe, or more severe, than some targeted disabilities. Nonetheless, EEOC only collects and maintains employment statistics for the nine individual targeted disabilities. EEOC states that the purpose of focusing on targeted disabilities is to encourage the hiring, placement, and advancement of selected individuals with disabilities in affirmative action planning. The criteria EEOC used to select the nine disabilities that make up the group of targeted disabilities included the severity of the disability, the feasibility of recruitment, and the availability of workforce data for individuals with targeted disabilities.

[21]Data on targeted disabilities were not separated out by disability type for this analysis but were rolled into an overall targeted disabilities category.

Processes Used for Selecting Career SES Members Are to Follow Competitive Merit Staffing Requirements

Executive branch agencies have processes for selecting members into the career SES and developmental programs that are designed to create pools of candidates for senior positions. Federal executive agencies are to follow competitive merit staffing requirements for initial career appointments to the SES or for appointment to formal SES candidate development programs, which are competitive programs designed to create pools of candidates for SES positions.[22] Each agency head is to appoint one or more Executive Resources Boards (ERB) to conduct the merit staffing process for initial SES career appointments. ERBs review the executive and technical qualifications of each eligible candidate and make written recommendations to the appointing official concerning the candidates. The appointing official selects from among those candidates identified by the ERB as best qualified and certifies the executive and technical qualifications of those candidates selected.[23] Candidates who are selected must have their executive qualifications certified by an OPM-administered Qualifications Review Board (QRB) before being appointed to the SES.[24]

According to OPM, it convenes weekly QRBs to review the applications of candidates for initial career appointment to the SES. QRBs are independent boards of three senior executives that assess the executive qualifications of all new SES candidates. At least two of the three QRB members must be career appointees.[25] In addition, OPM guidance states that QRB members cannot review candidates from their own agencies. An OPM official stated that an OPM official acts as administrator, attending each QRB to answer questions, moderate, and offer technical guidance but does not vote or influence voting. OPM guidance states that the QRB does not rate, rank, or compare a candidate's qualifications against those of other candidates. Instead, QRB members judge the overall scope, quality, and depth of a candidate's executive qualifications within the context of five executive core qualifications—leading change, leading people, results driven, business acumen, and building coalitions—to certify that the candidate's demonstrated experience meets the executive core qualifications.

[22]See 5 C.F.R. § 317.501(c) and 412.104(c).

[23]See 5 C.F.R. § 317.501 and 5 U.S.C. § 3393(b).

[24]See 5 C.F.R. § 317.502 and 5 U.S.C. § 3393(c).

[25]Statute and OPM regulations provide that more than half of the members of the QRB must be SES career appointees. 5 U.S.C. § 3393(c) and 5 C.F.R. § 317.502(a).

To staff QRBs, an OPM official said that OPM sends a quarterly letter to the heads of agencies' human capital offices seeking volunteers for specific QRBs and encourages agencies to identify women and minority participants. Agencies then inform OPM of scheduled QRB participants, without a stipulation as to the profession of the participants. OPM solicits agencies once a year for an assigned quarter and requests QRB members on a proportional basis. The OPM official said that OPM uses a rotating schedule, so that the same agencies are not contacted each quarter. Although QRBs generally meet weekly, an OPM official said that QRBs can meet more than once a week, depending on case loads. The official said that because of the case load of recruitment for SES positions recently, OPM had been convening a second "ad hoc" QRB. According to another OPM official, after QRB certification, candidates are officially approved and can be placed.

In addition to certification based on demonstrated executive experience and another form of certification based on special or unique qualities,[26] OPM regulations permit the certification of the executive qualifications of graduates of candidate development programs by a QRB and selection for the SES without further competition.[27] OPM regulations state that for agency candidate development programs, agencies must have a written policy describing how their programs will operate and must have OPM approval before conducting them. According to OPM, candidate development programs typically run from 18 to 24 months and are open to GS-15s and GS-14s or employees at equivalent levels from within or outside the federal government. Agencies are to use merit staffing procedures to select participants for their programs, and most program vacancies are announced governmentwide or to all sources. OPM regulations provide that candidates who compete governmentwide for participation in a candidate development program, successfully complete the program, and obtain QRB certification are eligible for noncompetitive

[26]5 C.F.R. § 317.502(c). According to OPM, in very rare cases when exceptional candidates with demonstrated experience are not available, a QRB may certify a candidate whose professional/technical background makes him or her particularly well-suited for an SES vacancy although the candidate lacks demonstrated experience in one or more of the executive core qualifications. The candidate must have the potential for quickly acquiring full competence in all of the core qualifications.

[27]5 C.F.R. § 412.104. See also 5 U.S.C. § 3393(c)(2).

appointment to the SES.[28] OPM guidance states that candidate development program graduates are not guaranteed placement in the SES. Agencies' ERB chairs must certify that candidates have successfully completed all program activities, and OPM staff review candidate packages to verify that regulatory requirements have been met. An "ad hoc" QRB then reviews the candidates' training and development and work experiences to ensure he or she possesses the required executive qualifications.

OPM also periodically sponsors a centrally administered federal candidate development program. According to an OPM official, the OPM-sponsored federal candidate development program can be attractive to smaller agencies that may not have their own candidate development program, and OPM administers the federal program for them. According to OPM officials, from the first OPM-sponsored federal candidate development program, 12 graduated in September 2006. Of those, 9 individuals were placed in SES positions within 1 year of graduating from the program. In January 2008, OPM advertised the second OPM-sponsored federal candidate development program but subsequently suspended the program. In June 2008, OPM re-advertised the second OPM-sponsored federal candidate development program, and 18 candidates were selected for the program and have started their 12-month training and development program.

Agency Comments and Our Evaluation

We provided the Acting Director of OPM and the Chair of EEOC with a draft of this report for their review and comment. OPM provided technical comments via e-mail, which we incorporated as appropriate, but did not otherwise comment on the report. In an e-mail, EEOC said it had no comments.

We are sending copies of this report to the Acting Director of OPM, the Chair of EEOC, and other interested congressional parties. We also make copies available to others upon request. In addition, the report will be available at no charge on GAO's Web site at http://www.gao.gov.

[28]In some cases, candidate development program openings are announced only to an agency's employees rather than governmentwide; graduates from such programs must compete for SES positions. 5 C.F.R. § 412.104.

If you or your staffs have questions about this report, please contact me at (202) 512-9490 or stalcupg@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix II.

George H. Stalcup
Director, Strategic Issues

Appendix I: Demographic Profiles of Career SES, GS-15, and GS-14 Employees Governmentwide and at the 24 Chief Financial Officers Act Agencies

Table 10: Demographic Profiles of Career SES, GS-15, and GS-14 Employees Governmentwide

Equal employment opportunity (EEO) group	SES			
	October 1, 2000		September 2007	
	Number	Percent	Number	Percent
African American men	348	5.5	328	5.0
African American women	180	2.9	232	3.5
American Indian/Alaska Native men	55	0.9	60	0.9
American Indian/Alaska Native women	21	0.3	28	0.4
Asian/Pacific Islander men	70	1.1	96	1.5
Asian/Pacific Islander women	33	0.5	57	0.9
Hispanic men	123	2.0	176	2.7
Hispanic women	43	0.7	60	0.9
White men	4,239	67.3	3,976	60.7
White women	1,180	18.7	1,526	23.3
Unspecified/other	4	0.1	16	0.2
Total[a]	**6,296**	**100.0**	**6,555**	**100.0**
Minorities	873	13.9	1,037	15.8
Men	4,838	76.8	4,646	70.9
Minority men	596	9.5	660	10.1
Women	1,458	23.2	1,909	29.1
Minority women	277	4.4	377	5.8

GS-15				GS-14			
October 1, 2000		September 2007		October 1, 2000		September 2007	
Number	Percent	Number	Percent	Number	Percent	Number	Percent
1,740	3.3	2,123	3.6	3,507	4.1	4,316	4.8
1,516	2.9	2,374	4.1	4,131	4.8	6,734	7.4
278	0.5	353	0.6	584	0.7	585	0.6
103	0.2	193	0.3	296	0.3	397	0.4
2,072	4.0	2,904	5.0	2,463	2.9	3,401	3.7
836	1.6	1,604	2.8	1,042	1.2	1,899	2.1
1,228	2.3	1,660	2.8	2,237	2.6	2,758	3.0
471	0.9	760	1.3	898	1.1	1,433	1.6
33,913	64.8	32,931	56.5	51,059	59.8	46,787	51.5
10,150	19.4	13,326	22.9	19,147	22.4	22,324	24.6
39	0.1	87	0.1	75	0.1	200	0.2
52,346	**100.0**	**58,315**	**100.0**	**85,439**	**100.0**	**90,834**	**100.0**
8,244	15.7	11,971	20.5	15,158	17.7	21,523	23.7
39,258	75.0	40,030	68.6	59,915	70.1	57,973	63.8
5,318	10.2	7,040	12.1	8,791	10.3	11,060	12.2
13,088	25.0	18,285	31.4	25,524	29.9	32,861	36.2
2,926	5.6	4,931	8.5	6,367	7.5	10,463	11.5

Source: GAO analysis of the Office of Personnel Management's Central Personnel Data File.

Notes: Governmentwide includes civilian employees of all cabinet-level departments, independent agencies, commissions, councils, and boards in the executive branch except the intelligence agencies, the Postal Service, and the Foreign Service (as of 2007).

We included GS-15, GS-14, and equivalent employees. GS-equivalent employees are those in equivalent grades under other pay plans that follow the GS grade structure and job evaluation methodology or are equivalent by statute.

Data on the SES and the SES developmental pool for 2000 in this report differ from prior GAO products. We first identified SES and SES developmental pool data for 2000 in our 2003 report (GAO-03-34), in which we excluded the FBI from the SES and the SES developmental pool because that report contained projected SES and the SES developmental pool levels for the end of fiscal year 2007 based on separation and appointment data, and the FBI did not submit separation and appointment data to the CPDF for 2000. We subsequently cited data on the SES and SES developmental pool for 2000 from that report in four additional products (GAO-04-123T, GAO-07-838T, GAO-08-609T, and GAO-08-725T). Data on the SES and the SES developmental pool for 2007 include the FBI.

[a]Percentages may not add to 100 because of rounding.

Table 11: Demographic Profiles of Career SES, GS-15, and GS-14 Employees at the Department of Agriculture

	SES			
	October 1, 2000		September 2007	
EEO group	Number	Percent	Number	Percent
African American men	28	9.9	22	6.9
African American women	11	3.9	11	3.5
American Indian/Alaska Native men	2	0.7	3	0.9
American Indian/Alaska Native women	1	0.4	1	0.3
Asian/Pacific Islander men	5	1.8	8	2.5
Asian/Pacific Islander women	0	0.0	3	0.9
Hispanic men	8	2.8	9	2.8
Hispanic women	2	0.7	3	0.9
White men	168	59.4	186	58.5
White women	58	20.5	71	22.3
Unspecified/other	0	0.0	1	0.3
Total[a]	**283**	**100.0**	**318**	**100.0**
Minorities	57	20.1	60	18.9
Men	211	74.6	228	71.7
Minority men	43	15.2	42	13.2
Women	72	25.4	90	28.3
Minority women	14	4.9	18	5.7

GS-15				GS-14			
October 1, 2000		September 2007		October 1, 2000		September 2007	
Number	Percent	Number	Percent	Number	Percent	Number	Percent
72	4.0	90	4.4	122	3.5	179	4.5
53	2.9	79	3.9	153	4.4	235	5.9
8	0.4	14	0.7	32	0.9	30	0.8
2	0.1	1	0.0	8	0.2	21	0.5
41	2.3	74	3.6	95	2.8	152	3.8
7	0.4	15	0.7	35	1.0	62	1.6
37	2.0	59	2.9	82	2.4	108	2.7
3	0.2	13	0.6	22	0.6	53	1.3
1,302	72.0	1,294	63.4	2,188	63.6	2,148	53.7
283	15.6	401	19.7	695	20.2	1,006	25.2
1	0.1	0	0.0	7	0.2	5	0.1
1,809	**100.0**	**2,040**	**100.0**	**3,439**	**100.0**	**3,999**	**100.0**
223	12.3	345	16.9	549	16.0	840	21.0
1,460	80.7	1,531	75.0	2,519	73.2	2,620	65.5
158	8.7	237	11.6	331	9.6	469	11.7
348	19.2	509	25.0	913	26.5	1,379	34.5
65	3.6	108	5.3	218	6.3	371	9.3

Source: GAO analysis of the Office of Personnel Management's Central Personnel Data File.

Note: We included GS-15, GS-14, and equivalent employees. GS-equivalent employees are those in equivalent grades under other pay plans that follow the GS grade structure and job evaluation methodology or are equivalent by statute.

[a]Percentages may not add to 100 because of rounding.

Table 12: Demographic Profiles of Career SES, GS-15, and GS-14 Employees at the Agency for International Development

	SES			
	October 1, 2000		September 2007	
EEO group	Number	Percent	Number	Percent
African American men	2	8.0	2	9.1
African American women	1	4.0	4	18.2
American Indian/Alaska Native men	1	4.0	0	0.0
American Indian/Alaska Native women	0	0.0	0	0.0
Asian/Pacific Islander men	0	0.0	0	0.0
Asian/Pacific Islander women	0	0.0	1	4.5
Hispanic men	1	4.0	1	4.5
Hispanic women	0	0.0	0	0.0
White men	16	64.0	9	40.9
White women	4	16.0	5	22.7
Unspecified/other	0	0.0	0	0.0
Total[a]	**25**	**100.0**	**22**	**100.0**
Minorities	5	20.0	8	36.4
Men	20	80.0	12	54.5
Minority men	4	16.0	3	13.6
Women	5	20.0	10	45.5
Minority women	1	4.0	5	22.7

GS-15				GS-14			
October 1, 2000		September 2007		October 1, 2000		September 2007	
Number	Percent	Number	Percent	Number	Percent	Number	Percent
24	5.7	18	4.1	23	4.1	31	6.8
19	4.5	28	6.4	36	6.5	70	15.3
2	0.5	0	0.0	1	0.2	0	0.0
1	0.2	0	0.0	0	0.0	1	0.2
9	2.1	10	2.3	17	3.1	13	2.8
6	1.4	9	2.1	10	1.8	13	2.8
11	2.6	13	3.0	15	2.7	12	2.6
1	0.2	4	0.9	3	0.5	5	1.1
257	60.6	230	52.6	290	52.3	170	37.1
94	22.2	125	28.6	160	28.8	143	31.2
0	0.0	0	0.0	0	0.0	0	0.0
424	**100.0**	**437**	**100.0**	**555**	**100.0**	**458**	**100.0**
73	17.2	82	18.8	105	18.9	145	31.7
303	71.5	271	62.0	346	62.3	226	49.3
46	10.8	41	9.4	56	10.1	56	12.2
121	28.5	166	38.0	209	37.7	232	50.7
27	6.4	41	9.4	49	8.8	89	19.4

Source: GAO analysis of the Office of Personnel Management's Central Personnel Data File.

Note: We included GS-15, GS-14, and equivalent employees. GS-equivalent employees are those in equivalent grades under other pay plans that follow the GS grade structure and job evaluation methodology or are equivalent by statute.

[a]Percentages may not add to 100 because of rounding.

Table 13: Demographic Profiles of Career SES, GS-15, and GS-14 Employees at the Department of Commerce

	SES			
	October 1, 2000		September 2007	
EEO group	Number	Percent	Number	Percent
African American men	17	5.7	17	5.4
African American women	5	1.7	9	2.8
American Indian/Alaska Native men	2	0.7	1	0.3
American Indian/Alaska Native women	0	0.0	0	0.0
Asian/Pacific Islander men	3	1.0	5	1.6
Asian/Pacific Islander women	3	1.0	5	1.6
Hispanic men	4	1.4	7	2.2
Hispanic women	3	1.0	2	0.6
White men	201	67.9	197	62.1
White women	58	19.6	74	23.3
Unspecified/other	0	0.0	0	0.0
Total[a]	**296**	**100.0**	**317**	**100.0**
Minorities	37	12.5	46	14.5
Men	227	76.7	227	71.6
Minority men	26	8.8	30	9.5
Women	69	23.3	90	28.4
Minority women	11	3.7	16	5.0

GS-15				GS-14			
October 1, 2000		September 2007		October 1, 2000		September 2007	
Number	Percent	Number	Percent	Number	Percent	Number	Percent
69	3.0	105	3.6	183	3.8	339	4.9
53	2.3	93	3.2	177	3.7	411	6.0
2	0.1	7	0.2	10	0.2	13	0.2
0	0.0	7	0.2	8	0.2	9	0.1
111	4.8	214	7.4	335	7.0	695	10.1
28	1.2	79	2.7	139	2.9	314	4.5
39	1.7	52	1.8	65	1.4	119	1.7
14	0.6	26	0.9	43	0.9	76	1.1
1,573	68.5	1,726	59.8	2,910	60.7	3,480	50.4
408	17.8	577	20.0	923	19.2	1,449	21.0
1	0.0	1	0.0	2	0.0	1	0.0
2,298	**100.0**	**2,887**	**100.0**	**4,795**	**100.0**	**6,906**	**100.0**
316	13.8	583	20.2	960	20.0	1,976	28.6
1,794	78.1	2,105	72.9	3,503	73.1	4,647	67.3
221	9.6	378	13.1	593	12.4	1,166	16.9
503	21.9	782	27.1	1,290	26.9	2,259	32.7
95	4.1	205	7.1	367	7.7	810	11.7

Source: GAO analysis of the Office of Personnel Management's Central Personnel Data File.

Note: We included GS-15, GS-14, and equivalent employees. GS-equivalent employees are those in equivalent grades under other pay plans that follow the GS grade structure and job evaluation methodology or are equivalent by statute.

[a]Percentages may not add to 100 because of rounding.

Table 14: Demographic Profiles of Career SES, GS-15, and GS-14 Employees at the Department of Defense

	SES			
	October 1, 2000		September 2007	
EEO group	Number	Percent	Number	Percent
African American men	21	1.8	27	2.4
African American women	10	0.9	16	1.4
American Indian/Alaska Native men	6	0.5	8	0.7
American Indian/Alaska Native women	1	0.1	2	0.2
Asian/Pacific Islander men	13	1.1	15	1.3
Asian/Pacific Islander women	9	0.8	9	0.8
Hispanic men	7	0.6	12	1.1
Hispanic women	3	0.3	4	0.4
White men	909	79.5	802	71.4
White women	163	14.2	221	19.7
Unspecified/other	2	0.2	7	0.6
Total[a]	**1,144**	**100.0**	**1,123**	**100.0**
Minorities	70	6.1	93	8.3
Men	956	83.6	869	77.4
Minority men	47	4.1	62	5.5
Women	186	16.3	254	22.6
Minority women	23	2.0	31	2.8

GS-15				GS-14			
October 1, 2000		September 2007		October 1, 2000		September 2007	
Number	Percent	Number	Percent	Number	Percent	Number	Percent
231	2.1	221	2.6	604	3.1	576	3.7
124	1.1	122	1.5	468	2.4	486	3.1
50	0.4	33	0.4	72	0.4	63	0.4
9	0.1	12	0.1	24	0.1	24	0.2
282	2.5	307	3.7	554	2.9	563	3.6
37	0.3	69	0.8	141	0.7	184	1.2
158	1.4	173	2.1	335	1.7	386	2.5
28	0.3	40	0.5	104	0.5	139	0.9
8,795	79.0	6,173	73.7	13,612	70.4	10,151	65.8
1,409	12.7	1,221	14.6	3,409	17.6	2,831	18.3
14	0.1	5	0.1	25	0.1	32	0.2
11,137	**100.0**	**8,376**	**100.00**	**19,348**	**100.0**	**15,435**	**100.0**
919	8.3	977	11.7	2,302	11.9	2,421	15.7
9,516	85.4	6,911	82.5	15,177	78.4	11,756	76.2
721	6.5	734	8.8	1,565	8.1	1,588	10.3
1,607	14.4	1,465	17.5	4,146	21.4	3,679	23.8
198	1.8	243	2.9	737	3.8	833	5.4

Source: GAO analysis of the Office of Personnel Management's Central Personnel Data File.

Note: We included GS-15, GS-14, and equivalent employees. GS-equivalent employees are those in equivalent grades under other pay plans that follow the GS grade structure and job evaluation methodology or are equivalent by statute.

[a]Percentages may not add to 100 because of rounding.

Table 15: Demographic Profiles of Career SES, GS-15, and GS-14 Employees at the Department of Education

	SES			
	October 1, 2000		September 2007	
EEO group	Number	Percent	Number	Percent
African American men	8	13.3	3	4.5
African American women	1	1.7	5	7.6
American Indian/Alaska Native men	1	1.7	0	0.0
American Indian/Alaska Native women	0	0.0	0	0.0
Asian/Pacific Islander men	1	1.7	1	1.5
Asian/Pacific Islander women	1	1.7	1	1.5
Hispanic men	1	1.7	0	0.0
Hispanic women	0	0.0	0	0.0
White men	32	53.3	38	57.6
White women	15	25.0	18	27.3
Unspecified/other	0	0.0	0	0.0
Total[a]	**60**	**100.0**	**66**	**100.0**
Minorities	13	21.7	10	15.2
Men	43	71.7	42	63.6
Minority men	11	18.3	4	6.1
Women	17	28.3	24	36.4
Minority women	2	3.3	6	9.1

GS-15				GS-14			
October 1, 2000		September 2007		October 1, 2000		September 2007	
Number	Percent	Number	Percent	Number	Percent	Number	Percent
31	6.7	30	6.3	68	8.7	68	8.0
40	8.7	51	10.8	117	14.9	154	18.2
1	0.2	2	0.4	3	0.4	2	0.2
4	0.9	4	0.8	3	0.4	3	0.4
7	1.5	8	1.7	10	1.3	19	2.2
1	0.2	3	0.6	10	1.3	25	2.9
8	1.7	7	1.5	9	1.1	12	1.4
6	1.3	5	1.1	12	1.5	11	1.3
212	46.1	187	39.5	300	38.2	270	31.8
150	32.6	177	37.3	254	32.3	284	33.5
0	0.0	0	0.0	0	0.0	0	0.0
460	**100.0**	**474**	**100.0**	**786**	**100.0**	**848**	**100.0**
98	21.3	110	23.2	232	29.5	294	34.7
259	56.3	234	49.4	390	49.6	371	43.8
47	10.2	47	9.9	90	11.5	101	11.9
201	43.7	240	50.6	396	50.4	477	56.3
51	11.1	63	13.3	142	18.1	193	22.8

Source: GAO analysis of the Office of Personnel Management's Central Personnel Data File.

Note: We included GS-15, GS-14, and equivalent employees. GS-equivalent employees are those in equivalent grades under other pay plans that follow the GS grade structure and job evaluation methodology or are equivalent by statute.

[a]Percentages may not add to 100 because of rounding.

Table 16: Demographic Profiles of Career SES, GS-15, and GS-14 Employees at the Department of Energy

	SES			
	October 1, 2000		September 2007	
EEO group	Number	Percent	Number	Percent
African American men	14	3.6	16	3.8
African American women	5	1.3	7	1.7
American Indian/Alaska Native men	3	0.8	2	0.5
American Indian/Alaska Native women	0	0.0	2	0.5
Asian/Pacific Islander men	8	2.0	5	1.2
Asian/Pacific Islander women	1	0.3	6	1.4
Hispanic men	9	2.3	17	4.0
Hispanic women	2	0.5	5	1.2
White men	283	72.4	285	67.7
White women	66	16.9	76	18.1
Unspecified/other	0	0.0	0	0.0
Total[a]	**391**	**100.0**	**421**	**100.0**
Minorities	42	10.7	60	14.3
Men	317	81.1	325	77.2
Minority men	34	8.7	40	9.5
Women	74	18.9	96	22.8
Minority women	8	2.0	20	4.8

GS-15				GS-14			
October 1, 2000		September 2007		October 1, 2000		September 2007	
Number	Percent	Number	Percent	Number	Percent	Number	Percent
65	3.3	68	3.4	84	3.0	82	3.0
44	2.2	65	3.3	106	3.8	151	5.6
7	0.4	13	0.7	20	0.7	21	0.8
3	0.2	3	0.2	8	0.3	11	0.4
59	3.0	85	4.3	128	4.6	112	4.1
14	0.7	29	1.5	29	1.0	39	1.4
42	2.1	42	2.1	91	3.2	95	3.5
10	0.5	21	1.1	34	1.2	68	2.5
1,429	71.5	1,230	62.3	1,731	61.7	1,475	54.4
325	16.3	418	21.2	573	20.4	645	23.8
1	0.1	1	0.1	2	0.1	10	0.4
1,999	**100.0**	**1,975**	**100.0**	**2,806**	**100.0**	**2,709**	**100.0**
244	12.2	326	16.5	500	17.8	579	21.4
1,602	80.1	1,439	72.9	2,054	73.2	1,792	66.1
173	8.7	208	10.5	323	11.5	310	11.4
396	19.8	536	27.1	750	26.7	917	33.9
71	3.6	118	6.0	177	6.3	269	9.9

Source: GAO analysis of the Office of Personnel Management's Central Personnel Data File.

Note: We included GS-15, GS-14, and equivalent employees. GS-equivalent employees are those in equivalent grades under other pay plans that follow the GS grade structure and job evaluation methodology or are equivalent by statute.

[a]Percentages may not add to 100 because of rounding.

Table 17: Demographic Profiles of Career SES, GS-15, and GS-14 Employees at the Environmental Protection Agency

	SES			
	October 1, 2000		September 2007	
EEO group	Number	Percent	Number	Percent
African American men	18	7.1	14	5.4
African American women	5	2.0	10	3.8
American Indian/Alaska Native men	0	0.0	0	0.0
American Indian/Alaska Native women	0	0.0	1	0.4
Asian/Pacific Islander men	2	0.8	3	1.1
Asian/Pacific Islander women	4	1.6	4	1.5
Hispanic men	9	3.5	11	4.2
Hispanic women	1	0.4	2	0.8
White men	150	58.8	134	51.3
White women	66	25.9	81	31.0
Unspecified/other	0	0.0	1	0.4
Total[a]	**255**	**100.0**	**261**	**100.0**
Minorities	39	15.3	45	17.2
Men	179	70.2	163	62.5
Minority men	29	11.4	28	10.7
Women	76	29.8	98	37.5
Minority women	10	3.9	17	6.5

GS-15				GS-14			
October 1, 2000		September 2007		October 1, 2000		September 2007	
Number	Percent	Number	Percent	Number	Percent	Number	Percent
41	2.3	61	2.6	102	3.4	129	4.4
80	4.4	132	5.7	201	6.7	257	8.8
2	0.1	6	0.3	7	0.2	6	0.2
2	0.1	4	0.2	5	0.2	6	0.2
30	1.7	46	2.0	78	2.6	98	3.4
14	0.8	37	1.6	49	1.6	69	2.4
27	1.5	46	2.0	63	2.1	72	2.5
14	0.8	40	1.7	48	1.6	51	1.8
1,086	60.2	1,211	52.2	1,558	51.9	1,325	45.5
508	28.1	728	31.4	890	29.7	896	30.8
1	0.1	9	0.4	0	0.0	4	0.1
1,805	**100.0**	**2,320**	**100.0**	**3,001**	**100.0**	**2,913**	**100.0**
210	11.6	372	16.0	553	18.4	688	23.6
1,186	65.7	1,377	59.4	1,808	60.2	1,632	56.0
100	5.5	159	6.9	250	8.3	305	10.5
618	34.2	943	40.6	1,193	39.8	1,281	44.0
110	6.1	213	9.2	303	10.1	383	13.1

Source: GAO analysis of the Office of Personnel Management's Central Personnel Data File.

Note: We included GS-15, GS-14, and equivalent employees. GS-equivalent employees are those in equivalent grades under other pay plans that follow the GS grade structure and job evaluation methodology or are equivalent by statute.

[a]Percentages may not add to 100 because of rounding.

Table 18: Demographic Profiles of Career SES, GS-15, and GS-14 Employees at the General Services Administration

	SES			
	October 1, 2000		September 2007	
EEO group	Number	Percent	Number	Percent
African American men	6	7.1	3	3.8
African American women	4	4.8	5	6.3
American Indian/Alaska Native men	0	0.0	0	0.0
American Indian/Alaska Native women	0	0.0	0	0.0
Asian/Pacific Islander men	0	0.0	1	1.3
Asian/Pacific Islander women	1	1.2	0	0.0
Hispanic men	0	0.0	1	1.3
Hispanic women	1	1.2	2	2.5
White men	54	64.3	52	65.0
White women	18	21.4	16	20.0
Unspecified/other	0	0.0	0	0.0
Total[a]	**84**	**100.0**	**80**	**100.0**
Minorities	12	14.3	12	15.0
Men	60	71.4	57	71.3
Minority men	6	7.1	5	6.3
Women	24	28.6	23	28.8
Minority women	6	7.1	7	8.8

GS-15				GS-14			
October 1, 2000		September 2007		October 1, 2000		September 2007	
Number	Percent	Number	Percent	Number	Percent	Number	Percent
28	4.7	34	5.4	85	6.5	137	8.6
31	5.2	52	8.2	125	9.6	180	11.3
3	0.5	2	0.3	4	0.3	4	0.3
0	0.0	1	0.2	2	0.2	2	0.1
6	1.0	11	1.7	31	2.4	45	2.8
4	0.7	11	1.7	14	1.1	32	2.0
3	0.5	10	1.6	16	1.2	32	2.0
4	0.7	7	1.1	13	1.0	25	1.6
383	64.4	323	51.1	656	50.3	707	44.4
133	22.4	178	28.2	359	27.5	423	26.6
0	0.0	3	0.5	0	0.0	6	0.4
595	**100.0**	**632**	**100.0**	**1,305**	**100.0**	**1,593**	**100.0**
79	13.3	128	20.3	290	22.2	457	28.7
423	71.1	383	60.6	792	60.7	927	58.2
40	6.7	57	9.0	136	10.4	218	13.7
172	28.9	249	39.4	513	39.3	666	41.8
39	6.6	71	11.2	154	11.8	239	15.0

Source: GAO analysis of the Office of Personnel Management's Central Personnel Data File.

Note: We included GS-15, GS-14, and equivalent employees. GS-equivalent employees are those in equivalent grades under other pay plans that follow the GS grade structure and job evaluation methodology or are equivalent by statute.

[a]Percentages may not add to 100 because of rounding.

Table 19: Demographic Profiles of Career SES, GS-15, and GS-14 Employees at the Department of Health and Human Services

	SES			
	October 1, 2000		September 2007	
EEO group	Number	Percent	Number	Percent
African American men	22	5.5	18	5.1
African American women	27	6.8	24	6.7
American Indian/Alaska Native men	11	2.8	12	3.4
American Indian/Alaska Native women	6	1.5	6	1.7
Asian/Pacific Islander men	6	1.5	3	0.8
Asian/Pacific Islander women	3	0.8	4	1.1
Hispanic men	5	1.3	6	1.7
Hispanic women	5	1.3	0	0.0
White men	211	52.9	160	44.9
White women	103	25.8	123	34.6
Unspecified/other	0	0.0	0	0.0
Total[a]	**399**	**100.0**	**356**	**100.0**
Minorities	85	21.3	73	20.5
Men	255	63.9	199	55.9
Minority men	44	11.0	39	11.0
Women	144	36.1	157	44.1
Minority women	41	10.3	34	9.6

GS-15				GS-14			
October 1, 2000		September 2007		October 1, 2000		September 2007	
Number	Percent	Number	Percent	Number	Percent	Number	Percent
137	3.9	161	3.7	225	3.9	296	4.0
139	4.0	221	5.0	359	6.2	658	9.0
46	1.3	60	1.4	73	1.3	76	1.0
29	0.8	50	1.1	83	1.4	103	1.4
101	2.9	144	3.3	223	3.9	362	4.9
49	1.4	116	2.6	158	2.7	316	4.3
53	1.5	74	1.7	103	1.8	120	1.6
38	1.1	59	1.3	56	1.0	103	1.4
1,774	50.9	1,886	43.0	2,450	42.5	2,493	34.1
1,118	32.1	1,610	36.7	2,024	35.1	2,764	37.8
4	0.1	10	0.2	10	0.2	26	0.4
3,488	**100.0**	**4,391**	**100.0**	**5,764**	**100.0**	**7,317**	**100.0**
592	17.0	885	20.2	1,280	22.2	2,034	27.8
2,111	60.5	2,329	53.0	3,074	53.3	3,363	46.0
337	9.7	439	10.0	624	10.8	854	11.7
1,373	39.4	2,062	47.0	2,680	46.5	3,954	54.0
255	7.3	446	10.2	656	11.4	1,180	16.1

Source: GAO analysis of the Office of Personnel Management's Central Personnel Data File.

Note: We included GS-15, GS-14, and equivalent employees. GS-equivalent employees are those in equivalent grades under other pay plans that follow the GS grade structure and job evaluation methodology or are equivalent by statute.

[a]Percentages may not add to 100 because of rounding.

Table 20: Demographic Profiles of Career SES, GS-15, and GS-14 Employees at the Department of Homeland Security

	SES			
	October 1, 2000		September 2007	
EEO group	Number	Percent	Number	Percent
African American men	[b]	[b]	13	4.0
African American women	[b]	[b]	7	2.2
American Indian/Alaska Native men	[b]	[b]	1	0.3
American Indian/Alaska Native women	[b]	[b]	0	0.0
Asian/Pacific Islander men	[b]	[b]	1	0.3
Asian/Pacific Islander women	[b]	[b]	1	0.3
Hispanic men	[b]	[b]	18	5.5
Hispanic women	[b]	[b]	2	0.6
White men	[b]	[b]	207	63.7
White women	[b]	[b]	75	23.1
Unspecified/other	[b]	[b]	0	0.0
Total[a]	[b]	[b]	**325**	**100.0**
Minorities	[b]	[b]	43	13.2
Men	[b]	[b]	240	73.8
Minority men	[b]	[b]	33	10.2
Women	[b]	[b]	85	26.2
Minority women	[b]	[b]	10	3.1

GS-15				GS-14			
October 1, 2000		September 2007		October 1, 2000		September 2007	
Number	Percent	Number	Percent	Number	Percent	Number	Percent
[b]	[b]	140	4.6	[b]	[b]	327	4.6
[b]	[b]	146	4.8	[b]	[b]	537	7.6
[b]	[b]	12	0.4	[b]	[b]	24	0.3
[b]	[b]	4	0.1	[b]	[b]	15	0.2
[b]	[b]	46	1.5	[b]	[b]	158	2.2
[b]	[b]	27	0.9	[b]	[b]	111	1.6
[b]	[b]	134	4.4	[b]	[b]	507	7.2
[b]	[b]	60	2.0	[b]	[b]	185	2.6
[b]	[b]	1,728	57.0	[b]	[b]	3,741	52.9
[b]	[b]	733	24.2	[b]	[b]	1,462	20.7
[b]	[b]	2	0.1	[b]	[b]	8	0.1
[b]	[b]	**3,032**	**100.0**	[b]	[b]	**7,075**	**100.0**
[b]	[b]	569	18.8	[b]	[b]	1,864	26.3
[b]	[b]	2,061	68.0	[b]	[b]	4,763	67.3
[b]	[b]	332	10.9	[b]	[b]	1,016	14.4
[b]	[b]	971	32.0	[b]	[b]	2,312	32.7
[b]	[b]	237	7.8	[b]	[b]	848	12.0

Source: GAO analysis of the Office of Personnel Management's Central Personnel Data File.

Note: We included GS-15, GS-14, and equivalent employees. GS-equivalent employees are those in equivalent grades under other pay plans that follow the GS grade structure and job evaluation methodology or are equivalent by statute.

[a]Percentages may not add to 100 because of rounding.

[b]The Department of Homeland Security did not exist before March 2003. Its creation united 22 agencies or parts of agencies, including the U.S. Customs Service, which was formerly located in the Department of the Treasury; the Federal Emergency Management Agency; and the Coast Guard.

Table 21: Demographic Profiles of Career SES, GS-15, and GS-14 Employees at the Department of Housing and Urban Development

	SES			
	October 1, 2000		September 2007	
EEO group	Number	Percent	Number	Percent
African American men	9	12.3	12	13.5
African American women	11	15.1	18	20.2
American Indian/Alaska Native men	1	1.4	1	1.1
American Indian/Alaska Native women	1	1.4	0	0.0
Asian/Pacific Islander men	0	0.0	1	1.1
Asian/Pacific Islander women	0	0.0	2	2.2
Hispanic men	2	2.7	3	3.4
Hispanic women	2	2.7	2	2.2
White men	40	54.8	38	42.7
White women	7	9.6	12	13.5
Unspecified/other	0	0.0	0	0.0
Total[a]	**73**	**100.0**	**89**	**100.0**
Minorities	26	35.6	39	43.8
Men	52	71.2	55	61.8
Minority men	12	16.4	17	19.1
Women	21	28.8	34	38.2
Minority women	14	19.2	22	24.7

GS-15				GS-14			
October 1, 2000		September 2007		October 1, 2000		September 2007	
Number	Percent	Number	Percent	Number	Percent	Number	Percent
100	11.7	111	12.0	134	10.1	140	10.0
112	13.1	177	19.1	221	16.7	315	22.5
7	0.8	9	1.0	9	0.7	5	0.4
0	0.0	1	0.1	2	0.2	5	0.4
12	1.4	22	2.4	26	2.0	36	2.6
9	1.1	11	1.2	18	1.4	35	2.5
21	2.5	28	3.0	47	3.5	47	3.3
22	2.6	20	2.2	22	1.7	39	2.8
398	46.5	357	38.6	545	41.1	446	31.8
175	20.4	188	20.3	301	22.7	335	23.9
0	0.0	2	0.2	0	0.0	0	0.0
856	**100.0**	**926**	**100.0**	**1,325**	**100.0**	**1,403**	**100.0**
283	33.1	379	40.9	479	36.2	622	44.3
538	62.9	528	57.0	761	57.4	674	48.0
140	16.4	170	18.4	216	16.3	228	16.3
318	37.1	398	43.0	564	42.6	729	52.0
143	16.7	209	22.6	263	19.8	394	28.1

Source: GAO analysis of the Office of Personnel Management's Central Personnel Data File.

Note: We included GS-15, GS-14, and equivalent employees. GS-equivalent employees are those in equivalent grades under other pay plans that follow the GS grade structure and job evaluation methodology or are equivalent by statute.

[a]Percentages may not add to 100 because of rounding.

Table 22: Demographic Profiles of Career SES, GS-15, and GS-14 Employees at the Department of the Interior

	SES			
	October 1, 2000		September 2007	
EEO group	Number	Percent	Number	Percent
African American men	4	2.1	8	3.6
African American women	4	2.1	8	3.6
American Indian/Alaska Native men	18	9.4	20	9.0
American Indian/Alaska Native women	7	3.7	7	3.2
Asian/Pacific Islander men	1	0.5	4	1.8
Asian/Pacific Islander women	0	0.0	0	0.0
Hispanic men	4	2.1	5	2.3
Hispanic women	4	2.1	5	2.3
White men	103	53.9	112	50.7
White women	46	24.1	50	22.6
Unspecified/other	0	0.0	2	0.9
Total[a]	**191**	**100.0**	**221**	**100.0**
Minorities	42	22.0	57	25.8
Men	130	68.1	151	68.3
Minority men	27	14.1	37	16.7
Women	61	31.9	70	31.7
Minority women	15	7.9	20	9.0

GS-15				GS-14			
October 1, 2000		September 2007		October 1, 2000		September 2007	
Number	Percent	Number	Percent	Number	Percent	Number	Percent
32	2.5	28	1.8	54	1.9	68	2.0
18	1.4	28	1.8	70	2.4	95	2.8
65	5.0	85	5.4	145	5.0	167	4.9
25	1.9	52	3.3	79	2.7	119	3.5
16	1.2	17	1.1	38	1.3	44	1.3
4	0.3	11	0.7	16	0.6	33	1.0
14	1.1	24	1.5	61	2.1	82	2.4
3	0.2	6	0.4	24	0.8	49	1.4
928	71.2	986	62.7	1,859	63.9	1,936	56.4
198	15.2	332	21.1	561	19.3	818	23.8
1	0.1	4	0.3	1	0.0	23	0.7
1,304	**100.0**	**1,573**	**100.0**	**2,908**	**100.0**	**3,434**	**100.0**
177	13.6	251	16.0	487	16.7	657	19.1
1,055	80.9	1,143	72.7	2,157	74.2	2,314	67.4
127	9.7	154	9.8	298	10.2	361	10.5
248	19.0	430	27.3	750	25.8	1,120	32.6
50	3.8	97	6.2	189	6.5	296	8.6

Source: GAO analysis of the Office of Personnel Management's Central Personnel Data File.

Note: We included GS-15, GS-14, and equivalent employees. GS-equivalent employees are those in equivalent grades under other pay plans that follow the GS grade structure and job evaluation methodology or are equivalent by statute.

[a]Percentages may not add to 100 because of rounding.

Table 23: Demographic Profiles of Career SES, GS-15, and GS-14 Employees at the Department of Justice

	SES			
	October 1, 2000		September 2007	
EEO group	Number	Percent	Number	Percent
African American men	39	6.6	50	7.8
African American women	14	2.4	21	3.3
American Indian/Alaska Native men	3	0.5	5	0.8
American Indian/Alaska Native women	0	0.0	1	0.2
Asian/Pacific Islander men	3	0.5	3	0.5
Asian/Pacific Islander women	2	0.3	1	0.2
Hispanic men	27	4.5	31	4.8
Hispanic women	2	0.3	3	0.5
White men	413	69.5	412	63.9
White women	91	15.3	117	18.1
Unspecified/other	0	0.0	1	0.2
Total[a]	**594**	**100.0**	**645**	**100.0**
Minorities	90	15.2	115	17.8
Men	485	81.6	502	77.8
Minority men	72	12.1	89	13.8
Women	109	18.4	143	22.2
Minority women	18	3.0	26	4.0

GS-15				GS-14			
October 1, 2000		September 2007		October 1, 2000		September 2007	
Number	Percent	Number	Percent	Number	Percent	Number	Percent
154	3.6	214	4.2	341	5.2	450	6.0
155	3.6	223	4.3	320	4.9	529	7.0
11	0.3	11	0.2	28	0.4	36	0.5
6	0.1	10	0.2	8	0.1	11	0.1
67	1.5	119	2.3	102	1.6	192	2.5
48	1.1	79	1.5	58	0.9	66	0.9
160	3.7	184	3.6	367	5.6	381	5.1
63	1.5	78	1.5	90	1.4	107	1.4
2,478	57.3	2,793	54.3	3,799	58.0	4,118	54.7
1,179	27.3	1,425	27.7	1,423	21.7	1,619	21.5
3	0.1	6	0.1	10	0.2	22	0.3
4,324	**100.0**	**5,142**	**100.0**	**6,546**	**100.0**	**7,531**	**100.0**
664	15.4	918	17.9	1,314	20.1	1,772	23.5
2,872	66.4	3,325	64.7	4,646	71.0	5,198	69.0
392	9.1	528	10.3	838	12.8	1,059	14.1
1,452	33.6	1,817	35.3	1,900	29.0	2,333	31.0
272	6.3	390	7.6	476	7.3	713	9.5

Source: GAO analysis of the Office of Personnel Management's Central Personnel Data File.

Notes: We included GS-15, GS-14, and equivalent employees. GS-equivalent employees are those in equivalent grades under other pay plans that follow the GS grade structure and job evaluation methodology or are equivalent by statute.

The data on Justice for 2000 in this report differ from such data in prior GAO products. We first identified Justice SES and GS-15 and GS-14 data for 2000 in our 2003 report (GAO-03-34), in which we excluded the FBI from Justice data because that report contained projected SES and SES developmental pool levels for the end of fiscal year 2007 based on separation and appointment data, and the FBI did not submit separation and appointment data to the CPDF for 2000. We subsequently cited 2000 data from that report in four additional products (GAO-04-123T, GAO-07-838T, GAO-08-609T, GAO-08-725T).

The data on Justice for 2007 include the FBI.

[a]Percentages may not add to 100 because of rounding.

Table 24: Demographic Profiles of Career SES, GS-15, and GS-14 Employees at the Department of Labor

	SES			
	October 1, 2000		September 2007	
EEO group	Number	Percent	Number	Percent
African American men	13	9.8	8	6.0
African American women	8	6.1	7	5.3
American Indian/Alaska Native men	0	0.0	1	0.8
American Indian/Alaska Native women	1	0.8	0	0.0
Asian/Pacific Islander men	0	0.0	1	0.8
Asian/Pacific Islander women	0	0.0	2	1.5
Hispanic men	6	4.5	5	3.8
Hispanic women	0	0.0	4	3.0
White men	76	57.6	74	55.6
White women	28	21.2	31	23.3
Unspecified/other	0	0.0	0	0.0
Total[a]	**132**	**100.0**	**133**	**100.0**
Minorities	28	21.2	28	21.1
Men	95	72.0	89	66.9
Minority men	19	14.4	15	11.3
Women	37	28.0	44	33.1
Minority women	9	6.8	13	9.8

GS-15				GS-14			
October 1, 2000		September 2007		October 1, 2000		September 2007	
Number	Percent	Number	Percent	Number	Percent	Number	Percent
31	5.0	45	5.7	87	6.1	86	5.7
33	5.3	52	6.6	128	8.9	173	11.5
2	0.3	2	0.3	9	0.6	10	0.7
2	0.3	0	0.0	4	0.3	3	0.2
2	0.3	9	1.1	25	1.7	43	2.8
8	1.3	10	1.3	7	0.5	33	2.2
14	2.2	16	2.0	46	3.2	45	3.0
8	1.3	12	1.5	22	1.5	28	1.9
378	60.4	406	51.3	728	50.7	677	44.9
148	23.6	239	30.2	381	26.5	411	27.2
0	0.0	0	0.0	0	0.0	0	0.0
626	**100.0**	**791**	**100.0**	**1,437**	**100.0**	**1,509**	**100.0**
100	16.0	146	18.5	328	22.8	421	27.9
427	68.2	478	60.4	895	62.3	861	57.1
49	7.8	72	9.1	167	11.6	184	12.2
199	31.8	313	39.6	542	37.7	648	42.9
51	8.1	74	9.4	161	11.2	237	15.7

Source: GAO analysis of the Office of Personnel Management's Central Personnel Data File.

Note: We included GS-15, GS-14, and equivalent employees. GS-equivalent employees are those in equivalent grades under other pay plans that follow the GS grade structure and job evaluation methodology or are equivalent by statute.

[a]Percentages may not add to 100 because of rounding.

Table 25: Demographic Profiles of Career SES, GS-15, and GS-14 Employees at the National Aeronautics and Space Administration

	SES			
	October 1, 2000		September 2007	
EEO group	Number	Percent	Number	Percent
African American men	18	4.6	13	3.0
African American women	11	2.8	13	3.0
American Indian/Alaska Native men	3	0.8	0	0.0
American Indian/Alaska Native women	1	0.3	1	0.2
Asian/Pacific Islander men	9	2.3	13	3.0
Asian/Pacific Islander women	1	0.3	4	0.9
Hispanic men	7	1.8	14	3.2
Hispanic women	2	0.5	5	1.2
White men	280	71.1	290	67.3
White women	62	15.7	77	17.9
Unspecified/other	0	0.0	1	0.2
Total[a]	**394**	**100.0**	**431**	**100.0**
Minorities	52	13.2	63	14.6
Men	317	80.5	330	76.6
Minority men	37	9.4	40	9.3
Women	77	19.5	101	23.4
Minority women	15	3.8	23	5.3

GS-15				GS-14			
October 1, 2000		September 2007		October 1, 2000		September 2007	
Number	Percent	Number	Percent	Number	Percent	Number	Percent
63	2.5	119	3.2	123	3.3	161	3.8
23	0.9	88	2.4	80	2.1	178	4.2
13	0.5	14	0.4	21	0.6	28	0.7
1	0.0	6	0.2	8	0.2	8	0.2
124	4.9	199	5.3	160	4.3	217	5.1
26	1.0	49	1.3	37	1.0	57	1.3
61	2.4	135	3.6	125	3.3	145	3.4
19	0.7	33	0.9	34	0.9	50	1.2
1,890	74.4	2,441	65.4	2,588	69.0	2,519	59.6
318	12.5	641	17.2	574	15.3	853	20.2
3	0.1	6	0.2	0	0.0	9	0.2
2,541	**100.0**	**3,731**	**100.0**	**3,750**	**100.0**	**4,225**	**100.0**
330	13.0	643	17.2	588	15.7	844	20.0
2,151	84.7	2,914	78.1	3,017	80.5	3,073	72.7
261	10.3	467	12.5	429	11.4	551	13.0
387	15.2	817	21.9	733	19.5	1,152	27.3
69	2.7	176	4.7	159	4.2	293	6.9

Source: GAO analysis of the Office of Personnel Management's Central Personnel Data File.

Note: We included GS-15, GS-14, and equivalent employees. GS-equivalent employees are those in equivalent grades under other pay plans that follow the GS grade structure and job evaluation methodology or are equivalent by statute.

[a]Percentages may not add to 100 because of rounding.

Table 26: Demographic Profiles of Career SES, GS-15, and GS-14 Employees at the Nuclear Regulatory Commission

	SES			
	October 1, 2000		September 2007	
EEO group	Number	Percent	Number	Percent
African American men	7	5.0	7	4.8
African American women	2	1.4	3	2.1
American Indian/Alaska Native men	0	0.0	1	0.7
American Indian/Alaska Native women	0	0.0	0	0.0
Asian/Pacific Islander men	4	2.9	5	3.4
Asian/Pacific Islander women	1	0.7	2	1.4
Hispanic men	2	1.4	1	0.7
Hispanic women	0	0.0	1	0.7
White men	107	77.0	103	70.5
White women	16	11.5	23	15.8
Unspecified/other	0	0.0	0	0.0
Total[a]	**139**	**100.0**	**146**	**100.0**
Minorities	16	11.5	20	13.7
Men	120	86.3	117	80.1
Minority men	13	9.4	14	9.6
Women	19	13.7	29	19.9
Minority women	3	2.2	6	4.1

GS-15				GS-14			
October 1, 2000		September 2007		October 1, 2000		September 2007	
Number	Percent	Number	Percent	Number	Percent	Number	Percent
18	2.8	37	4.1	27	3.8	38	4.5
16	2.5	24	2.6	21	2.9	56	6.6
3	0.5	5	0.5	0	0.0	2	0.2
0	0.0	1	0.1	0	0.0	0	0.0
56	8.7	85	9.3	52	7.2	68	8.0
8	1.2	19	2.1	8	1.1	15	1.8
4	0.6	17	1.9	14	1.9	22	2.6
2	0.3	3	0.3	2	0.3	8	0.9
453	70.7	553	60.6	467	65.0	500	58.9
81	12.6	169	18.5	128	17.8	138	16.3
0	0.0	0	0.0	0	0.0	2	0.2
641	**100.0**	**913**	**100.0**	**719**	**100.0**	**849**	**100.0**
107	16.7	191	20.9	124	17.2	209	24.6
534	83.3	697	76.3	560	77.9	631	74.3
81	12.6	144	15.8	93	12.9	130	15.3
107	16.7	216	23.7	159	22.1	218	25.7
26	4.1	47	5.1	31	4.3	79	9.3

Source: GAO analysis of the Office of Personnel Management's Central Personnel Data File.

Note: We included GS-15, GS-14, and equivalent employees. GS-equivalent employees are those in equivalent grades under other pay plans that follow the GS grade structure and job evaluation methodology or are equivalent by statute.

[a]Percentages may not add to 100 because of rounding.

Table 27: Demographic Profiles of Career SES, GS-15, and GS-14 Employees at the National Science Foundation

	SES			
	October 1, 2000		September 2007	
EEO group	Number	Percent	Number	Percent
African American men	5	6.3	2	2.5
African American women	1	1.3	2	2.5
American Indian/Alaska Native men	0	0.0	0	0.0
American Indian/Alaska Native women	0	0.0	0	0.0
Asian/Pacific Islander men	3	3.8	4	5.1
Asian/Pacific Islander women	1	1.3	2	2.5
Hispanic men	1	1.3	3	3.8
Hispanic women	0	0.0	0	0.0
White men	46	58.2	35	44.3
White women	22	27.8	31	39.2
Unspecified/other	0	0.0	0	0.0
Total[a]	**79**	**100.0**	**79**	**100.0**
Minorities	11	13.9	13	16.5
Men	55	69.6	44	55.7
Minority men	9	11.4	9	11.4
Women	24	30.4	35	44.3
Minority women	2	2.5	4	5.1

GS-15				GS-14			
October 1, 2000		September 2007		October 1, 2000		September 2007	
Number	Percent	Number	Percent	Number	Percent	Number	Percent
4	4.9	4	4.9	3	3.8	6	5.2
4	4.9	6	7.3	10	12.5	15	13.0
1	1.2	0	0.0	0	0.0	0	0.0
0	0.0	0	0.0	0	0.0	1	0.9
1	1.2	1	1.2	0	0.0	3	2.6
2	2.4	4	4.9	3	3.8	1	0.9
0	0.0	0	0.0	1	1.3	3	2.6
1	1.2	0	0.0	1	1.3	0	0.0
36	43.9	33	40.2	31	38.8	35	30.4
33	40.2	34	41.5	31	38.8	51	44.3
0	0.0	0	0.0	0	0.0	0	0.0
82	**100.0**	**82**	**100.0**	**80**	**100.0**	**115**	**100.0**
13	15.9	15	18.3	18	22.5	29	25.2
42	51.2	38	46.3	35	43.8	47	40.9
6	7.3	5	6.1	4	5.0	12	10.4
40	48.8	44	53.7	45	56.3	68	59.1
7	8.5	10	12.2	14	17.5	17	14.8

Source: GAO analysis of the Office of Personnel Management's Central Personnel Data File.

Note: We included GS-15, GS-14, and equivalent employees. GS-equivalent employees are those in equivalent grades under other pay plans that follow the GS grade structure and job evaluation methodology or are equivalent by statute.

[a]Percentages may not add to 100 because of rounding.

Table 28: Demographic Profiles of Career SES, GS-15, and GS-14 Employees at the Office of Personnel Management

	SES			
	October 1, 2000		September 2007	
EEO group	Number	Percent	Number	Percent
African American men	2	5.6	1	2.4
African American women	1	2.8	2	4.8
American Indian/Alaska Native men	0	0.0	0	0.0
American Indian/Alaska Native women	1	2.8	0	0.0
Asian/Pacific Islander men	0	0.0	1	2.4
Asian/Pacific Islander women	0	0.0	0	0.0
Hispanic men	2	5.6	2	4.8
Hispanic women	1	2.8	1	2.4
White men	17	47.2	22	52.4
White women	12	33.3	13	31.0
Unspecified/other	0	0.0	0	0.0
Total[a]	**36**	**100.0**	**42**	**100.0**
Minorities	7	19.4	7	16.7
Men	21	58.3	26	61.9
Minority men	4	11.1	4	9.5
Women	15	41.7	16	38.1
Minority women	3	8.3	3	7.1

GS-15				GS-14			
October 1, 2000		September 2007		October 1, 2000		September 2007	
Number	Percent	Number	Percent	Number	Percent	Number	Percent
7	6.6	13	8.6	14	6.3	19	5.1
5	4.7	14	9.2	22	9.9	74	19.9
0	0.0	0	0.0	0	0.0	0	0.0
0	0.0	0	0.0	0	0.0	2	0.5
0	0.0	1	0.7	4	1.8	5	1.3
0	0.0	0	0.0	2	0.9	12	3.2
3	2.8	4	2.6	7	3.2	4	1.1
3	2.8	3	2.0	4	1.8	8	2.2
62	58.5	72	47.4	96	43.2	127	34.2
26	24.5	45	29.6	73	32.9	120	32.3
0	0.0	0	0.0	0	0.0	0	0.0
106	**100.0**	**152**	**100.0**	**222**	**100.0**	**371**	**100.0**
18	17.0	35	23.0	53	23.9	124	33.4
72	67.9	90	59.2	121	54.5	155	41.8
10	9.4	18	11.8	25	11.3	28	7.5
34	32.1	62	40.8	101	45.5	216	58.2
8	7.5	17	11.2	28	12.6	96	25.9

Source: GAO analysis of the Office of Personnel Management's Central Personnel Data File.

Note: We included GS-15, GS-14, and equivalent employees. GS-equivalent employees are those in equivalent grades under other pay plans that follow the GS grade structure and job evaluation methodology or are equivalent by statute.

[a]Percentages may not add to 100 because of rounding.

Table 29: Demographic Profiles of Career SES, GS-15, and GS-14 Employees at the Small Business Administration

	SES			
	October 1, 2000		September 2007	
EEO group	Number	Percent	Number	Percent
African American men	6	15.4	6	16.7
African American women	4	10.3	2	5.6
American Indian/Alaska Native men	0	0.0	0	0.0
American Indian/Alaska Native women	0	0.0	0	0.0
Asian/Pacific Islander men	0	0.0	0	0.0
Asian/Pacific Islander women	0	0.0	1	2.8
Hispanic men	2	5.1	4	11.1
Hispanic women	1	2.6	1	2.8
White men	18	46.2	16	44.4
White women	8	20.5	6	16.7
Unspecified/other	0	0.0	0	0.0
Total[a]	**39**	**100.0**	**36**	**100.0**
Minorities	13	33.3	14	38.9
Men	26	66.7	26	72.2
Minority men	8	20.5	10	27.8
Women	13	33.3	10	27.8
Minority women	5	12.8	4	11.1

GS-15				GS-14			
October 1, 2000		September 2007		October 1, 2000		September 2007	
Number	Percent	Number	Percent	Number	Percent	Number	Percent
13	7.3	14	7.3	26	7.0	24	6.9
11	6.1	21	10.9	27	7.3	45	12.9
3	1.7	2	1.0	0	0.0	1	0.3
0	0.0	0	0.0	0	0.0	0	0.0
2	1.1	5	2.6	8	2.2	7	2.0
0	0.0	3	1.6	7	1.9	14	4.0
11	6.1	11	5.7	13	3.5	6	1.7
4	2.2	6	3.1	10	2.7	13	3.7
99	55.3	96	49.7	186	50.4	155	44.5
36	20.1	35	18.1	92	24.9	83	23.9
0	0.0	0	0.0	0	0.0	0	0.0
179	**100.0**	**193**	**100.0**	**369**	**100.0**	**348**	**100.0**
44	24.6	62	32.1	91	24.7	110	31.6
128	71.5	128	66.3	233	63.1	193	55.5
29	16.2	32	16.6	47	12.7	38	10.9
51	28.5	65	33.7	136	36.9	155	44.5
15	8.4	30	15.5	44	11.9	72	20.7

Source: GAO analysis of the Office of Personnel Management's Central Personnel Data File.

Note: We included GS-15, GS-14, and equivalent employees. GS-equivalent employees are those in equivalent grades under other pay plans that follow the GS grade structure and job evaluation methodology or are equivalent by statute.

[a]Percentages may not add to 100 because of rounding.

Table 30: Demographic Profiles of Career SES, GS-15, and GS-14 Employees at the Social Security Administration

	SES			
	October 1, 2000		September 2007	
EEO group	Number	Percent	Number	Percent
African American men	13	11.0	13	9.7
African American women	12	10.2	12	9.0
American Indian/Alaska Native men	0	0.0	0	0.0
American Indian/Alaska Native women	0	0.0	1	0.7
Asian/Pacific Islander men	0	0.0	0	0.0
Asian/Pacific Islander women	2	1.7	0	0.0
Hispanic men	7	5.9	6	4.5
Hispanic women	5	4.2	5	3.7
White men	56	47.5	59	44.0
White women	23	19.5	38	28.4
Unspecified/other	0	0.0	0	0.0
Total[a]	**118**	**100.0**	**134**	**100.0**
Minorities	39	33.1	37	27.6
Men	76	64.4	78	58.2
Minority men	20	16.9	19	14.2
Women	42	35.6	56	41.8
Minority women	19	16.1	18	13.4

GS-15				GS-14			
October 1, 2000		September 2007		October 1, 2000		September 2007	
Number	Percent	Number	Percent	Number	Percent	Number	Percent
34	6.8	40	5.6	99	5.8	151	6.0
39	7.8	90	12.7	162	9.5	336	13.4
1	0.2	5	0.7	14	0.8	15	0.6
4	0.8	6	0.8	7	0.4	12	0.5
3	0.6	5	0.7	16	0.9	35	1.4
0	0.0	7	1.0	15	0.9	34	1.4
15	3.0	24	3.4	60	3.5	76	3.0
7	1.4	10	1.4	43	2.5	95	3.8
267	53.7	300	42.2	836	49.1	939	37.4
127	25.6	224	31.5	450	26.4	813	32.4
0	0.0	0	0.0	0	0.0	5	0.2
497	**100.0**	**711**	**100.0**	**1,702**	**100.0**	**2,511**	**100.0**
103	20.7	187	26.3	416	24.4	754	30.0
320	64.4	374	52.6	1,025	60.2	1,217	48.5
53	10.7	74	10.4	189	11.1	277	11.0
177	35.6	337	47.4	677	39.8	1,294	51.5
50	10.1	113	15.9	227	13.3	477	19.0

Source: GAO analysis of the Office of Personnel Management's Central Personnel Data File.

Note: We included GS-15, GS-14, and equivalent employees. GS-equivalent employees are those in equivalent grades under other pay plans that follow the GS grade structure and job evaluation methodology or are equivalent by statute.

[a]Percentages may not add to 100 because of rounding.

Table 31: Demographic Profiles of Career SES, GS-15, and GS-14 Employees at the Department of State

	SES			
	October 1, 2000		September 2007	
EEO group	Number	Percent	Number	Percent
African American men	0	0.0	2	1.8
African American women	1	1.0	1	0.9
American Indian/Alaska Native men	0	0.0	0	0.0
American Indian/Alaska Native women	0	0.0	0	0.0
Asian/Pacific Islander men	0	0.0	2	1.8
Asian/Pacific Islander women	0	0.0	0	0.0
Hispanic men	4	4.0	2	1.8
Hispanic women	0	0.0	0	0.0
White men	68	67.3	71	62.3
White women	28	27.7	36	31.6
Unspecified/other	0	0.0	0	0.0
Total[a]	**101**	**100.0**	**114**	**100.0**
Minorities	5	5.0	7	6.1
Men	72	71.3	77	67.5
Minority men	4	4.0	6	5.3
Women	29	28.7	37	32.5
Minority women	1	1.0	1	0.9

GS-15				GS-14			
October 1, 2000		September 2007		October 1, 2000		September 2007	
Number	Percent	Number	Percent	Number	Percent	Number	Percent
58	3.7	20	2.9	74	2.9	61	5.3
52	3.3	36	5.2	88	3.5	96	8.3
6	0.4	3	0.4	5	0.2	0	0.0
1	0.1	0	0.0	4	0.2	1	0.1
25	1.6	10	1.5	66	2.6	39	3.4
15	0.9	14	2.0	30	1.2	22	1.9
46	2.9	7	1.0	67	2.6	21	1.8
22	1.4	8	1.2	28	1.1	14	1.2
972	61.3	360	52.3	1,584	62.3	530	45.8
387	24.4	224	32.6	598	23.5	357	30.8
2	0.1	6	0.9	0	0.0	17	1.5
1,586	**100.0**	**688**	**100.0**	**2,544**	**100.0**	**1,158**	**100.0**
225	14.2	98	14.2	362	14.2	254	21.9
1,107	69.8	404	58.7	1,796	70.6	663	57.3
135	8.5	40	5.8	212	8.3	121	10.4
477	30.1	284	41.3	748	29.4	495	42.7
90	5.7	58	8.4	150	5.9	133	11.5

Source: GAO analysis of the Office of Personnel Management's Central Personnel Data File.

Notes: We included GS-15, GS-14, and equivalent employees. GS-equivalent employees are those in equivalent grades under other pay plans that follow the GS grade structure and job evaluation methodology or are equivalent by statute.

The number of GS-15s, GS-14s and equivalents decreased because the Department of State stopped reporting data on Foreign Service employees to the Office of Personnel Management's Central Personnel Data File in fiscal year 2006.

[a]Percentages may not add to 100 because of rounding.

Table 32: Demographic Profiles of Career SES, GS-15, and GS-14 Employees at the Department of Transportation

	SES			
	October 1, 2000		September 2007	
EEO group	Number	Percent	Number	Percent
African American men	14	7.9	11	5.9
African American women	7	3.9	10	5.3
American Indian/Alaska Native men	0	0.0	0	0.0
American Indian/Alaska Native women	0	0.0	0	0.0
Asian/Pacific Islander men	5	2.8	6	3.2
Asian/Pacific Islander women	0	0.0	1	0.5
Hispanic men	0	0.0	1	0.5
Hispanic women	0	0.0	1	0.5
White men	111	62.4	102	54.3
White women	41	23.0	56	29.8
Unspecified/other	0	0.0	0	0.0
Total[a]	**178**	**100.0**	**188**	**100.0**
Minorities	26	14.6	30	16.0
Men	130	73.0	120	63.8
Minority men	19	10.7	18	9.6
Women	48	27.0	68	36.2
Minority women	7	3.9	12	6.4

GS-15				GS-14			
October 1, 2000		September 2007		October 1, 2000		September 2007	
Number	Percent	Number	Percent	Number	Percent	Number	Percent
60	5.1	55	5.5	221	4.5	239	5.6
41	3.5	54	5.4	202	4.1	213	4.9
11	0.9	3	0.3	52	1.0	39	0.9
2	0.2	1	0.1	15	0.3	6	0.1
26	2.2	29	2.9	150	3.0	147	3.4
8	0.7	15	1.5	29	0.6	46	1.1
29	2.5	29	2.9	181	3.6	174	4.0
5	0.4	11	1.1	51	1.0	39	0.9
789	67.6	609	60.5	3,289	66.3	2,754	64.0
196	16.8	197	19.6	768	15.5	642	14.9
0	0.0	3	0.3	4	0.1	5	0.1
1,167	**100.0**	**1,006**	**100.0**	**4,962**	**100.0**	**4,304**	**100.0**
182	15.6	197	19.6	901	18.2	903	21.0
915	78.4	726	72.2	3,893	78.5	3,357	78.0
126	10.8	116	11.5	604	12.2	599	13.9
252	21.6	280	27.8	1,065	21.5	947	22.0
56	4.8	81	8.1	297	6.0	304	7.1

Source: GAO analysis of the Office of Personnel Management's Central Personnel Data File.

Note: We included GS-15, GS-14, and equivalent employees. GS-equivalent employees are those in equivalent grades under other pay plans that follow the GS grade structure and job evaluation methodology or are equivalent by statute.

[a]Percentages may not add to 100 because of rounding.

Table 33: Demographic Profiles of Career SES, GS-15, and GS-14 Employees at the Department of the Treasury

	SES			
	October 1, 2000		September 2007	
EEO group	Number	Percent	Number	Percent
African American men	42	7.8	29	7.5
African American women	11	2.0	12	3.1
American Indian/Alaska Native men	1	0.2	0	0.0
American Indian/Alaska Native women	2	0.4	5	1.3
Asian/Pacific Islander men	4	0.7	9	2.3
Asian/Pacific Islander women	1	0.2	4	1.0
Hispanic men	6	1.1	8	2.1
Hispanic women	2	0.4	4	1.0
White men	359	66.9	198	51.3
White women	109	20.3	115	29.8
Unspecified/other	0	0.0	2	0.5
Total[a]	**537**	**100.0**	**386**	**100.0**
Minorities	69	12.8	71	18.4
Men	412	76.7	244	63.2
Minority men	53	9.9	46	11.9
Women	125	23.3	142	36.8
Minority women	16	3.0	25	6.5

GS-15				GS-14			
October 1, 2000		September 2007		October 1, 2000		September 2007	
Number	Percent	Number	Percent	Number	Percent	Number	Percent
148	4.8	73	4.0	417	4.7	284	4.7
148	4.8	136	7.5	583	6.6	774	12.7
12	0.4	5	0.3	46	0.5	20	0.3
6	0.2	3	0.2	16	0.2	20	0.3
46	1.5	42	2.3	149	1.7	151	2.5
18	0.6	35	1.9	95	1.1	191	3.1
85	2.8	36	2.0	286	3.2	117	1.9
27	0.9	19	1.1	114	1.3	114	1.9
1,844	59.8	887	49.1	4,902	55.5	2,555	41.9
746	24.2	564	31.2	2,219	25.1	1,848	30.3
3	0.1	5	0.3	5	0.1	17	0.3
3,083	**100.0**	**1,805**	**100.0**	**8,832**	**100.0**	**6,091**	**100.0**
490	15.9	349	19.3	1,706	19.3	1,671	27.4
2,135	69.3	1,045	57.9	5,800	65.7	3,135	51.5
291	9.4	156	8.6	898	10.2	572	9.4
945	30.7	760	42.1	3,027	34.3	2,956	48.5
199	6.5	193	10.7	808	9.1	1,099	18.0

Source: GAO analysis of the Office of Personnel Management's Central Personnel Data File.

Note: We included GS-15, GS-14, and equivalent employees. GS-equivalent employees are those in equivalent grades under other pay plans that follow the GS grade structure and job evaluation methodology or are equivalent by statute.

[a]Percentages may not add to 100 because of rounding.

Table 34: Demographic Profiles of Career SES, GS-15, and GS-14 Employees at the Department of Veterans Affairs

	SES			
	October 1, 2000		September 2007	
EEO group	Number	Percent	Number	Percent
African American men	12	4.9	13	5.5
African American women	4	1.6	7	3.0
American Indian/Alaska Native men	3	1.2	5	2.1
American Indian/Alaska Native women	0	0.0	0	0.0
Asian/Pacific Islander men	1	0.4	2	0.8
Asian/Pacific Islander women	1	0.4	1	0.4
Hispanic men	3	1.2	6	2.5
Hispanic women	0	0.0	1	0.4
White men	190	76.9	136	57.6
White women	31	12.6	64	27.1
Unspecified/other	2	0.8	1	0.4
Total[a]	**247**	**100.0**	**236**	**100.0**
Minorities	24	9.7	35	14.8
Men	209	84.6	163	69.1
Minority men	19	7.7	26	11.0
Women	36	14.6	73	30.9
Minority women	5	2.0	9	3.8

GS-15				GS-14			
October 1, 2000		September 2007		October 1, 2000		September 2007	
Number	Percent	Number	Percent	Number	Percent	Number	Percent
173	2.2	296	2.7	98	4.0	177	5.2
109	1.4	239	2.2	104	4.2	279	8.2
17	0.2	55	0.5	11	0.4	12	0.4
4	0.1	25	0.2	7	0.3	9	0.3
997	12.9	1,337	12.2	62	2.5	70	2.1
499	6.4	892	8.1	45	1.8	50	1.5
322	4.2	471	4.3	55	2.2	60	1.8
131	1.7	243	2.2	28	1.1	53	1.6
4,382	56.6	5,439	49.7	1,465	59.2	1,643	48.3
1,107	14.3	1,927	17.6	592	23.9	1,044	30.7
5	0.1	22	0.2	8	0.3	4	0.1
7,746	**100.0**	**10,946**	**100.0**	**2,475**	**100.0**	**3,401**	**100.0**
2,252	29.1	3,558	32.5	410	16.6	710	20.9
5,891	76.1	7,614	69.6	1,691	68.3	1,965	57.8
1,509	19.5	2,159	19.7	226	9.1	319	9.4
1,850	23.9	3,332	30.4	776	31.4	1,436	42.2
743	9.6	1,399	12.8	184	7.4	391	11.5

Source: GAO analysis of the Office of Personnel Management's Central Personnel Data File.

Note: We included GS-15, GS-14, and equivalent employees. GS-equivalent employees are those in equivalent grades under other pay plans that follow the GS grade structure and job evaluation methodology or are equivalent by statute.

[a]Percentages may not add to 100 because of rounding.

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

George H. Stalcup on (202) 512-9490 or at stalcupg@gao.gov

Acknowledgments

In addition to the individual named above, Kiki Theodoropoulos, Assistant Director; Clifton Douglas, Jr.; Jessica Drucker; Karin Fangman; Kirsten B. Lauber; Mary Martin; Michael R. Volpe; and Gregory H. Wilmoth made key contributions to this report.

U.S. GOVERNMENT PRINTING OFFICE

KEEPING AMERICA INFORMED

AUDIT REPORT 08-10

DIVERSITY MANAGEMENT PROGRAMS AT THE GOVERNMENT PRINTING OFFICE

September 11, 2008

OFFICE OF INSPECTOR GENERAL

U.S. GOVERNMENT PRINTING OFFICE
KEEPING AMERICA INFORMED
WASHINGTON, DC 20401

Memorandum

OFFICE OF THE INSPECTOR GENERAL

DATE: September 11, 2008

REPLY TO ATTN OF: Assistant Inspector General for Audits and Inspections

SUBJECT: Final Report on Audit of Diversity Management Programs at the GPO
Report Number 08-10

TO: Public Printer
Director, Office of Equal Employment Opportunity
Chief Human Capital Officer

Enclosed please find the subject final report. Please refer to the Executive Summary for the overall audit results. Our evaluation of your response has been incorporated into the body of the report and is included in its entirety as Appendix J. While management concurred with each of the report's recommendations, specific planned actions for each of the recommendations were not provided. We are requesting that you provide additional details related to specific actions the Agency plans to take to implement the recommendations. As a result, pending receipt of details related to implementation, each of the recommendations is considered unresolved. The final report distribution is in Appendix L.

We appreciate the courtesies extended to the audit staff. If you have any questions concerning the report, please contact Mr. Joseph Verch, Supervisory Auditor at (202) 512-0065, or me at (202) 512-2009.

(Original signed by)

Kevin J. Carson
Assistant Inspector General for Audits and Inspections

cc:
Chief of Staff
Chief Management Officer
General Counsel

Contents

Office of Inspector General

Report Number 08-10 **September 11, 2008**

Diversity Management Programs at the Government Printing Office

Executive Summary

Background. The Government Printing Office (GPO) Office of Inspector General (OIG) has completed an audit of diversity management programs at the GPO. The audit was conducted in response to a request from the Chairman of the Subcommittee on Federal Workforce, Postal Service, and the District of Columbia, of the House of Representatives' Committee on Oversight and Government Reform. The Subcommittee requested that the OIGs of each legislative branch agency assess the programs the diversity offices have in place to address diversity concerns.[1] The participating OIGs plan to publish the final results in a consolidated report by September 2008.

Objectives. The overall objective of the audit was to review diversity within GPO, specifically to:

- Identify and assess the diversity program at GPO to determine if it is yielding the desired results—that of creating a more diverse population of women and minorities in top leadership positions, specifically the Senior Level Service (SLS);[2]

- Evaluate the accuracy and completeness of the complaints and discrimination data reported to Congress; and

- Assess the degree to which diversity offices or functions are independent of the General Counsel and the Public Printer.

See Appendix A for details on the audit objectives, scope, and methodology.

Results of Audit. While not mandated to comply with the guidelines and directives of the Equal Employment Opportunity Commission (EEOC) concerning model affirmative action programs, prior to this audit commencing, senior officials at GPO, including the Directors of the Office of Equal Employment Opportunity (EEO) and Human Capital began adopting some elements of both EEOC Management Directive 715 (MD-715) and

[1] Other legislative branch agencies include the Library of Congress, Government Accountability Office, Architect of the Capitol, and the Capitol Police.
[2] Senior Level Service is the GPO equivalent to the Senior Executive Service (SES).

the leading diversity management practices identified by the Government Accountability Office (GAO). GPO has also made progress in developing its pool of Grade 15s (PG-15s) to ensure a qualified minority pool for the Agency's SLS.[3] However, improvements can be made towards enhancing the diversity of the Agency's corps of SLS employees.

The audit also showed that GPO complaints and discrimination data reported to the EEOC during fiscal year (FY) 2007 and eventually reported to Congress were accurate and complete. (See Appendix G). Further, although diversity management programs are incorporated in the Affirmative Employment Program (AEP) Division of GPO's EEO Office, the Director of EEO is independent of the General Counsel, and to a certain extent independent of the Public Printer in EEO matters. (See Appendix H).

Opportunities do exist for GPO to provide a more diverse population of qualified women and minorities in top leadership positions by incorporating the remaining essential elements of MD-715 as well as implementing the nine leading practices for diversity management identified by the GAO. Such modifications should help the agency manage the workforce and create an environment that helps diminish barriers for protected groups. In addition, changes brought about through diversity management should help attract and retain capable employees. With an expectation that a high percentage of the Government workforce will retire in the next decade, GPO should continue developing a comprehensive diversity program to meet those employment challenges.

The audit specifically identified that although GPO is not required to comply with MD-715 or GAO's leading diversity management practices:

- GPO has generally adopted three elements for creating and maintaining a model EEO program identified by MD-715, referred to as (1) demonstrated commitment from leadership, (2) efficiency, and (3) responsiveness and legal compliance. (Finding A); and

- Agency officials have partially adopted one of the GAO's nine leading diversity management practices (top leadership commitment). (Finding B).

Recommendations. We made two recommendations to GPO management, which, if implemented, should not only improve the GPO diversity program by providing a more diverse population of qualified women and minorities in top leadership, but also contribute to GPO's ability to meet its future employment challenges.

Management's Response. GPO Management concurred with each of the report's two recommendations and stated that implementation would require the Public Printer's review and approval (see Appendix J).

[3] At GPO, a Printing Office Grade (PG) 15 is the senior most grade and is generally equivalent to the General Schedule (GS) Grade 15 classified by the Office of Personnel Management. Positions at GPO above Grade PG-15 are in the Senior Level Service (SLS).

Evaluation of Management's Response. While GPO management concurred with each of the recommendations, they did not provide details regarding what actions the Agency plans to take to implement the recommendations. As a result, pending receipt of details related to implementation, the recommendations are considered unresolved.

Introduction

In November 2007, the Chairman of the Federal Workforce, Postal Service, and the District of Columbia Subcommittee of the House of Representatives' Oversight and Government Reform Committee issued a report entitled "Senior Executive Service: Women and Minorities are Underrepresented in Most Legislative Branch Agencies."[4] The report discusses racial and gender diversity of the Senior Executive Service corps in the six legislative branch agencies during FY 2007. The report stated that:

- Minorities represent 16.8 percent and women represent 35.8 percent of Senior Executive Service corps members in the six legislative branch agencies.

- In FY 2007, Senior Executive Service corps members at each agency were less diverse in terms of minorities than the agency's workforce as a whole and in four of the six agencies less diverse in terms of women.

- The representation of minorities in the legislative branch Senior Executive Service corps is stagnant, with representation of women improving only slightly between FY 2002 and FY 2007.

- General Schedule-15 successor pools[5] at some agencies were less diverse than the Senior Executive Service corps.

- In some agencies, the average total salary for minorities and women in FY 2007 was less than for nonminority and male counterparts.

To ensure equal opportunity and diversity, the EEO Office at the GPO is responsible for complying with civil rights statutes and regulations governing Federal employment.[6] As of January 28, 2008, GPO had a total of 2,263 white and blue collar employees (see Appendix C). White collar employees generally consist of administrative, technical, clerical, professional and management personnel while blue collar employees consist generally of those employees who work in production departments. Of the 2,263 employees at GPO, 956 were women (42.3 percent) and 1,359 were minorities (60.1 percent). On staff at GPO are a total of 26 SLS employees consisting of 3 women (11.5 percent) and 3 minorities (11.5 percent). For white collar workers, the ratio between women and minorities and SLS employees was similar—645 women (42.3 percent) and

[4] Report may be found at http://federalworkforce.oversight.house.gov/story.asp?ID=1617

[5] The November 2007 report of the Chairman of the Federal Workforce, Postal Service, and the District of Columbia Subcommittee of the House of Representatives' Oversight and Government Reform Committee defines successor pools as an agency's GS-15 and equivalent ranks of which the diversity of such pools can provide an indicator of how diverse the Senior Executive Service (or equivalent rank) could become in the future.

[6] Title VII of Civil Rights Act of 1964, Age Discrimination in Employment Act of 1967, and Title I of the Americans with Disabilities Act of 1990.

611 minorities (52.5 percent). Tables 1 and 2 below provide more detail between the makeup of GPO's total workforce and between the total white collar workforce and the SLS corps.

Table. 1. FY 2008 Total Workforce (as of January 28, 2008)

Employees	Workforce	
Males	**Number**	**Percent**
White	610	27.0
African American	639	28.2
Asian American/Pacific Islander	26	1.1
Hispanic American	26	1.1
Native American	6	0.3
Total Males	**1,307**	**57.7**
Females		
White	294	13.0
African American	622	27.5
Asian American/Pacific Islander	24	1.1
Hispanic American	12	0.5
Native American	4	0.2
Total Females	**956**	**42.3**
Overall Totals	**2,263**	**100.0**

Table 2. FY 2008 White Collar Workforce Contrasted with SLS Employees (as of January 28, 2008)

Employees	Workforce		SLS	
Males	**Number**	**Percent**	**Number**	**Percent**
White	315	27.1	22	84.6
African American	165	14.2	0	0.0
Asian American/Pacific Islander	19	1.6	0	0.0
Hispanic American	17	1.4	1	3.9
Native American	2	0.2	0	0.0
Total Males	**518**	**44.5**	**23**	**88.5**
Females				
White	237	20.4	1	3.8
African American	372	32.0	2	7.7
Asian American/Pacific Islander	20	1.7	0	0.0
Hispanic American	12	1.0	0	0.0
Native American	4	0.4	0	0.0
Total Females	**645**	**55.5**	**3**	**11.5**
Overall Totals	**1,163**	**100.0**	**26**	**100.0**

The EEO Director is responsible for ensuring that equal opportunities exist for employees and applicants without regard to race, sex, color, religion, national origin, sexual orientation, age, and physical and mental disability. The EEO Office consists of two divisions: (1) the Affirmative Employment Program (AEP) Division; and (2) the Counseling and Complaints Processing Division (CCPD). For FY 2007, the GPO EEO Office had a budget of $888,500 and a staff of seven employees.[7]

AEP Division

The AEP Manager assures that equal opportunity principles are an integral part of every aspect of personnel policy and practice in the recruitment, employment, development, advancement, and treatment of GPO staff and applicants for employment. In addition, the AEP Manager also manages special emphasis programs that implement Presidential Executive Orders and Federal personnel programs for eliminating demographic group imbalances in targeted occupations, and achieving diversity in the workforce.

The AEP manager oversees three special emphasis programs assigned to GPO managers who work the programs as a collateral duty. Collateral duty managers can spend up to 25 percent of their time managing the following special emphasis programs.

- ***Disability Program***

The Disability Program at GPO consists of a program manager and ten employees who voluntarily serve on the Disability Program Committee. The mission of the committee is to raise awareness of disability policies and programs through information dissemination and education programs and help elevate disability concerns to the EEO Office. The program committee works with the EEO Office to identify employment barriers to individuals with disabilities, review Agency policies addressing employment issues, and recommend changes.

- ***Federal Women's Program***

The Federal Women's Program (FWP) at GPO has the involvement of the EEO Director, the AEP Manager, and an FWP Manager, who performs the job as a collateral duty. The FWP committee also has 34 members. The FWP committee's mission is to continually identify, promote, and enhance employment and training opportunities for women. The committee also helps keep women at GPO apprised of employment issues; assists women in training, career development, and advancement; provides networking channels with other FWP organizations on issues related to eliminating barriers to equal access and opportunity; and promotes professionalism that furthers the progress of women.

[7] GPO's budget for FY 2007 was $848.225 million.

- ***Hispanic Employment Program***

The GPO Hispanic Employment Program's (HEP) mission is to eliminate discriminatory practices, assist in eliminating areas of under-representation or underutilization, evaluate practices for disparate impact or treatment, and recommend changes to eliminate barriers to Hispanic employment. The HEP manager serves in the position as a collateral duty and also serves as the Secretary to the National Council of HEP Managers, a body consisting of members from 40 different federal agencies appointed as their agency's designee responsible for building relationships between federal agencies and the Hispanic community. The HEP manager also is responsible for e-mailing GPO job vacancies to not only 67 Hispanic organizations, but also to more than 800 individuals who belong to the Washington DC-Hispanic Employment Network.

- ***Other Programs***

The AEP Manager also manages the pilot Employee Mentoring Program and the Passport-to-Work Summer Youth Program, and also co-manages the Coming Home to Work Program. The GPO Employee Mentoring Program (GEM) began as a pilot program in April 2008 and is designed to enhance employee retention, job satisfaction, and cross-organizational communication through employees receiving guidance, counseling, and coaching from designated GPO mentors. In another program, the Department of Veterans Affairs works with GPO and sponsors the Coming Home to Work Program that helps provide suitable employment opportunities for eligible members of the armed services. The Passport-to-Work Summer Youth Program offers District of Columbia youths, ages 14 to 21, a 10-week temporary summer job at GPO—funded by the District of Columbia Youth Employment Office. GPO has participated in this program for several years, and placed an average of 52 students from this program during the last 6 years, with 48 placed in 2008.

CCPD Division

The Assistant Director/Chief of CCPD manages the EEO complaint process for GPO employees and applicants for employment involving issues of discrimination on the basis of race, sex, color, religion, national origin, sexual orientation, age, disability, and reprisal for prior participation in the EEO complaints process. Along with three EEO specialists, the Chief of CCPD issues policy and guidelines related to discrimination complaint procedures, monitors complaints of discrimination to detect indications of discriminatory patterns and practices, and prepares final Agency decisions on complaints. The CCPD also collects, maintains, and analyzes data on the discrimination complaint process and serves as the official source of information for the status of complaints at GPO. CCPD also oversees recruiting, selecting, and maintaining a cadre of trained EEO specialists.

Leadership, Development, and Recruitment Program

The Agency has also recently started a new leadership program for employees. The Leadership, Development, and Recruitment (LDR) program is a 2-year program, and is staffed with employees recruited from both within and outside the Agency. The LDR program allows employees to work in a number of business units—receiving well-rounded, hands-on experience necessary to prepare them as future GPO leaders.

Findings and Recommendations

Finding A. Incorporating the Essential Elements of EEOC Management Directive-715

Although not mandated, senior officials at GPO have begun to generally follow several of the key elements of the EEOC's MD-715 for creating and maintaining a model EEO program into the structure of the Agency. For example, of the six essential elements outlined in MD-715, GPO has generally incorporated three: (1) demonstrated commitment from agency leadership; (2) efficiency; and (3) responsiveness and legal compliance. The three additional elements that would help establish a model EEO program include: (1) integration of EEO into the agency's strategic mission; (2) management and program accountability; and (3) proactive prevention of unlawful discrimination.

Basic Tenets of Management Directive 715

Effective October 1, 2003, the EEOC issued MD-715. The directive provides the basic elements necessary for creating and maintaining a model EEO program in the Federal government. The directive specifically applies to agencies in the executive branch and Military Departments (except uniformed members), the U.S. Postal Service, the Postal Rate Commission, the Tennessee Valley Authority, the Smithsonian Institution, and those units of the judicial branch of the Federal Government having positions in the competitive service.

When establishing a model EEO program, MD-715 provides that an agency should incorporate into its design a structure for effective management, accountability, and self-analysis that will ensure program success. MD-715 not only contains reporting requirements, but states that six essential elements make up a model EEO program including:

- Demonstrated commitment from agency leadership.
- Integration of EEO into the agency's strategic mission.
- Management and program accountability.
- Proactive prevention of unlawful discrimination.
- Efficiency.
- Responsiveness and legal compliance.

As part of the audit, the OIG assessed the current status of GPO's voluntary efforts to integrate the elements of MD-715 into the structure of the Agency. The results of our assessment are discussed in the following section and are summarized in Appendix B.

Essential Element One – Demonstrated Commitment From Agency Leadership

Element One recommends that the demonstrated commitment from agency leadership start with an effective EEO program policy statement. The criteria states that at the beginning of a tenure and each year thereafter, the head of an agency should issue a signed written policy statement announcing the agency's position against discrimination based on the areas that Federal law covers. GPO has voluntarily adopted this element as the Public Printer issued a policy statement to all GPO employees on April 8, 2008, emphasizing his personal commitment to equal opportunity and diversity. (See Appendix E for the complete text of that statement).[8]

The element further recommends that the head of an agency and other senior management officials demonstrate a commitment to equal employment by incorporating the principles of EEO into an agency's organizational structure and disseminating a policy demonstrating this commitment annually. Publishing such a statement sends a clear message to others in the organization about the seriousness and business relevance of diversity management. Accordingly, we recommend that the Public Printer continue to issue a policy statement addressing his commitment to EEO and diversity on a yearly basis as suggested by MD-715.

Essential Element Two – Integration of EEO into the Agency's Strategic Mission

Element Two provides that the concepts of EEO should be a part of the strategic mission and that an agency's EEO program should be organized and structured in a way that maintains a workplace free from discrimination through its policies, procedures, or practices. Although GPO's current strategic plan entitled *A Strategic Vision for the 21st Century* (December 1, 2004) does not include an EEO message, GPO has followed several of the other concepts of Element Two in that GPO has:

- Maintained a reporting structure that allows the EEO Director the appropriate authority and resources to effectively carry out a successful EEO program.

- Committed sufficient human resources and budget allocations to the EEO program for a successful operation.

- Empowered the EEO Director to have regular and effective ways of informing the Public Printer and senior management officials of the status of EEO programs and being involved in, and consulting on, management and personnel actions.

While management has recognized several aspects of Element Two, management should integrate EEO into the Agency's strategic plan. Accordingly, we recommend that as the new Public Printer formulates his strategic plan, he include EEO and diversity as an integral part of GPO's strategic mission.

[8] The current Public Printer was appointed by the President on November 6, 2007. While the current Public Printer issued a policy statement to employees at the beginning of his tenure as Public Printer, over three years had elapsed since the previous Public Printer issued his statement on February 1, 2005.

Essential Element Three – Management and Program Accountability

To ensure management and program accountability, criteria in Element Three discusses overall accountability and EEO program management. The criteria recommends that the head of an agency should hold managers, supervisors, and EEO officials responsible for effective implementation of an agency's EEO program and plan.

The thrust of management and program accountability is that EEO officials advise and provide assistance to managers about the status of EEO programs within each manager's area of responsibility. In addition, the Directors of EEO and Human Capital should meet regularly and assess whether personnel programs, policies, and procedures conform to EEOC management directives. MD-715 also instructs that the agency explore whether disciplinary actions should be taken when findings of discrimination are made.

In October 2007, EEO officials at GPO began meeting with business unit managers semiannually to discuss EEO issues and concerns within business units, provide information on EEO programs and analysis of workforce data, and obtain input that could assist in developing strategies for improving EEO programs at GPO.

While GPO practices address portions of Element Three's criteria, we recommend that EEO continue to work with business unit managers to develop EEO plans and that EEO and Human Capital officials work together and with business unit managers to identify systemic barriers in hiring, promotions, training, and awards.

Essential Element Four – Proactive Prevention of Unlawful Discrimination

Element Four states that an agency has an obligation to prevent discrimination on the basis of race, color, national origin, religion, sex, age, reprisal and disability, and to eliminate barriers that impede free and open competition in the workplace.[9] Putting such an obligation into place begins with informing employees about an effective anti-discrimination policy that explains the protections afforded by the civil rights laws, the rights afforded in such situations, and the process for redress. Further, the head of an agency must make efforts early to prevent discriminatory actions and eliminate barriers to equal employment opportunity in the workplace.

The criteria recommends that agencies conduct annual self-assessments to monitor progress, identify areas where barriers may operate to exclude certain groups, and develop strategic plans to eliminate identified barriers. In an attempt to benchmark GPO's status, we requested that the EEO officials conduct a self-assessment to help identify gaps and potential areas for development. The results of this assessment are summarized in Table 3.

[9] The Statement of the Public Printer, dated April 8, 2008, is more comprehensive than that recommended by MD-715: "Employment actions must be based upon merit principles and made without regard to an individual's race, color, religion, national origin, sex, age, mental/physical disability or sexual orientation."

Table 3. Types of Information Needed for Accurate Self-Assessment as Prescribed by MD-715

	Workforce Profiles	Provided	Not Provided
1.	Total workforce distribution by race, national origin, and sex for both the permanent and temporary workforce	X[10]	
2.	Permanent and temporary workforce participation rates for each grade level by race, national origin, and sex	X[11]	
3.	Permanent and temporary workforce participation rates for each of the agency's major occupational categories (divided by grade level) by race, national origin, and sex		X[12]
4.	Participation rates in supervisory and management positions by race, national origin, and sex		X[13]
5.	Race, national origin, and sex of applicants for both permanent and temporary employment		X
6.	Rates of selections for promotions, training opportunities and performance incentives, by race, national origin, and sex	X[14]	
7.	Rates of both voluntary and involuntary separations from employment by race, national origin, and sex	X[15]	

Since GPO is not required to follow MD-715, the AEP Manager has not yet implemented annual self-assessments. However, we recommend annual self-assessments so that the AEP Manager can more effectively monitor progress, identify areas where barriers exclude certain groups, and develop strategic plans to help eliminate barriers. Additionally, in the absence of a formal requirement for self-assessments, the data necessary to complete these assessments is not readily available from Information Technology and Systems (IT&S) in the desired format. Under the circumstances, the AEP Manager must now manually reformat data from Human Capital and arrange it in a format suitable for agency needs or congressional hearings. A request for software that would assist the efforts of the AEP Manager, is pending. Since more complete and accurate data would help the AEP Manager monitor progress and identify areas where barriers are possibly excluding certain groups, we recommend further action in order to meet the requirements of Element Four.

[10] Provided only permanent workforce for FY 2006 and 2007; did not provide temporary workforce.
[11] Provided only permanent workforce for FY 2006 and 2007; did not provide temporary workforce.
[12] Provided occupation by organization for FY 2007 and organization profile by occupation series for full-time, part-time, and other for FY 2006 and 2007.
[13] Provided organizational profile by supervisor and manager for full-time, part-time, and other for FY 2006 and 2007.
[14] Provided promotions for FY 2006 and 2007; Human Capital was not asked by EEO to provide profiles for training opportunities and performance incentives.
[15] Provided separations for FY 2006 and 2007; report did not distinguish between voluntary and involuntary for both years.

Essential Element Five – Efficiency

Element Five requires that the agency head ensure that there are effective systems in place for evaluating the impact and effectiveness of the agency's EEO programs as well as an efficient and fair dispute resolution process. Critical to this element are adequate and accurate information collection systems. Such systems fully integrated into an agency's infrastructure help it conduct periodic reviews—thus allowing the agency to stay on top of those items affecting the myriad of EEO areas.

Element Five identifies six areas for the agency to comply with EEOC's instructions including: (1) sufficient staffing, funding, and authority to achieve the elimination of identified barriers; (2) an effective complaint tracking and monitoring system in place to increase the effectiveness of the agency's EEO programs; (3) sufficient staffing, funding and authority to comply with the time frames in accordance with EEOC regulations for processing EEO complaints of employment discrimination; (4) an efficient and fair dispute resolution process and effective systems for evaluating the impact and effectiveness of the agency's EEO complaint processing program; (5) effective systems in place for maintaining and evaluating the impact and effectiveness of its EEO programs; and (6) ensuring that the investigation and adjudication function of its complaint resolution process are separate from its legal defense arm of the agency or other offices with conflicting or competing interests.

GPO is achieving many of the objectives of Essential Element Five. However, further progress can be made to develop methods to identify and eliminate barriers and implement specific strategies for evaluating the impact and effectiveness of EEO programs.

Additionally, EEO officials have experienced difficulty consolidating the information obtained from Human Capital due to the variances in data formats available for tracking the information required to achieve the elimination of identified barriers. Accordingly, we recommend that GPO management identify a solution to ensure the ability to obtain accurate data for use in identifying and eliminating barriers and to help evaluate the impact and effectiveness of its EEO programs.

Illustrative of this point is the absence of recruitment effort tracking and analysis. For example, between September 2007 and February 2008, the EEO Director visited universities in California, New Mexico, and Texas to recruit Hispanic Americans for GPO's 2008 Leadership Program and other job vacancies. In addition, Human Capital officials made similar visits to universities to recruit for the Leadership Program. Despite these efforts, Human Capital did not track these recruitment efforts or have a written plan for attracting a supply of qualified, diverse applicants for GPO employment. Since the EEO Director and Human Capital officials are not the hiring officials for GPO's individual business units, consideration should be given to having business unit managers participate in future recruiting efforts.

Although GPO was generally following most of the six subcategories, we recommend that management emphasize these additional areas, to help ensure that effective systems are in place for evaluating the impact and effectiveness of the EEO programs.

Essential Element Six – Responsiveness and Legal Compliance

Element Six contains a requirement that each year an agency certify that it is complying with EEO laws and EEOC regulations, policy guidance, and other written instructions. Element Six also identifies that agency personnel should be accountable for the timely compliance with EEOC orders. While the EEO staff are formally trained and responsible for compliance with EEO laws and EEOC regulations and orders, these requirements are not fully incorporated into the performance standards of GPO employees. The EEO Office has a system called EEO Network (EEONET) which ensures that any EEO cases over 30-days old are identified. This system is backed up by a manual calendar system which ensures that GPO officials comply in a timely manner with any orders or directives issued by EEOC Administrative Judges.

Although generally following the requirements of Element Six, management can send a positive and clear message to all GPO employees about maintaining a workplace free of discrimination and harassment as well as a commitment to EEO and diversity by requiring compliance with EEO laws and EEOC regulations in the performance standards of all managers and SLS personnel.

While GPO is voluntarily complying with several of the essential elements identified by the EEOC, the opportunity exists through fully incorporating the six elements to create and maintain a model EEO program at GPO. Creation of a model program will help further ensure that the agency is not only free from employment discrimination, but also has a diverse workforce.

Recommendation

1. The Public Printer should incorporate the six essential elements of Equal Employment Opportunity Commission Management Directive 715 by taking the following actions:

a. Continue to issue and disseminate to GPO employees an annual signed written policy statement expressing Agency commitment to equal employment opportunity as well as maintaining a workplace free of discriminatory harassment and practices.

b. Integrate equal employment opportunity policy and practices into future agency strategic plans.

c. Require, with assistance from EEO officials, that business unit managers develop an EEO plan for their individual units and that EEO and Human Capital officials meet regularly to identify any systemic barriers in hiring, promotions, training, and awards.

d. Conduct annual self-assessments that monitor progress, identify areas where barriers may exclude certain groups, and develop strategic recruitment plans to eliminate those barriers to the extent possible and to attract a qualified, diverse pool of applicants.

e. Maintain and provide sufficient resources—including staffing, funding, and authority—for EEO officials to track workforce profiles that will help eliminate identified barriers and recruitment efforts that will assist officials with identifying potential barriers. The resources provided should also include the information technology infrastructure (hardware, software, etc.) necessary to allow EEO officials to effectively produce workforce diversity statistics.

f. Incorporate compliance with EEO laws and EEOC regulations in performance standards for all managers including SLS personnel.

Management's Response. Concur. Implementation of the recommendation will require the Public Printer's review and approval (see Appendix J).

Evaluation of Management's Response. While GPO management concurred with the recommendation, they did not provide details regarding what actions the Agency plans to take to implement the recommendation. As a result, pending receipt of details related to implementation, the recommendation is considered unresolved. The OIG will work with GPO management to review any proposed actions to implement the recommendation.

Finding B. Incorporating GAO's Leading Diversity Management Practices

To date, GPO officials have partially adopted the nine practices identified by the GAO as the most common leading diversity management practices. Specifically, the Agency has partially adopted one of the GAO leading practices and is actively working on developing a plan for another of the practices--succession planning. GPO had not made decisions regarding adoption of the remaining practices at the time of the audit. Similar to the key elements of EEOC MD-715 for creating and maintaining a model EEO program, adoption of the nine practices identified by the GAO would help further ensure that the agency has a diverse workforce and an effective EEO program.

The GAO Leading Practices

In January 2005, GAO issued a report to the Ranking Minority Member, Committee on Homeland Security and Government Affairs, U.S. Senate entitled "Diversity Management: Expert-Identified Leading Practices and Agency Examples."[16] This report identified nine leading practices to be considered when an organization is developing and implementing a diversity management program. These nine practices were developed by GAO after speaking with experts in the field of diversity management and reviewing their publications. The practices that GAO identified include:

- **Top leadership commitment**—a vision of diversity demonstrated and communicated throughout an organization by top-level management;

- **Diversity as part of an organization's strategic plan**—a diversity strategy and plan that are developed and aligned with the organization's strategic plan;

- **Diversity linked to performance**—the understanding that a more diverse and inclusive work environment can yield greater productivity and help improve individual and organizational performance;

- **Measurement**—a set of quantitative and qualitative measures of the impact of various aspects of an overall diversity program;

- **Accountability**—the means to ensure that leaders are responsible for diversity by linking their performance assessment and compensation to the progress of diversity initiatives;

- **Succession planning**—an ongoing, strategic process for identifying and developing a diverse pool of talent for an organization's potential future leaders;

- **Recruitment**—the process of attracting a supply of qualified, diverse applicants for employment;

[16] GAO 05-90, January 14, 2005, available at http://www.gao.gov/newitems/d0590.pdf

- **Employee involvement**—the contribution of employees in driving diversity throughout an organization; and

- **Diversity training**—organizational efforts to inform and educate management and staff about diversity.

We reviewed GPO's diversity programs to benchmark the Agency's standing in relation to GAO's nine leading diversity management practices. The results of our review are discussed in the following section and are summarized in Appendix D.

1. Top Leadership Commitment

A commitment of top leadership is the first leading practice that GAO identifies in its January 2005 report. That practice requires that the head of an agency and other senior officials commit themselves to diversity by incorporating the principles of EEO into an agency's organizational structure. The Public Printer issued a policy statement to all GPO employees on April 8, 2008, emphasizing his personal commitment to equal opportunity and diversity. (See Appendix E for the complete text of that statement). While the current Public Printer issued a signed policy statement to employees at the beginning of his tenure as Public Printer, over three years had elapsed since the previous Public Printer issued his statement on February 1, 2005. As previously recommended, the Public Printer should follow MD-715 guidance and continue to issue a signed policy statement annually to all employees addressing his commitment to diversity and EEO. This ongoing demonstration of commitment from the Public Printer is critical to the success of GPO's diversity and EEO programs.

2. Diversity as Part of an Organization's Strategic Plan

An emphasis on diversity as part of an organization's strategic plan is the second leading practice that GAO identifies in its January 2005 report. Such a practice requires an emphasis on integrating diversity management into an organization's strategic plan because it fosters a culture change that supports and values differences. Since it typically takes five to seven years to complete the initiatives of an agency's strategic plan, sustaining top leadership commitment to improvement is particularly challenging since the turnover rate for political appointees is just less than three years.[17] The Public Printer should link diversity to any future update of the Agency's Strategic Plan to ensure that EEO and diversity are considered an integral part of the agency's strategic mission.

3. Diversity Linked to Performance

The contribution that diversity plays in achieving improved individual and organizational performance is the next leading practice that GAO identifies in its January 2005 report. Diversity management makes good business sense, enhancing productivity and

[17] GAO, *High –Risk Series: Strategic Human Capital* Management, GAO-03-120 (Washington, D.C. January 2003) reported that governmentwide the average tenure of political appointees for 1990 through 2001 was just under three years.

innovation. In addition, diversity management can help reduce costs by reducing turnover, increasing employee retention across demographic groups, and improving morale. GPO should include the development of diversity management as part of its strategic plan.

4. Measurement

Quantitative and qualitative measures are vital tools in helping an agency evaluate the effectiveness of its diversity management in terms of return on investment, recruitment efforts, and retention. These tools can also help an agency compute the return on their investments in areas such as diversity training and recruiting. As previously noted, EEO officials have not been able to easily obtain workforce data to aid in such measurements. Further, the absence of written plans for attracting a supply of qualified, diverse applicants for employment, makes it difficult to measure success.

Since GPO has not implemented methods to measure or evaluate the effectiveness of the organization's diversity management, it was not possible to evaluate the return on investment for training or retraining. This type of measurement is important because it provides an agency an idea of where barriers might be that are hindering success with diversity-related goals. Although EEO officials informed us that GPO will adopt this GAO leading practice, it is our opinion that this decision should be made by the GPO Chief Human Capital Officer, who is responsible for workforce data and recruitment.

5. Accountability

Ensuring that managers maintain diversity, evaluate progress, and can manage diverse groups is the next leading practice that GAO identifies. Accountability is defined by GAO as the means to ensure that leaders are responsible for diversity by linking their performance assessment and compensation to the progress of diversity initiatives. To accomplish accountability, organizations should link ratings and compensation. The Government's Senior Executive Service corps is already held to that type of accountability—consistent with section 4313 of Title 5, which provides performance appraisal criteria for achieving EEO requirements. This accountability is also consistent with the EEOC's instructions to Federal agencies implementing MD-715.[18]

At GPO, managers and supervisors are held to core EEO commitments in order to obtain performance bonuses. As a point of interest, FY 2007 performance agreements for supervisors and the SLS corps contained a statement about EEO issues, whereas, in the FY 2008 agreements, that statement was changed. For the differences in the two agreements, see the portion below highlighted in *italics*.

[18] The instructions describe the requirement that agencies inform managers and supervisors that success and a positive evaluation will include an assessment of how that manager contributes to the agency's EEO program by emphasizing to managers and supervisors that equality of opportunity is essential to attracting, developing, and retaining the most qualified workforce, with such a workforce being essential to ensuring the agency's achievement of its strategic mission.

FY 2008 Performance Agreement

I will make decisions in areas such as hiring, training, awards, special projects and developmental assignments without regard to sex, race, color, religion, national origin, age, disability, sexual orientation, or reprisal. I will conduct myself in accordance with all applicable legal and ethical standards of behavior and will assist on and enforce these standards within my organization. In the event that the above core commitment is not being met, the supervisor's rater must immediately provide guidance and advice to address any performance-related problems.

FY 2007 Performance Agreement

I will make decisions in areas such as hiring, training, awards, special projects and developmental assignments without regard to sex, race, color, religion, national origin, age, disability, sexual orientation, or reprisal *in order to nurture talent, create diverse opportunities and maximize the potential of GPO's workforce. I will promote staff participation in EEO events and programs. I will work with EEO to address and resolve allegations of discrimination and/or harassment within my organization.*

EEO officials stated that no decision had been made to adopt this practice although Human Capital officials stated that the draft EEO core commitment for FY 2009 performance agreements would be similar to the previous FY 2007 core commitment. We recommend that the agency adopt core commitments that emphasize the value of creating a diverse workforce and address the culture of diversity as opposed to mere compliance with laws and regulations.

6. Succession Planning

Succession planning is the sixth leading practice that GAO identifies in its January 2005 report. Succession planning is tied to the Federal Government's opportunity to change the diversity of the executive corps through new appointments and is a comprehensive, ongoing strategic process that enables management to forecast an organization's leadership needs. Identifying and developing candidates who have the potential to be future leaders, and selecting individuals from among a diverse pool of qualified candidates to meet executive resource needs is at the heart of succession planning.

As Table 4 shows, in the last five years GPO has made significant progress in the overall diversity of its workforce. Specifically, in FY 2002, there were 32 Grade 15s consisting of 31 males (6 minorities) and one female (0 minorities). In FY 2007, there were 56 males (14 minorities) and 23 females (11 minorities).

Table 4. 5-Year Trend Grade 15 (PG-15) Employees

Fiscal Year	**2002**		**2007**	
Males	**Number**	**Percent**	**Number**	**Percent**
White	25	78.2	42	53.1
African American	5	15.6	11	13.9
Asian American/Pacific Islander	1	3.1	1	1.3
Hispanic American	0	0.0	1	1.3
Native American	0	0.0	1	1.3
Total Males	**31**	**96.9**	**56**	**70.9**
Females				
White	1	3.1	12	15.2
African American	0	0.0	6	7.6
Asian American/Pacific Islander	0	0.0	5	6.3
Hispanic American	0	0.0	0	0.0
Native American	0	0.0	0	0.0
Total Females	**1**	**3.1**	**23**	**29.1**
Overall Totals	**32**	**100.0**	**79**	**100.0**

The result of the progress GPO has made in their succession planning has affected the makeup of its SLS employees. As shown in Table 5 below, in FY 2002, there were 21 SLS employees consisting of 20 males (0 minorities) and one female (1 minority). In FY 2007, there were a total of 26 SLS employees consisting of 23 males (1 minority) and 3 females (2 minorities).

Table 5. 5-Year Trend Senior Level Service (SLS) Employees

Fiscal Year	**2002**		**2007**	
Males	**Number**	**Percent**	**Number**	**Percent**
White	20	95.2	22	84.6
African American	0	0.0	0	0.0
Asian American/Pacific Islander	0	0.0	0	0.0
Hispanic American	0	0.0	1	3.9
Native American	0	0.0	0	0.0
Total Males	**20**	**95.2**	**23**	**88.5**
Females				
White	0	0.0	1	3.8
African American	1	4.8	2	7.7
Asian American/Pacific Islander	0	0.0	0	0.0
Hispanic American	0	0.0	0	0.0
Native American	0	0.0	0	0.0
Total Females	**1**	**4.8**	**3**	**11.5**
Overall Totals	**21**	**100.0**	**26**	**100.0**

Another way GPO supports succession planning is through leadership programs. A new program at GPO is called the Leadership, Development, and Recruitment (LDR) program. The LDR program—a two-year career-building program—began in FY 2007. As part of the LDR program, employees are recruited from both inside and outside the Agency. The program allows employees to work in a number of business units to get a range of hands-on experience of GPO to become potential future leaders within those same business units. In FY 2007, there were 13 employees—8 males (4 minorities) and 5 females (3 minorities)—enrolled in the LDR program. The second LDR class began in June 2008 with seven employees—five males and two females (1 minority). Table 6 provides more detail on the makeup of these two classes.

Table 6. Leadership Development and Recruitment (LDR) Program Employees

Fiscal Year	**2007**		**2008**	
Males	**Number**	**Percent**	**Number**	**Percent**
White	4	30.8	5	71.4
African American	3	23.0	0	0.0
Asian American/Pacific Islander	0	0.0	0	0.0
Hispanic American	1	7.7	0	0.0
Native American	0	0.0	0	0.0
Total Males	**8**	**61.5**	**5**	**71.4**
Females				
White	2	15.4	1	14.3
African American	3	23.1	1	14.3
Asian American/Pacific Islander	0	0.0	0	0.0
Hispanic American	0	0.0	0	0.0
Native American	0	0.0	0	0.0
Total Females	**5**	**38.5**	**2**	**28.6**
Overall Totals	**13**	**100.0**	**7**	**100.0**

Although GPO can still improve the diversity of its SLS corps with the inclusion of Asian American/Pacific Islanders, Hispanic Americans, and Native Americans, in the last five years, GPO has worked to create a diverse pool of qualified candidates for future SLS positions at both the Grade 15 level and through implementation of the LDR program.

7. Recruitment

Attracting a supply of qualified, diverse applicants for employment is the next leading practice listed by GAO. GAO states that organizations can widen selection of schools from which they can recruit to include, for example, Historically Black Colleges and Universities, Hispanic-Serving Institutions, women's colleges, and schools with international programs. Because of the number of Federal employees, including those in

senior level positions eligible for retirement in the next decade, the Federal Government will need more midcareer employees, defined by the GAO as employees generally 40 and older with 10 or more years of work experience.

In 2006, GPO hired a Recruitment Manager who worked with GPO managers including EEO and established a plan to recruit diverse candidates for a number of positions including the LDR Program. The Recruitment Manager along with other recruiters visited Historically Black Colleges and Universities and Hispanic-Serving Institutions. In addition, the manager used his personal contacts to generate renewed interest in GPO. A similar plan created in coordination with the EEO Manager is in place for 2008/2009. Also, the Hispanic Employment Program Manager e-mails job vacancies to 67 Hispanic organizations and to more than 800 Hispanic Employment Network individuals. Finally, significant recruitment planning, efforts and advertising took place in order to find diverse candidates to fill the positions at GPO's Secure Production Facility (SPF) in Mississippi. However, such efforts by Human Capital and EEO may not be fully realized in the absence of participation by the business unit managers making the employment selections. Accordingly, we recommend that the business unit managers responsible for employment selection and recruiting be included in outreach and recruitment efforts.

8. Employee Involvement

Employee involvement is GAO's eighth practice. Involving employees in diversity management helps contribute to diversity throughout the organization. Employees can get involved by: (1) forming employee diversity task forces, councils, boards, and networks to identify issues, recommend actions, and help develop initiatives to facilitate change; (2) providing mentoring opportunities to help identify and develop high-potential employees, improve employee productivity and performance, and promote retention and diversity; and (3) encouraging employees to volunteer in their communities and allocating mission personnel to participate in community outreach programs with private employers, public schools, and universities.

In its report, GAO provides an example of an agency that established a diversity advisory board and provided a visible forum for independent advice and assistance to management officials on diversity-related plans, policies, and programs. The same agency also created an advisory council chaired by a senior manager. The two groups contributed to the diversity strategic plan which was adopted by agency management. The diversity strategic plan had the following four objectives:

- Increased awareness of diversity values and sensitivities by senior management, managers, and staff.

- Retention of existing diversity and work-life enhancement.

- Active promotion of outreach and creation of a visible network of connections or routes to the agency.

- Recruitment and workforce planning for enhanced diversity.

GPO has several diverse employee groups such as the Federal Women's Program, Hispanic Employment Program, and the Disability Committee. These groups help identify issues and recommend actions to GPO management. These groups could also aid GPO management in the development of initiatives and recommendations for a diversity strategic plan similar to that identified in the GAO report.

In another effort to enhance employee involvement, the AEP Manager introduced GPO's Employee Mentoring Program in April 2008. The program is a formal six-month pilot with 11 mentors and protégés and is designed to enhance employee retention, job satisfaction, and cross-organizational communication through employees receiving teaching, guidance, counseling, and coaching from other GPO employees.

GPO also has very active employee involvement. As the GAO report emphasizes, employees should be empowered to address and identify diversity issues, recommend actions, and help develop initiatives to address concerns and create greater cultural and diversity awareness in the workplace for all employees. We recommend that GPO management evaluate its existing employee groups, identify whether employees' issues are fully represented and ensure that the groups are meeting the objectives as identified by GAO.

9. Diversity Training

GAO's ninth practice of training can help an organization's management and staff increase their awareness and understanding of diversity as well as help it develop concrete skills for assisting it with communicating and increasing productivity. Training can provide employees with an awareness of their differences—including cultural, work style, and personal presentation-and an understanding of how diverse perspectives can improve organizational performance. GAO also states that to increase employee effectiveness in a diverse environment, training should include teambuilding, communication styles, decision-making, and conflict resolution.

EEO officials informed us that GPO plans to adopt this leading practice. The OIG believes that officials from both EEO and Human Capital should work together to develop a diversity training curriculum that can be provided to all GPO employees.

Recommendation

2. The Public Printer should adopt all or a combination of the leading practices GAO recommends to create and maintain a positive work environment with qualified and diverse senior officials by taking the following steps:

    a. Continue to issue to all employees an annual policy statement on his personal commitment to equal opportunity and diversity.

b. Link diversity to GPO's strategic plan.
c. Include the development of diversity management in its strategic plan.

d. Develop a data gathering and tracking system for workforce data that will help the agency eliminate identified barriers.

e. Develop a written plan for attracting a supply of qualified, diverse applicants for employment, identifying quantitative and qualitative performance measures that can track data on its workforce to evaluate the effectiveness of the Agency's diversity management efforts as well as track the return on investment in such areas as diversity training and recruitment.

f. Ensure that managers are responsible for diversity in their business units and that awards are based partly on a manager's success in achieving diversity-related goals.

g. Identify, develop, and select candidates for new appointments who have the potential to be future leaders from a diverse pool of qualified candidates.

h. Empower employees to get involved in diversity management by forming employee task forces, councils, and boards that identify issues and recommend actions to the diversity strategic plan.

i. Develop a diversity training program for managers and employees that increases awareness and understanding of diversity as well as help develop concrete skills to assist in communicating and increasing productivity.

Management's Response. Concur. Implementation of the recommendation will require the Public Printer's review and approval (see Appendix J).

Evaluation of Management's Response. While GPO management concurred with the recommendation, they did not provide details regarding what actions the Agency plans to take to implement the recommendation. As a result, pending receipt of details related to implementation, the recommendation is considered unresolved. The OIG will work with GPO management to review any proposed actions to implement the recommendation.

Appendix A. Objectives, Scope, and Methodology

Objectives

The overall objective of the audit was to conduct a review of the diversity office within the GPO at the request of the Subcommittee on Federal Workforce, Postal Service, and the District of Columbia, Committee on Oversight and Government Reform, House of Representatives. The Subcommittee expressed concern about the under representation of women and minorities in the senior-level positions at the legislative branch agencies. The GPO OIG was one of five legislative branch agencies jointly conducting this review. The other legislative branch agencies participating in the review are the Library of Congress, Government Accountability Office, Architect of the Capitol, and U.S. Capitol Police. Participating agencies will issue a consolidated report to Congress by September 2008.

The specific audit objectives were to:

- Identify and assess the diversity program at GPO to determine if it is yielding the desired results, that of creating a more diverse population of women and minorities in top leadership positions (SLS).

- Evaluate the accuracy and completeness of the complaints and discrimination data being reported to the Congress.

- Assess to what degree the diversity offices are independent of the GPO's General Counsel and the Public Printer

Scope and Methodology

To be consistent in our scope and methodology in reporting each particular agency's position to the three specific objectives, we followed a uniform audit guide provided to each participating OIG by the Library of Congress OIG. To address the audit objectives, we:

1. Assessed the responses that the EEO Director provided in the: (1) Self-Assessment Checklist in MD-715 which identifies the effectiveness of the GPO diversity programs; and (2) Data Collection Instrument for Leading Diversity Management Practices which gauges the agency's progress in following leading diversity management practices as of January 1, 2008.

2. Evaluated the accuracy and completeness of GPO's complaint and discrimination data for Fiscal Year 2007.

3. Assessed the current independence of GPO's EEO Director and the diversity programs with the Public Printer and GPO's General Counsel.

We also interviewed officials from the Offices of the General Counsel and Human Capital to determine whether policies and procedures related to EEO were implemented and followed. Human Capital officials also provided workforce profile reports and documentation on recruiting applicants for Agency leadership programs.

Management Controls Reviewed

We reviewed management controls related to EEO areas, including complaint and discrimination reports as well as the reporting of data for workforce profile reports to ensure these practices are contained in GPO Instruction 825.18A.

Audit Field Work

We performed field work from April through August 2008 at the GPO Central Office in Washington, D.C. We performed the audit in accordance with generally accepted government auditing standards.

Appendix B. Assessment of Whether GPO Practiced the Essential Elements of EEOC Management Directive 715

	Essential Element	Generally Following	Not Following
1.	Demonstrated Commitment from Leadership	X	
2.	Integration of EEO into the Strategic Mission		X[19]
3.	Management and Program Accountability		X[20]
4.	Proactive Prevention		X[21]
5.	Efficiency	X	
6.	Responsiveness and Legal Compliance	X	

[19] Although GPO followed the four parts of Element B, the previous strategic plan did not address EEO.
[20] Although GPO followed portions of Element C, it did not include the portions for business unit managers developing EEO plans and EEO and Human Capital officials identifying any systemic barriers in past promotions, training, and awards.
[21] Because the data that Human Capital official provided was limited, the AEP Program Manager could not conduct an annual self-assessment to monitor the progress and identify areas where barriers may operate to exclude certain groups.

Appendix C. White and Blue Collar Workforce Profile by Grade, Race, and Sex (As of January 28, 2008)

Grade	Total Employees			White		Black		Hispanic		Asian / Pacific Islander		American Indian	
WHITE COLLAR WORKFORCE													
	All	Men	Women	Men	Women	Men	Women	Men	Women	Men	Women	Men	Women
SLS	26	23	3	22	1		2	1					
15	79	56	23	42	12	11	6	1		1	5	1	
14	95	60	35	46	24	8	10	3	1	3			
13	207	108	99	69	54	28	39	2	1	8	4	1	1
12	303	128	175	79	72	45	91		2	4	8		2
11	80	28	52	17	12	9	38	2	1		1		
10	4	1	3				3	1					
9	77	20	57	10	13	9	43			1			1
8	15	1	14		2	1	12						
7	95	15	80	8	19	6	56	1	3		2		
6	60	12	48	2	7	8	40	1	1	1			
5	91	49	42	13	10	31	29	5	3				
4	13	4	9	2	6	2	3						
3	8	6	2	2	2	4							
2	4	3	1	1	1	2							
0	6	4	2	2	2	1				1			
Subtotal	**1163**	**518**	**645**	**315**	**237**	**165**	**372**	**17**	**12**	**19**	**20**	**2**	**4**
BLUE COLLAR WORKFORCE													
Subtotal	**1100**	**789**	**311**	**296**	**57**	**473**	**250**	**9**		**7**	**4**	**4**	
GPO #	**2263**	**1307**	**956**	**611**	**294**	**638**	**622**	**26**	**12**	**26**	**24**	**6**	**4**

Source: GPO Office of Human Capital

Appendix D. Assessment of Whether GPO Exemplifies GAO's Leading Practices for Diversity Management

	Leading Diversity Practices[22]	Not Yet Adopted					Level of Adoption	
		Do not anticipate adopting	No decision	Will adopt	Plan under development	Written plan complete	Partially adopted	Fully adopted
1.	**Top leadership commitment –** a vision of diversity demonstrated and communicated throughout an organization by top-level.						X[23]	
2.	**Diversity as part of an organization's strategic plan –** a diversity strategy and plan that are developed and aligned with the organization's strategic plan.		X					
3.	**Diversity linked to performance –** the understanding that a more diverse and inclusive work environment can yield greater productivity and help improve individual and organizational performance.		X					
4.	**Measurement –** a set of quantitative and qualitative measures of the impact of various aspects of an overall diversity program.		X					
5.	**Accountability –** the means to ensure that leaders are responsible for diversity by linking their performance assessment and compensation to the progress of diversity initiatives.		X					
6.	**Succession planning –** an ongoing, strategic process for identifying and developing a diverse pool of talent for an organization's potential future leaders.				X[24]			
7.	**Recruitment –** the process of attracting a supply of qualified, diverse applicants for employment.		X					
8.	**Employee involvement –** the contribution of employees in driving diversity throughout an organization.		X					
9.	**Diversity training –** organizational efforts to inform and educate management and staff about diversity.		X					

[22] GAO report GAO-05-09, "Diversity Management Expert-Identified Leading Practices and Agency Examples," January 2005.

[23] Based on the Public Printer's April 8, 2008, letter on equal opportunity and diversity.

[24] The Human Capital Office did not have a written plan. However, GPO has made progress in the last five years to create a diverse pool of qualified candidates at the Grade 15 level and the implementation of the LDR program.

Appendix E. Public Printer's April 8, 2008 Letter on Equal Opportunity and Diversity

GPO U.S. GOVERNMENT PRINTING OFFICE
KEEPING AMERICA INFORMED

Robert C. Tapella
Public Printer

April 8, 2008

To All GPO Employees:

As Public Printer I want to emphasize my personal commitment to equal opportunity and diversity. It is imperative that we treat fairly all employees, applicants for employment, and customers of the U.S. Government Printing Office (GPO). Employment actions must be based upon merit principles and made without regard to an individual's race, color, religion, national origin, sex, age, mental/physical disability or sexual orientation.

Since becoming Public Printer at GPO, I have made it clear that I will not tolerate any form of discrimination in the workplace. I firmly believe that every GPO employee is entitled to work in an environment that is free of discrimination and harassment. I am committed to ensuring that every individual in GPO enjoys that right without regard to non-merit factors. This environment is necessary for accomplishing our goal of attracting, hiring, developing and retaining a quality diverse workforce that achieves our mission and meets the expectations of our citizens and the visitors we serve.

It is the policy of GPO to provide equal employment opportunity for all persons in its workforce, as well as applicants for employment and to prohibit discrimination in all aspects of its personnel policies, program practices and operations. Every GPO manager and supervisor is responsible for ensuring that we achieve that goal. I expect a "zero tolerance" approach to this important area. I take any confirmed violations of this policy very seriously. Employees who violate the law will be held accountable for their conduct. I encourage every level of management to maintain a high level of awareness regarding these matters and to foster a steadfast commitment to equal opportunity for all persons. I expect managers and supervisors to respond to complaints swiftly and appropriately, as they will be held accountable for taking steps to eliminate such behavior and to ensure that the work environment is one where employees are treated fairly, respectfully and with dignity.

As Public Printer, I will vigorously pursue these goals and I encourage all employees to fully support our commitment in principle and in action to ensure that our equal employment opportunity programs are successful. Each of you plays a part in creating and sustaining a workplace that will provide all employees with a working environment free from discrimination where individual differences are respected and valued.

Sincerely,

732 North Capitol Street, NW Washington, DC 20401 202-512-1000 rtapella@gpo.gov

Appendix F. Summary of Leading Practices GPO Followed (From PricewaterhouseCoopers[25] Study and EEOC Management Directive 715[26])

	Diversity Program Characteristics	Following	Generally Following	Not Following
1.	Diversity Program housed separate from the EEO office?			X
2.	Agency has a diversity action or strategic plan?			X
3.	Agency is conducting targeted recruitment and outreach efforts to attract potential under represented minority employees?		X	
4.	Mentoring Program?	X		
5.	Includes awareness events (for example, special emphasis functions)?	X		
6.	Includes a diversity council?			X
7.	Agency encourages the development of formally or informally constituted groups representing specific categories of employees such as women, African Americans, or gays and lesbians?		X	
8.	Includes focus on conflict management (for example, alternative dispute resolution or mediation)?	X		
9.	Diversity training required for managers and supervisors?			X
10.	Diversity training included in employee orientation?			X
11.	Have administered attitude survey as part of assessment?	X		
12.	Diversity element in supervisors/managers performance plans?			X
13.	Are management/personnel policies, procedures and practices examined at regular intervals to assess whether there are hidden impediments to equal opportunity?		X	
14.	Does the EEO Director have the authority and funding to ensure implementation of agency EEO action plans?	X		
15.	The agency tracks the race, national origin and sex of applicants for both permanent and temporary employment?			X
16.	The agency tracks the rates of selections for promotions by race, national origin and sex?			X
17.	The agency tracks the rates of training opportunities (hours per year) by race, national origin and sex?			X
18.	The agency tracks the rates of performance incentives (monetary awards, step increases) by race, national origin and sex?			X
19.	The agency tracks the rates of complaints by race, national origin and sex to see if a particular group has more complaints about promotions, disciplinary actions, performance appraisals, or awards?	X[27]		
20.	The agency tracks the rates of both voluntary and involuntary separations from employment by race, national origin and sex?			X

[25] "A Changing Workforce: Understanding Diversity Programs in the Federal Government" December 2001.
[26] This table will be included in the consolidated report of the five Legislative Branch agencies to Congress.
[27] The EEO Office uses this information in their semiannual meetings with business units that began in October 2007.

Appendix G. Accuracy and Completeness of EEO Data[28]

Tracking and Reporting the Number and Status of Discrimination Complaints

GPO's EEO Office uses EEONET, a case management system built to assist EEO managers and counselors in managing all aspects of information and program management related to EEO complaints and resolutions. Built to support the EEOC reporting requirements, EEONET allows automated generation of reports required by EEOC as well as a variety of other reports and documentation that can be customized to user and management requirements. The data in EEONET are supported by the manual files kept as well as a monthly report that is kept to ensure the data is accurate when it is entered into the system. GPO's EEO office is required to submit annually EEOC Form 462 report. EEOC incorporates the data along with the other agencies and report it to Congress. Although the format between "No Fear Act" and EEOC's 462 are somewhat different, the data collected are the same. One key difference is that the "No Fear Act" reporting reflects comparative data for the previous 5 years; EEOC Form 462 report includes activity that occurred during the preceding fiscal year.

No.	Discrimination Complaints	Yes	No
1	Does the agency have a system of management controls in place to ensure the timely, accurate, complete and consistent reporting of EEO complaint data?	X	
2	Does the agency use a complaint tracking system that allows identification of the location and status of complaints, and length of time elapsed at each stage of the agency's complaint resolution process?	X	
3	Does the agency's tracking system identify the issues and bases of the complaints, the aggrieved individuals/complainants, the involved management officials and other information to analyze complaint activity and trends?	X	
4	Is the agency statutorily mandated to follow the No Fear Act reporting requirements?		X
4a	Does the agency follow the No Fear Act reporting format?		X
4b	Does the agency post its No Fear Act (or similar) data on its web site?		X

[28] This table will be included in the consolidated report of the five Legislative Branch agencies to Congress.

Appendix H. Independence of the Diversity Office[29]

Independence

No.		Yes	No
1	Has the agency placed the EEO Director in a direct reporting relationship with the head of the agency?	X	
2	Does the EEO Director have a regular and effective means of informing the agency head and other top management officials of the effectiveness, efficiency and compliance (with agency regulations or EEOC Directives, if applicable) of the agency's EEO program?	X	
3	Is the EEO investigative and decision making process separate from the personnel function?	X	
4	Are the legal sufficiency reviews done by a unit separate from the personnel function?	X	
5	Does the agency offer Alternative Dispute Resolution or mediation?	X	

[29] This table will be included in the consolidated report of the five Legislative Branch agencies to Congress.

Appendix I. Acronyms Used in the Report

AEP	Affirmative Employment Program
CCPD	Counseling and Complaints Processing Division
EEO	Equal Employment Opportunity
EEOC	Equal Employment Opportunity Commission
EEONET	Equal Employment Opportunity Network
FWP	Federal Women's Program
FY	Fiscal Year
GAO	Government Accountability Office
GEM	GPO Employee Mentoring Program
GPO	Government Printing Office
GS	General Schedule
HEP	Hispanic Employment Program
LDR	Leadership, Development, and Recruitment Program
MD	Management Directive
OIG	Office of Inspector General
PG	Printing Office Grade
SES	Senior Executive Service
SLS	Senior Level Service

Appendix J. Management's Response

U.S. GOVERNMENT PRINTING OFFICE
KEEPING AMERICA INFORMED

memorandum

DATE: September 10, 2008

REPLY TO ATTN OF: Director, Equal Employment Opportunity

SUBJECT: Revised Draft Report on Audit of Diversity Management Programs at the GPO

TO: Assistant IG for Audits and Inspection

This is in response to your memorandum dated September 9, 2008, requesting comment on the above subject report. I fully concur with the recommendations outlined in the above subject report. However, it would require the Public Printer's review and approval before implementation.

Please contact me or Juanita M. Flores at (202) 512-2014 if you have any questions.

Juanita M. Flores

NADINE L. ELZY

U.S. GOVERNMENT PRINTING OFFICE
KEEPING AMERICA INFORMED
WASHINGTON, DC 20401

Memorandum

HUMAN CAPITAL OFFICE

DATE: September 10, 2008

REPLY TO
ATTN OF: Chief Human Capital Officer

SUBJECT: Draft Report on Audit of Diversity Management Programs at the GPO

TO: Assistant IG for Audits and Inspection

This is in response to your September 9, 2008 memorandum requesting comments on the revised draft report on the Audit of Diversity Management Program at the GPO. After a thorough review, we note that the changes made as a result of the September 5 meeting between the IG, EEO and Human Capital managers have greatly improved the report.

As far as the two recommendations are concerned, our office concurs with each of them. Thank you for the opportunity to review the draft. I am sure the report will have a positive impact to create a more diverse GPO in the future.

William T. Harris

Appendix K. Status of Recommendations

Recommendation No.	Resolved	Unresolved	Open/ECD*	Closed
1		X		
2		X		

*Estimated Completion Date.

Appendix L. Report Distribution

Government Printing Office

Deputy Public Printer
Chief of Staff
Chief Management Officer
Chief Financial Officer
Chief Information Officer
Chief Technology Officer
Director, Congressional Relations
Director, Library Services and Content Management
Director, Public Relations
Director, Publication and Information Sales
General Counsel
Managing Director, Customer Services
Managing Director, Official Journals of Government
Managing Director, Plant Operations

Major Contributors to the Report

Joseph J. Verch Jr., Supervisory Auditor

United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Federal Workforce, Postal Service, and the District of Columbia, Committee on Oversight and Government Reform, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. EDT
Tuesday, September 16, 2008

DIVERSITY MANAGEMENT

Important Actions Taken and Planned to Further Enhance Diversity

Statement of Ronald A. Stroman, Managing Director
Office of Opportunity and Inclusiveness

DIVERSITY MANAGEMENT

Important Actions Taken and Planned to Further Enhance Diversity

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-08-1160T, a testimony before the Subcommittee on Federal Workforce, Postal Service, and the District of Columbia, Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

For GAO, having a diverse workforce at all levels is an organizational strength that contributes to the achievement of results by bringing a wider variety of perspectives and approaches to policy development and implementation, strategic planning, problem solving and decision making. GAO's Office of Opportunity and Inclusiveness (O&I) is responsible for all functions and activities designed to promote diversity and maintain a work environment that is fair, unbiased, and inclusive. O&I's analysis of performance appraisal data indicated that there were significant differences in appraisal averages for African American and Caucasian analysts. GAO contracted with the Ivy Planning Group to assess the factors that influenced the differences. Ivy issued its African American Performance Assessment Study report on April 25, 2008 and the Acting Comptroller General issued a memorandum on April 30, 2008 expressing his commitment to addressing all of the report's recommendations.

The subcommittee asked GAO's Inspector General (IG) to examine the effectiveness of O&I and analyze the representation of women and minorities in the agency's Senior Executive Service (SES) and managerial ranks (GS-15 and equivalent level). This testimony focuses on the results of the IG's review and provides information on actions taken and planned to further enhance diversity at GAO.

To view the full product, including the scope and methodology, click on GAO-08-1160T. For more information, contact Ronald A. Stroman at 202-512-8401 or stromanr@gao.gov .

What GAO Found

The Inspector General's (IG) report recognizes the gains GAO has made to enhance the profile of its SES and managerial ranks. The report notes that the representation of most groups in GAO's SES and managerial ranks exceeded or equaled the representation in either the civilian labor force or the executive branch agencies. For example, the percentages of African Americans at the SES level and at the GS-15 and equivalent level exceeded the percentages in both the civilian labor force as well as in the executive branch agencies. The report also acknowledges that GAO has implemented many of the leading diversity management practices. Additionally, the report includes four recommendations that GAO has already taken steps to implement. For example, GAO is revising the discrimination complaint process order to clarify responsibilities and procedures when a complaint concerns O&I staff, and strengthening its internal controls for tracking, reviewing, and reporting on complaint data.

In addition to implementing the recommendations in the IG's report, GAO has taken steps to address many of the recommendations in the African American Performance Assessment Study report prepared by the Ivy Planning Group. The report included more than 25 recommendations. The Acting Comptroller General has committed to addressing all of them and issued a memorandum on September 10, 2008 that highlighted the progress made. For example, GAO has developed an approach for convening a series of facilitated conversations on race, begun to reassess the appraisal system, *c*reated standards for appraisal reviews, and taken steps to strengthen its recruitment and retention initiatives.

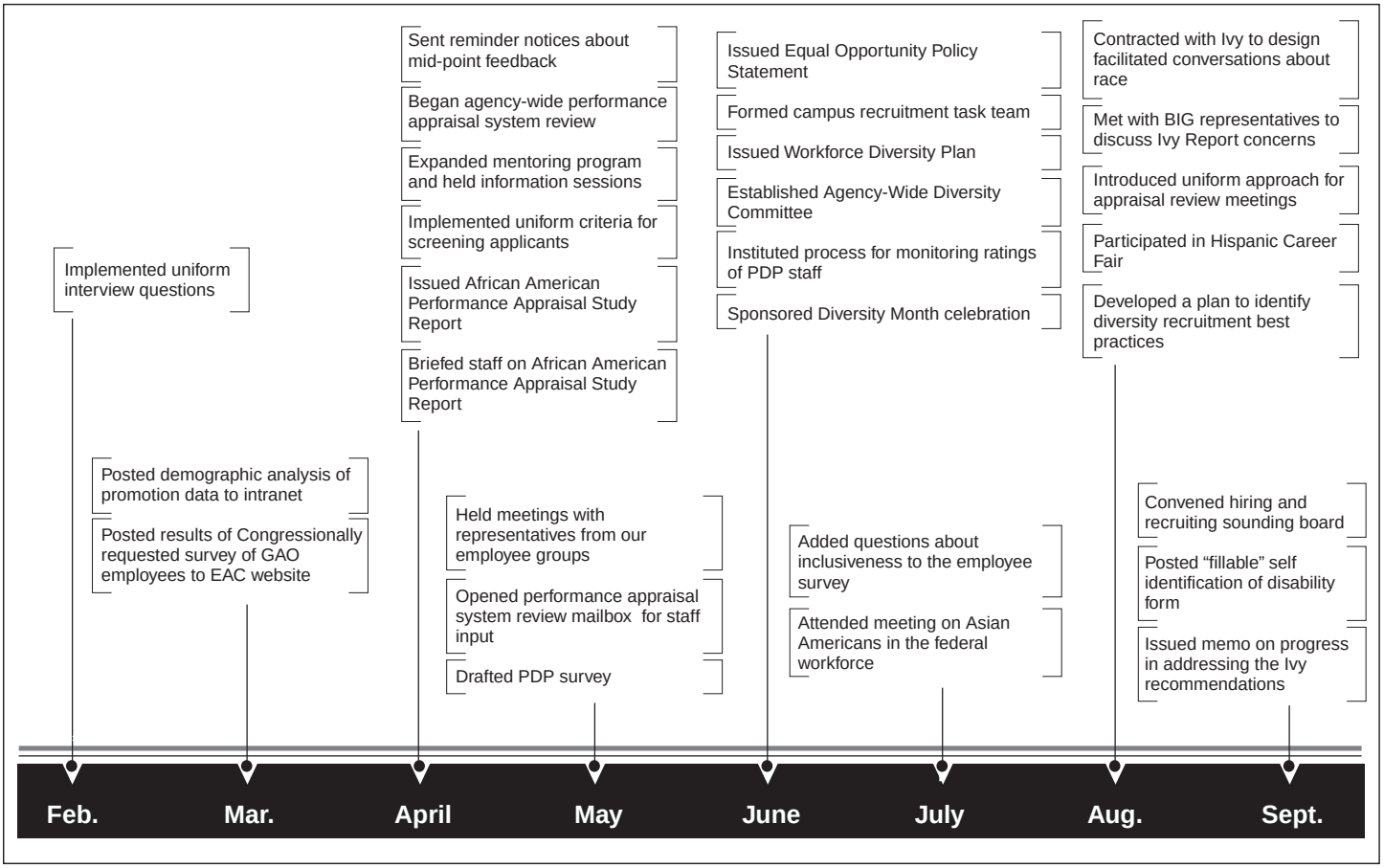
Furthermore, GAO plans to take additional steps to enhance its diversity by completing actions in its Workforce Diversity Plan**.** In June 2008, GAO issued a detailed Workforce Diversity Plan designed to build on the gains made in the diversity of its management and overall workforce. The plan lists about 20 actions that the agency will take. For example, the plan requires that GAO develop a diversity recruitment plan and calls for GAO to develop stronger relationships with Hispanic Serving Institutions and organizations that work with disabled students.

GAO is committed to working closely with all employees to ensure its diversity efforts and work environment are fully inclusive. GAO has established a comprehensive accountability framework to ensure the effective and efficient implementation of the Ivy report recommendations and the workforce diversity plan action steps. GAO has taken many steps and plans to take others to help enhance its diversity, recognizing that diversity is a journey that will require constant and sustained commitment.

Chairman Davis and Members of the Subcommittee:

I am Ron Stroman, Managing Director of the Office of Opportunity and Inclusiveness at the United States Government Accountability Office (GAO). Thank you for the opportunity to testify about the Inspector General's (IG) report on GAO's diversity efforts. GAO has a diverse workforce. Specifically, as of April 2008, minorities represented about 30 percent of our total workforce, and women comprised more than one-half. Nonetheless, we have gaps in certain categories. We are committed to making improvements. To this end, as figure 1 shows, we have completed several tasks in support of our diversity management efforts. Also, we have undertaken a number of important initiatives and have plans to implement others to improve the diversity of our leadership as well as our overall workforce, which I will discuss later in my testimony.

Figure 1: Timeline of Key Diversity Management Related Tasks Completed From February to September 10, 2008



Source: GAO.

IG Cites Diversity Improvements and Makes Recommendations That We Are Implementing

We appreciate the IG's recognition of the gains GAO has made to the diversity profile of our Senior Executive Service (SES) and managerial (GS-15 and equivalent) ranks. The IG's report indicates that from 2002 to 2007, the number of women in the SES increased and the number of African American, Asian American, and Hispanic managers also increased. For example, the data in the report show that the number of Hispanic managers increased from 17 in 2002 to 26 in 2007—an increase of 53 percent. Additionally, the report notes that the representation of most groups in GAO's SES and managerial ranks exceeded or equaled the representation in either the civilian labor force (CLF) or the executive branch agencies. Specifically, the percentages of

- African Americans at the SES level and at the GS-15 and equivalent level exceeded the percentages in both the CLF as well as in the executive branch agencies.
- Asian Americans at the SES level exceeded the percentages in the CLF as well as in the executive branch agencies.
- Hispanics at the GS-15 and equivalent level slightly exceeded the percentage in the executive branch agencies; and
- women at the SES and GS-15 and equivalent level exceeded the percentages in the executive branch agencies and at the GS-15 and equivalent level the percentage of women nearly equaled the percentage in the CLF.

The IG's report also acknowledges that we have implemented many of the leading diversity management practices. For example, we have

- recruited at historically black colleges and universities as well as Hispanic serving institutions,
- implemented an agency-wide mentoring program,
- supported employee involvement in diversity management through our newly established Diversity Committee,
- included diversity in our strategic plan, and
- incorporated diversity principles into our performance appraisal systems.

Additionally, the IG's report identifies areas for improvement and includes four recommendations that we have already taken steps to implement. We are revising the Office of Opportunity and Inclusiveness (O&I) order to require an annual Workforce Diversity Plan and revising the discrimination complaint process order to clarify responsibilities and procedures when a complaint concerns staff within O&I. We are also strengthening our internal controls for tracking, reviewing, and reporting on complaint data. In addition, we are planning to incorporate the diversity plan goals into the SES performance appraisal system when it is revised. We are also looking into ways to remove O&I staff from the pre-complaint processing stage without reducing our ability to successfully resolve employee concerns informally.

Steps Taken to Address the Ivy Planning Group Recommendations

In April 2008, the Ivy Planning Group (Ivy) issued its African American Performance Assessment Study report. This study was undertaken in response to significant differences in performance appraisal averages between African American and Caucasian analysts. The fundamental issue identified by the Ivy report is that the GAO culture, which values a singular and uniform approach to producing its work for the Congress must continue to change. Ivy recommended that GAO improve its ability to adapt to the diverse backgrounds and working styles of its changing workforce and make its human capital process fairer, more consistent, and more transparent. Moreover, the Ivy Report recommended that GAO raise staff awareness of the role that race can and does play in affecting performance related communication. The report included more than 25 recommendations.

The Acting Comptroller General wrote to all GAO staff on April 30, 2008, to express his commitment to address all of the Ivy report's recommendations. He issued another memo on September 10, 2008 updating the progress in addressing these recommendations, including the following.

Convening a Series of Facilitated Conversations on Race

The Ivy report suggested that we begin our efforts to create a more inclusive environment by convening a series of facilitated conversations across the agency about perceptions and assumptions regarding race. These conversations are intended to eliminate barriers to effective performance-related communication and bridge different perceptions on the likely causes for ratings disparities. After thoroughly researching qualified firms and gaining an in-depth understanding of the complexities associated with this effort, we signed a contract with Ivy in August 2008 to help us design and facilitate these discussions. We decided to use Ivy because of its extensive experience in convening these sensitive discussions, and because of its knowledge of GAO's culture and understanding of diversity issues confronting GAO's workforce. Ivy has begun to plan for these sessions and we expect that they will begin this fall and last through the spring. Importantly everyone at GAO will participate in these conversations. Lessons learned from these conversations will inform agencywide diversity training—another of Ivy's recommendations—which we will develop as part of GAO's ongoing mandatory training curriculum for all employees.

Proactively Assessing the Needs of a Diverse Workforce

The Ivy report also stressed the importance of implementing our diversity initiatives in a broad and inclusive manner, and Ivy recommended that we proactively assess the needs of the broad ranges of groups within GAO as early steps in becoming more inclusive. O&I staff held meetings with representatives from Blacks in Government (BIG), the Advisory Council for Persons with Disabilities (ACPD), the Asian American Liaison Group (AALG), the Gay and Lesbian Employee Association, and the Hispanic Liaison Group (HLG) in conjunction with developing our June 2008 Workforce Diversity Plan. During these meetings the representatives shared their concerns about the work environment and suggested steps that we can take to make the environment more inclusive. We have already taken some steps to address several of these concerns. For example, to help address the concern about underrepresentation of Hispanics at GAO, we joined with HLG in setting up a booth at a Hispanic Career Fair. To help address a concern about retention of Asian Americans, we worked in partnership with AALG to attend an Equal Employment Opportunity Commission (EEOC) meeting on Asian-Americans in the federal workforce. Additionally, to help address the concern about limited information on staff with disabilities, we created a version of the self-identification of disability form that can be completed electronically.

Creating a More Inclusive Work Environment

In addition to the steps outlined above, this June we established and convened an agency-wide Diversity Committee, which aims to foster opportunities for dialogue and serve as an advisory body to the Executive Committee and other senior executives. Representation on the Committee is comprised of employees elected to the designated diversity seats on the interim council of GAO's Employee Organization, International Federation of Professional and Technical Engineers (IFPTE); employees designated by GAO employee organizations; and GAO management representatives. The committee has met twice to date, and a Website is in development so employees can learn more about its efforts.

In addition, in June the Acting Comptroller General issued an equal employment opportunity statement in which he articulated his view of and commitment to the principles of fairness and equal opportunity. Further, we added questions to the employee feedback survey to measure staff views about the inclusiveness of our work environment. We also instituted a process for monitoring the ratings of those in the Professional Development Program (PDP) to identify and assess any disparities by race or other factors, and opened up our existing mentoring program to PDP and other developmental staff.

Finally, but equally importantly, the Acting Comptroller General and members of the Executive Committee met with BIG representatives to discuss their views of the Ivy report and to learn more about their suggestions for our approach going forward. The Executive Committee committed to an ongoing dialogue with BIG and made the same pledge to other employee groups throughout the agency, including the new Diversity Committee.

Reassessing the Appraisal System - the PAS Study

Ivy recommended that GAO conduct an agency-wide review of our performance appraisal system. We had anticipated the need for such a study before Ivy's report was completed. Throughout the spring and summer, our Performance Appraisal System (PAS) study team has been working to re-examine what works, what does not, and what could be done better with our current system. The team is guided both by a Steering Committee of senior executives and a stakeholder group comprised of representatives from the Employee Advisory Council (EAC); IFPTE; and the Diversity Committee, as well as O&I and GAO's Applied Research and Methods (ARM) team, among others. The PAS study team has completed its interviews with more than 50 GAO executives and managers and conducted nearly 30 focus groups with staff from all pay plans and bands. Seven of the focus groups were convened to gather views from specific populations, including African Americans, Hispanics, and employees with disabilities, in order to determine whether there were issues of concern that were unique to these groups. In sum, more than 200 individuals participated in all of the team's interviews and focus groups. Additionally, the PAS team has drafted a survey that will be sent to all employees this fall. The objective of the survey is to systematically collect employee opinions on what aspects of the performance appraisal system are working well and what merits attention. The team's final report is expected in early 2009.

Training for Designated Performance Managers and All Staff on the Appraisal Process

Ivy also recommended that we retrain all Designated Performance Managers (DPMs) and reviewers and provide more specific examples of the performance that supports the work activities and standards for each rating. This month we issued a notice informing all DPMs that they will be required to take appraisal training by October 7. We also issued a notice advertising the briefings we have scheduled through September for employees on the appraisal process, as well as the one-on-one help sessions we will provide to (1) offer employees individual assistance with preparing self assessments and (2) provide an opportunity for DPMs to ask questions about or request guidance on assigning checkmarks or preparing narratives.

Creating Standards for Appraisal Reviews	Ivy also recommended that GAO create standards for team performance appraisal review meetings. In response, we studied existing practices across GAO as well as prevalent practices in the literature, and just recently issued interim guidelines for teams, staff offices, Chief Administrative Office (CAO) units and the field. These interim guidelines for review of performance ratings are to be used for the 2008 performance appraisal cycle.
Instituting and Deploying Upward Feedback Tools	Ivy also recommended that we design and implement a measure for upward feedback. Steps are underway to institute and systematically deploy an agency wide upward feedback tool to provide feedback on management's effectiveness in supervising and developing staff. The plan is to implement this tool in March 2009.
Monitoring Mid-Point Feedback	Ivy also honed in on the importance of ongoing feedback. In addition our staff, managers, and senior executives have indicated that mid-point feedback was either not occurring or not being documented. In response, we sent reminder notices earlier this spring about the importance of delivering mid-point feedback.
Addressing Concerns with the Professional Development Program (PDP)	We have established a working group of executives and managers to address the issues related to the PDP. Also, a survey instrument has been designed and pre-tested to assess the views of PDP staff as they complete the program. The survey includes questions about the role of the advisors.
Strengthening Recruitment and Retention Initiatives	We also have taken steps in response to three of Ivy's recommendations by (1) forming a task team to analyze the schools we visit; identify different types of on-campus activities we support; determine the numbers and types of staff that participate in our on-campus recruiting efforts; and measure the costs, outcomes, and yields from these efforts; (2) developing a plan to research and identify best practices in diversity recruitment; and (3) establishing consistent criteria for our screeners to use when evaluating applications and a consistent set of questions for our managers to use when interviewing candidates. We also plan to map the recruitment and hiring process to identify pain points and areas for improvement, and calculate the cost of turnover.

Workforce Diversity Plan Identifies Additional Steps We Will Take to Enhance Diversity

This spring we conducted a workforce diversity review. The review included a careful analysis of our workforce data in comparison to benchmarks recommended by the EEOC. In conducting this review, we consulted a wide range of sources to identify areas where barriers may exclude certain groups. Specifically, we shared data with and obtained views from representatives from our employee groups and the GAO unit of IFPTE, analyzed employee feedback survey responses for 2006 and 2007, reviewed relevant policies, procedures and practices; analyzed findings from prior O&I efforts; and interviewed responsible officials.

The review found that our overall workforce was diverse and included a significant percentage of minorities and women. Specifically, as of April 2008, our workforce was more diverse than the civilian labor force (CLF).[1] Minorities represented about 30 percent of GAO's total workforce, and women comprised more than one-half of the workforce. In comparison, minorities comprised about 28 percent of the CLF and women represented about 47 percent. Furthermore, the diversity in the predominant employee group—analyst and analyst-related staff—exceeded the diversity in the relevant civilian labor force (RCLF).[2] In addition, for three of the larger job series that included about two-thirds of the workforce—the analyst, auditor, and attorney job series—the representation of each minority group was about the same or exceeded such representation in the RCLF. Furthermore, we hired a diverse group of employees. From March 2007 to April 2008, we hired 238 new staff. The percentages of African American women hired equaled the CLF percentages and the percentages of Asian American men and women hired exceed the percentages in the CLF.

However, our review found that Hispanic staff were underrepresented in our total workforce when compared to the CLF. Although the total percentages of Hispanic staff in analyst and analyst-related positions as well as in attorney positions equaled the representation in such positions compared to the RCLF, the percentages of Hispanic staff in other positions were low. Our analysis revealed that additional steps are needed to recruit Hispanic staff. For the most part, our efforts have focused on recruiting

[1]The CLF is composed of those 16 and older (including federal workers) who are employed or looking for work and not in the military or institutionalized. We used 2000 CLF data because it is the most current and reliable at this time.

[2]RCLF data are the CLF data directly comparable (or relevant) to the occupational population being considered. We use the RCLF when analyzing occupational series. We use the 2000 RCLF because it is the most current and reliable data available at this time.

Hispanic staff for analyst and analyst-related positions. While we will continue to enhance these efforts, we also need to improve our approach to recruiting attorneys and recruiting for mission-support positions, recognizing that the number of opportunities to recruit for these positions may be limited.

Additionally, we determined that the percentage of staff with targeted disabilities in our workforce was lower than the EEOC-recommended benchmark.[3] The EEOC has raised concerns that data on employees with disabilities in the federal government may not be accurate. GAO shares this concern and will be following up to enhance the accuracy of self-reported information.

The review also indicated that there were few minorities at certain levels in several job categories. Furthermore, we obtained information about agency practices that need to be addressed to improve our efforts to develop and maintain an inclusive environment.

Based on the review we issued a detailed Workforce Diversity Plan in June 2008. The action steps in the plan are designed to build on the gains we have made in the diversity of our management and overall workforce. The Workforce Diversity Plan requires that we develop a specific diversity recruitment plan (also a recommendation in the Ivy report) that includes efforts to recruit for analyst, attorney, and administrative positions. We will expand our relationships with Hispanic-serving institutions as well as expand the range of sources from which candidates are found. Specifically, we plan to contact campus organizations, national sororities, and fraternities when visiting campuses; reach out to professional organizations that we have not previously established relationships with; and attend job fairs targeted to Hispanic and other minority candidates. We also are gathering information from our current Hispanic employees, as well as reviewing data from the national data base on college graduates.

The plan also commits GAO to take additional steps to recruit staff with targeted disabilities. In order to address this concern, we recently formed a working group on disability issues that included staff from the ACPD—our employee group that focuses on disability issues. Our diversity

[3]The targeted disabilities are deafness, blindness, missing extremities, partial paralysis, complete paralysis, convulsive disorders, mental retardation, mental illness, and distortion of limb and/or spine.

recruitment plan will include efforts to recruit persons with disabilities for analyst, attorney, and administrative positions. We plan to expand and enhance our relationships with institutions and organizations that work with students with disabilities such as the Career Opportunities for Students with Disabilities—a nationwide consortium of higher education institutions and employers that facilitates the career employment of college graduates with disabilities. Also, we plan to gather information to help inform our recruitment efforts by surveying staff to update their disability status, interviewing our staff with disabilities, and analyzing national data on graduates. Further, we plan to use our non-competitive appointment authority to hire staff with disabilities.

As shown in Table 1, the plan recommends changes that can be accomplished by April 2009—12 months from the start of our review—in order to hold ourselves accountable for achieving the plan's goals. The plan will be updated annually and will lead to significant long term improvements to our human capital processes that are at the heart of diversity issues confronting GAO.

Table 1: GAO's 2008—2009 Workforce Diversity Action Plan

GOAL: Recruit More Hispanics, African Americans and Staff with Disabilities		
Action items	**Completion date**	**Responsible units**
1. Develop a diversity recruitment and hiring plan to enhance participation from all groups	April 2009	O&I, HCO
In support of this plan	September 2008	O&I, HCO
a. Interview current minority and disabled staff to determine what led them to join GAO		
b. Analyze data from Department of Education on minority graduates with selected majors	December 2008	O&I, ARM, HCO
c. Develop stronger relationships with Hispanic-serving Institutions, historically-black colleges and universities and institutions and organizations that work with disabled students.	January 2009	HCO, Campus Executives
d. Expand the range of sources from which candidates are recruited (including campus organizations, national sororities and fraternities and professional organizations as well as using electronic recruiting efforts).	March 2009	HCO
e. Issue guidance to recruiters emphasizing diversity as a recruitment factor and ensure that recruitment efforts include law schools and job fairs targeted to higher concentrations of minority students.	March 2009	GC
2. Use noncompetitive appointment authority to hire qualified staff with disabilities	March 2009	O&I, HCO
GOAL: Enhance Staff-Development Opportunities That Prepare Staff for Upper-Level Positions		
1. Expand one-to-one mentoring program	August 2008	HCO/LC
2. Hold managers accountable for providing performance feedback by analyzing data in our competency based performance system	December 2008	O&I
3. Identify steps for success and discuss the unwritten rules during workshops to share this information	January 2009	O&I, HCO/LC
4. Complete data analysis for performance appraisal system review	September 2008	HCO
5. Announce opportunities for staff to participate in agency-wide projects.	March 2009	CG
GOAL: Create a More Inclusive Environment		
1. Revise employee survey to include questions to measure the extent to which staff view our work environment as inclusive	June 2008	ARM, HCO
2. Issue EEO statement	June 2008	O&I, CG
3. Provide training sessions on EEO Policy/Harassment Issues	October 2008	O&I, GC
4. Provide employee groups with information that would allow them to reach out to new GAO staff and help improve retention of minorities	October 2008	HCO, GC
5. Hold facilitated discussions on race	December 2008	HCO/LC; O&I
6. Modify/revise Self-Identification of Handicap Form (SF 256)	December 2008	O&I, KS
7. Survey staff to update disability status	January 2009	HCO, O&I, ARM
8. Revise the reasonable accommodation process	March 2009	O&I, HCO
9. Interview minorities and staff with disabilities to obtain information on reasons for staying and reasons for leaving and analyze staff retention data	March 2009	O&I
10. Conduct diversity training to help staff understand barriers that may limit effective communication, coaching, and career development.	April 2009	O&I, HCO/ LC;

Source: GAO.

Conclusion

With the support of our top leadership, we have made diversity a part of our strategic plan, implemented leading diversity practices throughout the organization and developed annual plans that will help us enhance our diversity, particularly within our managerial ranks. Moreover, we have established a comprehensive accountability framework to ensure the effective and efficient implementation of the recommendations in the Ivy Report as well as the action steps in our Workforce Diversity Plan.

Finally, we are committed to working closely with the entire GAO community to ensure that our diversity efforts and our work environment are fully inclusive. We intend to take many steps to help enhance diversity at GAO, recognizing that diversity is a journey that will require constant and sustained commitment.

This concludes my prepared statement. At this time I would be pleased to answer any questions that you or other members of the subcommittee may have.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "E-mail Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, DC 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

U.S. GOVERNMENT PRINTING OFFICE

KEEPING AMERICA INFORMED

AUDIT REPORT 08-10

DIVERSITY MANAGEMENT PROGRAMS AT THE GOVERNMENT PRINTING OFFICE

September 11, 2008

OFFICE OF INSPECTOR GENERAL

U.S. GOVERNMENT PRINTING OFFICE
KEEPING AMERICA INFORMED
WASHINGTON, DC 20401

Memorandum

OFFICE OF THE INSPECTOR GENERAL

DATE: September 11, 2008

REPLY TO ATTN OF: Assistant Inspector General for Audits and Inspections

SUBJECT: Final Report on Audit of Diversity Management Programs at the GPO
Report Number 08-10

TO: Public Printer
Director, Office of Equal Employment Opportunity
Chief Human Capital Officer

Enclosed please find the subject final report. Please refer to the Executive Summary for the overall audit results. Our evaluation of your response has been incorporated into the body of the report and is included in its entirety as Appendix J. While management concurred with each of the report's recommendations, specific planned actions for each of the recommendations were not provided. We are requesting that you provide additional details related to specific actions the Agency plans to take to implement the recommendations. As a result, pending receipt of details related to implementation, each of the recommendations is considered unresolved. The final report distribution is in Appendix L.

We appreciate the courtesies extended to the audit staff. If you have any questions concerning the report, please contact Mr. Joseph Verch, Supervisory Auditor at (202) 512-0065, or me at (202) 512-2009.

(Original signed by)

Kevin J. Carson
Assistant Inspector General for Audits and Inspections

cc:
Chief of Staff
Chief Management Officer
General Counsel

Contents

Office of Inspector General

Report Number 08-10 **September 11, 2008**

Diversity Management Programs at the Government Printing Office

Executive Summary

Background. The Government Printing Office (GPO) Office of Inspector General (OIG) has completed an audit of diversity management programs at the GPO. The audit was conducted in response to a request from the Chairman of the Subcommittee on Federal Workforce, Postal Service, and the District of Columbia, of the House of Representatives' Committee on Oversight and Government Reform. The Subcommittee requested that the OIGs of each legislative branch agency assess the programs the diversity offices have in place to address diversity concerns.[1] The participating OIGs plan to publish the final results in a consolidated report by September 2008.

Objectives. The overall objective of the audit was to review diversity within GPO, specifically to:

- Identify and assess the diversity program at GPO to determine if it is yielding the desired results—that of creating a more diverse population of women and minorities in top leadership positions, specifically the Senior Level Service (SLS);[2]

- Evaluate the accuracy and completeness of the complaints and discrimination data reported to Congress; and

- Assess the degree to which diversity offices or functions are independent of the General Counsel and the Public Printer.

See Appendix A for details on the audit objectives, scope, and methodology.

Results of Audit. While not mandated to comply with the guidelines and directives of the Equal Employment Opportunity Commission (EEOC) concerning model affirmative action programs, prior to this audit commencing, senior officials at GPO, including the Directors of the Office of Equal Employment Opportunity (EEO) and Human Capital began adopting some elements of both EEOC Management Directive 715 (MD-715) and

[1] Other legislative branch agencies include the Library of Congress, Government Accountability Office, Architect of the Capitol, and the Capitol Police.
[2] Senior Level Service is the GPO equivalent to the Senior Executive Service (SES).

the leading diversity management practices identified by the Government Accountability Office (GAO). GPO has also made progress in developing its pool of Grade 15s (PG-15s) to ensure a qualified minority pool for the Agency's SLS.[3] However, improvements can be made towards enhancing the diversity of the Agency's corps of SLS employees.

The audit also showed that GPO complaints and discrimination data reported to the EEOC during fiscal year (FY) 2007 and eventually reported to Congress were accurate and complete. (See Appendix G). Further, although diversity management programs are incorporated in the Affirmative Employment Program (AEP) Division of GPO's EEO Office, the Director of EEO is independent of the General Counsel, and to a certain extent independent of the Public Printer in EEO matters. (See Appendix H).

Opportunities do exist for GPO to provide a more diverse population of qualified women and minorities in top leadership positions by incorporating the remaining essential elements of MD-715 as well as implementing the nine leading practices for diversity management identified by the GAO. Such modifications should help the agency manage the workforce and create an environment that helps diminish barriers for protected groups. In addition, changes brought about through diversity management should help attract and retain capable employees. With an expectation that a high percentage of the Government workforce will retire in the next decade, GPO should continue developing a comprehensive diversity program to meet those employment challenges.

The audit specifically identified that although GPO is not required to comply with MD-715 or GAO's leading diversity management practices:

- GPO has generally adopted three elements for creating and maintaining a model EEO program identified by MD-715, referred to as (1) demonstrated commitment from leadership, (2) efficiency, and (3) responsiveness and legal compliance. (Finding A); and

- Agency officials have partially adopted one of the GAO's nine leading diversity management practices (top leadership commitment). (Finding B).

Recommendations. We made two recommendations to GPO management, which, if implemented, should not only improve the GPO diversity program by providing a more diverse population of qualified women and minorities in top leadership, but also contribute to GPO's ability to meet its future employment challenges.

Management's Response. GPO Management concurred with each of the report's two recommendations and stated that implementation would require the Public Printer's review and approval (see Appendix J).

[3] At GPO, a Printing Office Grade (PG) 15 is the senior most grade and is generally equivalent to the General Schedule (GS) Grade 15 classified by the Office of Personnel Management. Positions at GPO above Grade PG-15 are in the Senior Level Service (SLS).

Evaluation of Management's Response. While GPO management concurred with each of the recommendations, they did not provide details regarding what actions the Agency plans to take to implement the recommendations. As a result, pending receipt of details related to implementation, the recommendations are considered unresolved.

Introduction

In November 2007, the Chairman of the Federal Workforce, Postal Service, and the District of Columbia Subcommittee of the House of Representatives' Oversight and Government Reform Committee issued a report entitled "Senior Executive Service: Women and Minorities are Underrepresented in Most Legislative Branch Agencies."[4] The report discusses racial and gender diversity of the Senior Executive Service corps in the six legislative branch agencies during FY 2007. The report stated that:

- Minorities represent 16.8 percent and women represent 35.8 percent of Senior Executive Service corps members in the six legislative branch agencies.

- In FY 2007, Senior Executive Service corps members at each agency were less diverse in terms of minorities than the agency's workforce as a whole and in four of the six agencies less diverse in terms of women.

- The representation of minorities in the legislative branch Senior Executive Service corps is stagnant, with representation of women improving only slightly between FY 2002 and FY 2007.

- General Schedule-15 successor pools[5] at some agencies were less diverse than the Senior Executive Service corps.

- In some agencies, the average total salary for minorities and women in FY 2007 was less than for nonminority and male counterparts.

To ensure equal opportunity and diversity, the EEO Office at the GPO is responsible for complying with civil rights statutes and regulations governing Federal employment.[6] As of January 28, 2008, GPO had a total of 2,263 white and blue collar employees (see Appendix C). White collar employees generally consist of administrative, technical, clerical, professional and management personnel while blue collar employees consist generally of those employees who work in production departments. Of the 2,263 employees at GPO, 956 were women (42.3 percent) and 1,359 were minorities (60.1 percent). On staff at GPO are a total of 26 SLS employees consisting of 3 women (11.5 percent) and 3 minorities (11.5 percent). For white collar workers, the ratio between women and minorities and SLS employees was similar—645 women (42.3 percent) and

[4] Report may be found at http://federalworkforce.oversight.house.gov/story.asp?ID=1617

[5] The November 2007 report of the Chairman of the Federal Workforce, Postal Service, and the District of Columbia Subcommittee of the House of Representatives' Oversight and Government Reform Committee defines successor pools as an agency's GS-15 and equivalent ranks of which the diversity of such pools can provide an indicator of how diverse the Senior Executive Service (or equivalent rank) could become in the future.

[6] Title VII of Civil Rights Act of 1964, Age Discrimination in Employment Act of 1967, and Title I of the Americans with Disabilities Act of 1990.

611 minorities (52.5 percent). Tables 1 and 2 below provide more detail between the makeup of GPO's total workforce and between the total white collar workforce and the SLS corps.

Table. 1. FY 2008 Total Workforce (as of January 28, 2008)

Employees	Workforce	
Males	**Number**	**Percent**
White	610	27.0
African American	639	28.2
Asian American/Pacific Islander	26	1.1
Hispanic American	26	1.1
Native American	6	0.3
Total Males	**1,307**	**57.7**
Females		
White	294	13.0
African American	622	27.5
Asian American/Pacific Islander	24	1.1
Hispanic American	12	0.5
Native American	4	0.2
Total Females	**956**	**42.3**
Overall Totals	**2,263**	**100.0**

Table 2. FY 2008 White Collar Workforce Contrasted with SLS Employees (as of January 28, 2008)

Employees	Workforce		SLS	
Males	**Number**	**Percent**	**Number**	**Percent**
White	315	27.1	22	84.6
African American	165	14.2	0	0.0
Asian American/Pacific Islander	19	1.6	0	0.0
Hispanic American	17	1.4	1	3.9
Native American	2	0.2	0	0.0
Total Males	**518**	**44.5**	**23**	**88.5**
Females				
White	237	20.4	1	3.8
African American	372	32.0	2	7.7
Asian American/Pacific Islander	20	1.7	0	0.0
Hispanic American	12	1.0	0	0.0
Native American	4	0.4	0	0.0
Total Females	**645**	**55.5**	**3**	**11.5**
Overall Totals	**1,163**	**100.0**	**26**	**100.0**

The EEO Director is responsible for ensuring that equal opportunities exist for employees and applicants without regard to race, sex, color, religion, national origin, sexual orientation, age, and physical and mental disability. The EEO Office consists of two divisions: (1) the Affirmative Employment Program (AEP) Division; and (2) the Counseling and Complaints Processing Division (CCPD). For FY 2007, the GPO EEO Office had a budget of $888,500 and a staff of seven employees.[7]

AEP Division

The AEP Manager assures that equal opportunity principles are an integral part of every aspect of personnel policy and practice in the recruitment, employment, development, advancement, and treatment of GPO staff and applicants for employment. In addition, the AEP Manager also manages special emphasis programs that implement Presidential Executive Orders and Federal personnel programs for eliminating demographic group imbalances in targeted occupations, and achieving diversity in the workforce.

The AEP manager oversees three special emphasis programs assigned to GPO managers who work the programs as a collateral duty. Collateral duty managers can spend up to 25 percent of their time managing the following special emphasis programs.

- ***Disability Program***

The Disability Program at GPO consists of a program manager and ten employees who voluntarily serve on the Disability Program Committee. The mission of the committee is to raise awareness of disability policies and programs through information dissemination and education programs and help elevate disability concerns to the EEO Office. The program committee works with the EEO Office to identify employment barriers to individuals with disabilities, review Agency policies addressing employment issues, and recommend changes.

- ***Federal Women's Program***

The Federal Women's Program (FWP) at GPO has the involvement of the EEO Director, the AEP Manager, and an FWP Manager, who performs the job as a collateral duty. The FWP committee also has 34 members. The FWP committee's mission is to continually identify, promote, and enhance employment and training opportunities for women. The committee also helps keep women at GPO apprised of employment issues; assists women in training, career development, and advancement; provides networking channels with other FWP organizations on issues related to eliminating barriers to equal access and opportunity; and promotes professionalism that furthers the progress of women.

[7] GPO's budget for FY 2007 was $848.225 million.

- ***Hispanic Employment Program***

The GPO Hispanic Employment Program's (HEP) mission is to eliminate discriminatory practices, assist in eliminating areas of under-representation or underutilization, evaluate practices for disparate impact or treatment, and recommend changes to eliminate barriers to Hispanic employment. The HEP manager serves in the position as a collateral duty and also serves as the Secretary to the National Council of HEP Managers, a body consisting of members from 40 different federal agencies appointed as their agency's designee responsible for building relationships between federal agencies and the Hispanic community. The HEP manager also is responsible for e-mailing GPO job vacancies to not only 67 Hispanic organizations, but also to more than 800 individuals who belong to the Washington DC-Hispanic Employment Network.

- ***Other Programs***

The AEP Manager also manages the pilot Employee Mentoring Program and the Passport-to-Work Summer Youth Program, and also co-manages the Coming Home to Work Program. The GPO Employee Mentoring Program (GEM) began as a pilot program in April 2008 and is designed to enhance employee retention, job satisfaction, and cross-organizational communication through employees receiving guidance, counseling, and coaching from designated GPO mentors. In another program, the Department of Veterans Affairs works with GPO and sponsors the Coming Home to Work Program that helps provide suitable employment opportunities for eligible members of the armed services. The Passport-to-Work Summer Youth Program offers District of Columbia youths, ages 14 to 21, a 10-week temporary summer job at GPO—funded by the District of Columbia Youth Employment Office. GPO has participated in this program for several years, and placed an average of 52 students from this program during the last 6 years, with 48 placed in 2008.

CCPD Division

The Assistant Director/Chief of CCPD manages the EEO complaint process for GPO employees and applicants for employment involving issues of discrimination on the basis of race, sex, color, religion, national origin, sexual orientation, age, disability, and reprisal for prior participation in the EEO complaints process. Along with three EEO specialists, the Chief of CCPD issues policy and guidelines related to discrimination complaint procedures, monitors complaints of discrimination to detect indications of discriminatory patterns and practices, and prepares final Agency decisions on complaints. The CCPD also collects, maintains, and analyzes data on the discrimination complaint process and serves as the official source of information for the status of complaints at GPO. CCPD also oversees recruiting, selecting, and maintaining a cadre of trained EEO specialists.

Leadership, Development, and Recruitment Program

The Agency has also recently started a new leadership program for employees. The Leadership, Development, and Recruitment (LDR) program is a 2-year program, and is staffed with employees recruited from both within and outside the Agency. The LDR program allows employees to work in a number of business units—receiving well-rounded, hands-on experience necessary to prepare them as future GPO leaders.

Findings and Recommendations

Finding A. Incorporating the Essential Elements of EEOC Management Directive-715

Although not mandated, senior officials at GPO have begun to generally follow several of the key elements of the EEOC's MD-715 for creating and maintaining a model EEO program into the structure of the Agency. For example, of the six essential elements outlined in MD-715, GPO has generally incorporated three: (1) demonstrated commitment from agency leadership; (2) efficiency; and (3) responsiveness and legal compliance. The three additional elements that would help establish a model EEO program include: (1) integration of EEO into the agency's strategic mission; (2) management and program accountability; and (3) proactive prevention of unlawful discrimination.

Basic Tenets of Management Directive 715

Effective October 1, 2003, the EEOC issued MD-715. The directive provides the basic elements necessary for creating and maintaining a model EEO program in the Federal government. The directive specifically applies to agencies in the executive branch and Military Departments (except uniformed members), the U.S. Postal Service, the Postal Rate Commission, the Tennessee Valley Authority, the Smithsonian Institution, and those units of the judicial branch of the Federal Government having positions in the competitive service.

When establishing a model EEO program, MD-715 provides that an agency should incorporate into its design a structure for effective management, accountability, and self-analysis that will ensure program success. MD-715 not only contains reporting requirements, but states that six essential elements make up a model EEO program including:

- Demonstrated commitment from agency leadership.
- Integration of EEO into the agency's strategic mission.
- Management and program accountability.
- Proactive prevention of unlawful discrimination.
- Efficiency.
- Responsiveness and legal compliance.

As part of the audit, the OIG assessed the current status of GPO's voluntary efforts to integrate the elements of MD-715 into the structure of the Agency. The results of our assessment are discussed in the following section and are summarized in Appendix B.

Essential Element One – Demonstrated Commitment From Agency Leadership

Element One recommends that the demonstrated commitment from agency leadership start with an effective EEO program policy statement. The criteria states that at the beginning of a tenure and each year thereafter, the head of an agency should issue a signed written policy statement announcing the agency's position against discrimination based on the areas that Federal law covers. GPO has voluntarily adopted this element as the Public Printer issued a policy statement to all GPO employees on April 8, 2008, emphasizing his personal commitment to equal opportunity and diversity. (See Appendix E for the complete text of that statement).[8]

The element further recommends that the head of an agency and other senior management officials demonstrate a commitment to equal employment by incorporating the principles of EEO into an agency's organizational structure and disseminating a policy demonstrating this commitment annually. Publishing such a statement sends a clear message to others in the organization about the seriousness and business relevance of diversity management. Accordingly, we recommend that the Public Printer continue to issue a policy statement addressing his commitment to EEO and diversity on a yearly basis as suggested by MD-715.

Essential Element Two – Integration of EEO into the Agency's Strategic Mission

Element Two provides that the concepts of EEO should be a part of the strategic mission and that an agency's EEO program should be organized and structured in a way that maintains a workplace free from discrimination through its policies, procedures, or practices. Although GPO's current strategic plan entitled *A Strategic Vision for the 21st Century* (December 1, 2004) does not include an EEO message, GPO has followed several of the other concepts of Element Two in that GPO has:

- Maintained a reporting structure that allows the EEO Director the appropriate authority and resources to effectively carry out a successful EEO program.

- Committed sufficient human resources and budget allocations to the EEO program for a successful operation.

- Empowered the EEO Director to have regular and effective ways of informing the Public Printer and senior management officials of the status of EEO programs and being involved in, and consulting on, management and personnel actions.

While management has recognized several aspects of Element Two, management should integrate EEO into the Agency's strategic plan. Accordingly, we recommend that as the new Public Printer formulates his strategic plan, he include EEO and diversity as an integral part of GPO's strategic mission.

[8] The current Public Printer was appointed by the President on November 6, 2007. While the current Public Printer issued a policy statement to employees at the beginning of his tenure as Public Printer, over three years had elapsed since the previous Public Printer issued his statement on February 1, 2005.

Essential Element Three – Management and Program Accountability

To ensure management and program accountability, criteria in Element Three discusses overall accountability and EEO program management. The criteria recommends that the head of an agency should hold managers, supervisors, and EEO officials responsible for effective implementation of an agency's EEO program and plan.

The thrust of management and program accountability is that EEO officials advise and provide assistance to managers about the status of EEO programs within each manager's area of responsibility. In addition, the Directors of EEO and Human Capital should meet regularly and assess whether personnel programs, policies, and procedures conform to EEOC management directives. MD-715 also instructs that the agency explore whether disciplinary actions should be taken when findings of discrimination are made.

In October 2007, EEO officials at GPO began meeting with business unit managers semiannually to discuss EEO issues and concerns within business units, provide information on EEO programs and analysis of workforce data, and obtain input that could assist in developing strategies for improving EEO programs at GPO.

While GPO practices address portions of Element Three's criteria, we recommend that EEO continue to work with business unit managers to develop EEO plans and that EEO and Human Capital officials work together and with business unit managers to identify systemic barriers in hiring, promotions, training, and awards.

Essential Element Four – Proactive Prevention of Unlawful Discrimination

Element Four states that an agency has an obligation to prevent discrimination on the basis of race, color, national origin, religion, sex, age, reprisal and disability, and to eliminate barriers that impede free and open competition in the workplace.[9] Putting such an obligation into place begins with informing employees about an effective anti-discrimination policy that explains the protections afforded by the civil rights laws, the rights afforded in such situations, and the process for redress. Further, the head of an agency must make efforts early to prevent discriminatory actions and eliminate barriers to equal employment opportunity in the workplace.

The criteria recommends that agencies conduct annual self-assessments to monitor progress, identify areas where barriers may operate to exclude certain groups, and develop strategic plans to eliminate identified barriers. In an attempt to benchmark GPO's status, we requested that the EEO officials conduct a self-assessment to help identify gaps and potential areas for development. The results of this assessment are summarized in Table 3.

[9] The Statement of the Public Printer, dated April 8, 2008, is more comprehensive than that recommended by MD-715: "Employment actions must be based upon merit principles and made without regard to an individual's race, color, religion, national origin, sex, age, mental/physical disability or sexual orientation."

Table 3. Types of Information Needed for Accurate Self-Assessment as Prescribed by MD-715

	Workforce Profiles	Provided	Not Provided
1.	Total workforce distribution by race, national origin, and sex for both the permanent and temporary workforce	X[10]	
2.	Permanent and temporary workforce participation rates for each grade level by race, national origin, and sex	X[11]	
3.	Permanent and temporary workforce participation rates for each of the agency's major occupational categories (divided by grade level) by race, national origin, and sex		X[12]
4.	Participation rates in supervisory and management positions by race, national origin, and sex		X[13]
5.	Race, national origin, and sex of applicants for both permanent and temporary employment		X
6.	Rates of selections for promotions, training opportunities and performance incentives, by race, national origin, and sex	X[14]	
7.	Rates of both voluntary and involuntary separations from employment by race, national origin, and sex	X[15]	

Since GPO is not required to follow MD-715, the AEP Manager has not yet implemented annual self-assessments. However, we recommend annual self-assessments so that the AEP Manager can more effectively monitor progress, identify areas where barriers exclude certain groups, and develop strategic plans to help eliminate barriers. Additionally, in the absence of a formal requirement for self-assessments, the data necessary to complete these assessments is not readily available from Information Technology and Systems (IT&S) in the desired format. Under the circumstances, the AEP Manager must now manually reformat data from Human Capital and arrange it in a format suitable for agency needs or congressional hearings. A request for software that would assist the efforts of the AEP Manager, is pending. Since more complete and accurate data would help the AEP Manager monitor progress and identify areas where barriers are possibly excluding certain groups, we recommend further action in order to meet the requirements of Element Four.

[10] Provided only permanent workforce for FY 2006 and 2007; did not provide temporary workforce.
[11] Provided only permanent workforce for FY 2006 and 2007; did not provide temporary workforce.
[12] Provided occupation by organization for FY 2007 and organization profile by occupation series for full-time, part-time, and other for FY 2006 and 2007.
[13] Provided organizational profile by supervisor and manager for full-time, part-time, and other for FY 2006 and 2007.
[14] Provided promotions for FY 2006 and 2007; Human Capital was not asked by EEO to provide profiles for training opportunities and performance incentives.
[15] Provided separations for FY 2006 and 2007; report did not distinguish between voluntary and involuntary for both years.

Essential Element Five – Efficiency

Element Five requires that the agency head ensure that there are effective systems in place for evaluating the impact and effectiveness of the agency's EEO programs as well as an efficient and fair dispute resolution process. Critical to this element are adequate and accurate information collection systems. Such systems fully integrated into an agency's infrastructure help it conduct periodic reviews—thus allowing the agency to stay on top of those items affecting the myriad of EEO areas.

Element Five identifies six areas for the agency to comply with EEOC's instructions including: (1) sufficient staffing, funding, and authority to achieve the elimination of identified barriers; (2) an effective complaint tracking and monitoring system in place to increase the effectiveness of the agency's EEO programs; (3) sufficient staffing, funding and authority to comply with the time frames in accordance with EEOC regulations for processing EEO complaints of employment discrimination; (4) an efficient and fair dispute resolution process and effective systems for evaluating the impact and effectiveness of the agency's EEO complaint processing program; (5) effective systems in place for maintaining and evaluating the impact and effectiveness of its EEO programs; and (6) ensuring that the investigation and adjudication function of its complaint resolution process are separate from its legal defense arm of the agency or other offices with conflicting or competing interests.

GPO is achieving many of the objectives of Essential Element Five. However, further progress can be made to develop methods to identify and eliminate barriers and implement specific strategies for evaluating the impact and effectiveness of EEO programs.

Additionally, EEO officials have experienced difficulty consolidating the information obtained from Human Capital due to the variances in data formats available for tracking the information required to achieve the elimination of identified barriers. Accordingly, we recommend that GPO management identify a solution to ensure the ability to obtain accurate data for use in identifying and eliminating barriers and to help evaluate the impact and effectiveness of its EEO programs.

Illustrative of this point is the absence of recruitment effort tracking and analysis. For example, between September 2007 and February 2008, the EEO Director visited universities in California, New Mexico, and Texas to recruit Hispanic Americans for GPO's 2008 Leadership Program and other job vacancies. In addition, Human Capital officials made similar visits to universities to recruit for the Leadership Program. Despite these efforts, Human Capital did not track these recruitment efforts or have a written plan for attracting a supply of qualified, diverse applicants for GPO employment. Since the EEO Director and Human Capital officials are not the hiring officials for GPO's individual business units, consideration should be given to having business unit managers participate in future recruiting efforts.

Although GPO was generally following most of the six subcategories, we recommend that management emphasize these additional areas, to help ensure that effective systems are in place for evaluating the impact and effectiveness of the EEO programs.

Essential Element Six – Responsiveness and Legal Compliance

Element Six contains a requirement that each year an agency certify that it is complying with EEO laws and EEOC regulations, policy guidance, and other written instructions. Element Six also identifies that agency personnel should be accountable for the timely compliance with EEOC orders. While the EEO staff are formally trained and responsible for compliance with EEO laws and EEOC regulations and orders, these requirements are not fully incorporated into the performance standards of GPO employees. The EEO Office has a system called EEO Network (EEONET) which ensures that any EEO cases over 30-days old are identified. This system is backed up by a manual calendar system which ensures that GPO officials comply in a timely manner with any orders or directives issued by EEOC Administrative Judges.

Although generally following the requirements of Element Six, management can send a positive and clear message to all GPO employees about maintaining a workplace free of discrimination and harassment as well as a commitment to EEO and diversity by requiring compliance with EEO laws and EEOC regulations in the performance standards of all managers and SLS personnel.

While GPO is voluntarily complying with several of the essential elements identified by the EEOC, the opportunity exists through fully incorporating the six elements to create and maintain a model EEO program at GPO. Creation of a model program will help further ensure that the agency is not only free from employment discrimination, but also has a diverse workforce.

Recommendation

1. The Public Printer should incorporate the six essential elements of Equal Employment Opportunity Commission Management Directive 715 by taking the following actions:

a. Continue to issue and disseminate to GPO employees an annual signed written policy statement expressing Agency commitment to equal employment opportunity as well as maintaining a workplace free of discriminatory harassment and practices.

b. Integrate equal employment opportunity policy and practices into future agency strategic plans.

c. Require, with assistance from EEO officials, that business unit managers develop an EEO plan for their individual units and that EEO and Human Capital officials meet regularly to identify any systemic barriers in hiring, promotions, training, and awards.

d. Conduct annual self-assessments that monitor progress, identify areas where barriers may exclude certain groups, and develop strategic recruitment plans to eliminate those barriers to the extent possible and to attract a qualified, diverse pool of applicants.

e. Maintain and provide sufficient resources—including staffing, funding, and authority—for EEO officials to track workforce profiles that will help eliminate identified barriers and recruitment efforts that will assist officials with identifying potential barriers. The resources provided should also include the information technology infrastructure (hardware, software, etc.) necessary to allow EEO officials to effectively produce workforce diversity statistics.

f. Incorporate compliance with EEO laws and EEOC regulations in performance standards for all managers including SLS personnel.

Management's Response. Concur. Implementation of the recommendation will require the Public Printer's review and approval (see Appendix J).

Evaluation of Management's Response. While GPO management concurred with the recommendation, they did not provide details regarding what actions the Agency plans to take to implement the recommendation. As a result, pending receipt of details related to implementation, the recommendation is considered unresolved. The OIG will work with GPO management to review any proposed actions to implement the recommendation.

Finding B. Incorporating GAO's Leading Diversity Management Practices

To date, GPO officials have partially adopted the nine practices identified by the GAO as the most common leading diversity management practices. Specifically, the Agency has partially adopted one of the GAO leading practices and is actively working on developing a plan for another of the practices--succession planning. GPO had not made decisions regarding adoption of the remaining practices at the time of the audit. Similar to the key elements of EEOC MD-715 for creating and maintaining a model EEO program, adoption of the nine practices identified by the GAO would help further ensure that the agency has a diverse workforce and an effective EEO program.

The GAO Leading Practices

In January 2005, GAO issued a report to the Ranking Minority Member, Committee on Homeland Security and Government Affairs, U.S. Senate entitled "Diversity Management: Expert-Identified Leading Practices and Agency Examples."[16] This report identified nine leading practices to be considered when an organization is developing and implementing a diversity management program. These nine practices were developed by GAO after speaking with experts in the field of diversity management and reviewing their publications. The practices that GAO identified include:

- **Top leadership commitment**—a vision of diversity demonstrated and communicated throughout an organization by top-level management;

- **Diversity as part of an organization's strategic plan**—a diversity strategy and plan that are developed and aligned with the organization's strategic plan;

- **Diversity linked to performance**—the understanding that a more diverse and inclusive work environment can yield greater productivity and help improve individual and organizational performance;

- **Measurement**—a set of quantitative and qualitative measures of the impact of various aspects of an overall diversity program;

- **Accountability**—the means to ensure that leaders are responsible for diversity by linking their performance assessment and compensation to the progress of diversity initiatives;

- **Succession planning**—an ongoing, strategic process for identifying and developing a diverse pool of talent for an organization's potential future leaders;

- **Recruitment**—the process of attracting a supply of qualified, diverse applicants for employment;

[16] GAO 05-90, January 14, 2005, available at http://www.gao.gov/newitems/d0590.pdf

- **Employee involvement**—the contribution of employees in driving diversity throughout an organization; and

- **Diversity training**—organizational efforts to inform and educate management and staff about diversity.

We reviewed GPO's diversity programs to benchmark the Agency's standing in relation to GAO's nine leading diversity management practices. The results of our review are discussed in the following section and are summarized in Appendix D.

1. Top Leadership Commitment

A commitment of top leadership is the first leading practice that GAO identifies in its January 2005 report. That practice requires that the head of an agency and other senior officials commit themselves to diversity by incorporating the principles of EEO into an agency's organizational structure. The Public Printer issued a policy statement to all GPO employees on April 8, 2008, emphasizing his personal commitment to equal opportunity and diversity. (See Appendix E for the complete text of that statement). While the current Public Printer issued a signed policy statement to employees at the beginning of his tenure as Public Printer, over three years had elapsed since the previous Public Printer issued his statement on February 1, 2005. As previously recommended, the Public Printer should follow MD-715 guidance and continue to issue a signed policy statement annually to all employees addressing his commitment to diversity and EEO. This ongoing demonstration of commitment from the Public Printer is critical to the success of GPO's diversity and EEO programs.

2. Diversity as Part of an Organization's Strategic Plan

An emphasis on diversity as part of an organization's strategic plan is the second leading practice that GAO identifies in its January 2005 report. Such a practice requires an emphasis on integrating diversity management into an organization's strategic plan because it fosters a culture change that supports and values differences. Since it typically takes five to seven years to complete the initiatives of an agency's strategic plan, sustaining top leadership commitment to improvement is particularly challenging since the turnover rate for political appointees is just less than three years.[17] The Public Printer should link diversity to any future update of the Agency's Strategic Plan to ensure that EEO and diversity are considered an integral part of the agency's strategic mission.

3. Diversity Linked to Performance

The contribution that diversity plays in achieving improved individual and organizational performance is the next leading practice that GAO identifies in its January 2005 report. Diversity management makes good business sense, enhancing productivity and

[17] GAO, *High –Risk Series: Strategic Human Capital* Management, GAO-03-120 (Washington, D.C. January 2003) reported that governmentwide the average tenure of political appointees for 1990 through 2001 was just under three years.

innovation. In addition, diversity management can help reduce costs by reducing turnover, increasing employee retention across demographic groups, and improving morale. GPO should include the development of diversity management as part of its strategic plan.

4. Measurement

Quantitative and qualitative measures are vital tools in helping an agency evaluate the effectiveness of its diversity management in terms of return on investment, recruitment efforts, and retention. These tools can also help an agency compute the return on their investments in areas such as diversity training and recruiting. As previously noted, EEO officials have not been able to easily obtain workforce data to aid in such measurements. Further, the absence of written plans for attracting a supply of qualified, diverse applicants for employment, makes it difficult to measure success.

Since GPO has not implemented methods to measure or evaluate the effectiveness of the organization's diversity management, it was not possible to evaluate the return on investment for training or retraining. This type of measurement is important because it provides an agency an idea of where barriers might be that are hindering success with diversity-related goals. Although EEO officials informed us that GPO will adopt this GAO leading practice, it is our opinion that this decision should be made by the GPO Chief Human Capital Officer, who is responsible for workforce data and recruitment.

5. Accountability

Ensuring that managers maintain diversity, evaluate progress, and can manage diverse groups is the next leading practice that GAO identifies. Accountability is defined by GAO as the means to ensure that leaders are responsible for diversity by linking their performance assessment and compensation to the progress of diversity initiatives. To accomplish accountability, organizations should link ratings and compensation. The Government's Senior Executive Service corps is already held to that type of accountability—consistent with section 4313 of Title 5, which provides performance appraisal criteria for achieving EEO requirements. This accountability is also consistent with the EEOC's instructions to Federal agencies implementing MD-715.[18]

At GPO, managers and supervisors are held to core EEO commitments in order to obtain performance bonuses. As a point of interest, FY 2007 performance agreements for supervisors and the SLS corps contained a statement about EEO issues, whereas, in the FY 2008 agreements, that statement was changed. For the differences in the two agreements, see the portion below highlighted in *italics*.

[18] The instructions describe the requirement that agencies inform managers and supervisors that success and a positive evaluation will include an assessment of how that manager contributes to the agency's EEO program by emphasizing to managers and supervisors that equality of opportunity is essential to attracting, developing, and retaining the most qualified workforce, with such a workforce being essential to ensuring the agency's achievement of its strategic mission.

FY 2008 Performance Agreement

I will make decisions in areas such as hiring, training, awards, special projects and developmental assignments without regard to sex, race, color, religion, national origin, age, disability, sexual orientation, or reprisal. I will conduct myself in accordance with all applicable legal and ethical standards of behavior and will assist on and enforce these standards within my organization. In the event that the above core commitment is not being met, the supervisor's rater must immediately provide guidance and advice to address any performance-related problems.

FY 2007 Performance Agreement

I will make decisions in areas such as hiring, training, awards, special projects and developmental assignments without regard to sex, race, color, religion, national origin, age, disability, sexual orientation, or reprisal *in order to nurture talent, create diverse opportunities and maximize the potential of GPO's workforce. I will promote staff participation in EEO events and programs. I will work with EEO to address and resolve allegations of discrimination and/or harassment within my organization.*

EEO officials stated that no decision had been made to adopt this practice although Human Capital officials stated that the draft EEO core commitment for FY 2009 performance agreements would be similar to the previous FY 2007 core commitment. We recommend that the agency adopt core commitments that emphasize the value of creating a diverse workforce and address the culture of diversity as opposed to mere compliance with laws and regulations.

6. Succession Planning

Succession planning is the sixth leading practice that GAO identifies in its January 2005 report. Succession planning is tied to the Federal Government's opportunity to change the diversity of the executive corps through new appointments and is a comprehensive, ongoing strategic process that enables management to forecast an organization's leadership needs. Identifying and developing candidates who have the potential to be future leaders, and selecting individuals from among a diverse pool of qualified candidates to meet executive resource needs is at the heart of succession planning.

As Table 4 shows, in the last five years GPO has made significant progress in the overall diversity of its workforce. Specifically, in FY 2002, there were 32 Grade 15s consisting of 31 males (6 minorities) and one female (0 minorities). In FY 2007, there were 56 males (14 minorities) and 23 females (11 minorities).

Table 4. 5-Year Trend Grade 15 (PG-15) Employees

Fiscal Year	**2002**		**2007**	
Males	**Number**	**Percent**	**Number**	**Percent**
White	25	78.2	42	53.1
African American	5	15.6	11	13.9
Asian American/Pacific Islander	1	3.1	1	1.3
Hispanic American	0	0.0	1	1.3
Native American	0	0.0	1	1.3
Total Males	**31**	**96.9**	**56**	**70.9**
Females				
White	1	3.1	12	15.2
African American	0	0.0	6	7.6
Asian American/Pacific Islander	0	0.0	5	6.3
Hispanic American	0	0.0	0	0.0
Native American	0	0.0	0	0.0
Total Females	**1**	**3.1**	**23**	**29.1**
Overall Totals	**32**	**100.0**	**79**	**100.0**

The result of the progress GPO has made in their succession planning has affected the makeup of its SLS employees. As shown in Table 5 below, in FY 2002, there were 21 SLS employees consisting of 20 males (0 minorities) and one female (1 minority). In FY 2007, there were a total of 26 SLS employees consisting of 23 males (1 minority) and 3 females (2 minorities).

Table 5. 5-Year Trend Senior Level Service (SLS) Employees

Fiscal Year	**2002**		**2007**	
Males	**Number**	**Percent**	**Number**	**Percent**
White	20	95.2	22	84.6
African American	0	0.0	0	0.0
Asian American/Pacific Islander	0	0.0	0	0.0
Hispanic American	0	0.0	1	3.9
Native American	0	0.0	0	0.0
Total Males	**20**	**95.2**	**23**	**88.5**
Females				
White	0	0.0	1	3.8
African American	1	4.8	2	7.7
Asian American/Pacific Islander	0	0.0	0	0.0
Hispanic American	0	0.0	0	0.0
Native American	0	0.0	0	0.0
Total Females	**1**	**4.8**	**3**	**11.5**
Overall Totals	**21**	**100.0**	**26**	**100.0**

Another way GPO supports succession planning is through leadership programs. A new program at GPO is called the Leadership, Development, and Recruitment (LDR) program. The LDR program—a two-year career-building program—began in FY 2007. As part of the LDR program, employees are recruited from both inside and outside the Agency. The program allows employees to work in a number of business units to get a range of hands-on experience of GPO to become potential future leaders within those same business units. In FY 2007, there were 13 employees—8 males (4 minorities) and 5 females (3 minorities)—enrolled in the LDR program. The second LDR class began in June 2008 with seven employees—five males and two females (1 minority). Table 6 provides more detail on the makeup of these two classes.

Table 6. Leadership Development and Recruitment (LDR) Program Employees

Fiscal Year	**2007**		**2008**	
Males	**Number**	**Percent**	**Number**	**Percent**
White	4	30.8	5	71.4
African American	3	23.0	0	0.0
Asian American/Pacific Islander	0	0.0	0	0.0
Hispanic American	1	7.7	0	0.0
Native American	0	0.0	0	0.0
Total Males	**8**	**61.5**	**5**	**71.4**
Females				
White	2	15.4	1	14.3
African American	3	23.1	1	14.3
Asian American/Pacific Islander	0	0.0	0	0.0
Hispanic American	0	0.0	0	0.0
Native American	0	0.0	0	0.0
Total Females	**5**	**38.5**	**2**	**28.6**
Overall Totals	**13**	**100.0**	**7**	**100.0**

Although GPO can still improve the diversity of its SLS corps with the inclusion of Asian American/Pacific Islanders, Hispanic Americans, and Native Americans, in the last five years, GPO has worked to create a diverse pool of qualified candidates for future SLS positions at both the Grade 15 level and through implementation of the LDR program.

7. Recruitment

Attracting a supply of qualified, diverse applicants for employment is the next leading practice listed by GAO. GAO states that organizations can widen selection of schools from which they can recruit to include, for example, Historically Black Colleges and Universities, Hispanic-Serving Institutions, women's colleges, and schools with international programs. Because of the number of Federal employees, including those in

senior level positions eligible for retirement in the next decade, the Federal Government will need more midcareer employees, defined by the GAO as employees generally 40 and older with 10 or more years of work experience.

In 2006, GPO hired a Recruitment Manager who worked with GPO managers including EEO and established a plan to recruit diverse candidates for a number of positions including the LDR Program. The Recruitment Manager along with other recruiters visited Historically Black Colleges and Universities and Hispanic-Serving Institutions. In addition, the manager used his personal contacts to generate renewed interest in GPO. A similar plan created in coordination with the EEO Manager is in place for 2008/2009. Also, the Hispanic Employment Program Manager e-mails job vacancies to 67 Hispanic organizations and to more than 800 Hispanic Employment Network individuals. Finally, significant recruitment planning, efforts and advertising took place in order to find diverse candidates to fill the positions at GPO's Secure Production Facility (SPF) in Mississippi. However, such efforts by Human Capital and EEO may not be fully realized in the absence of participation by the business unit managers making the employment selections. Accordingly, we recommend that the business unit managers responsible for employment selection and recruiting be included in outreach and recruitment efforts.

8. Employee Involvement

Employee involvement is GAO's eighth practice. Involving employees in diversity management helps contribute to diversity throughout the organization. Employees can get involved by: (1) forming employee diversity task forces, councils, boards, and networks to identify issues, recommend actions, and help develop initiatives to facilitate change; (2) providing mentoring opportunities to help identify and develop high-potential employees, improve employee productivity and performance, and promote retention and diversity; and (3) encouraging employees to volunteer in their communities and allocating mission personnel to participate in community outreach programs with private employers, public schools, and universities.

In its report, GAO provides an example of an agency that established a diversity advisory board and provided a visible forum for independent advice and assistance to management officials on diversity-related plans, policies, and programs. The same agency also created an advisory council chaired by a senior manager. The two groups contributed to the diversity strategic plan which was adopted by agency management. The diversity strategic plan had the following four objectives:

- Increased awareness of diversity values and sensitivities by senior management, managers, and staff.

- Retention of existing diversity and work-life enhancement.

- Active promotion of outreach and creation of a visible network of connections or routes to the agency.

- Recruitment and workforce planning for enhanced diversity.

GPO has several diverse employee groups such as the Federal Women's Program, Hispanic Employment Program, and the Disability Committee. These groups help identify issues and recommend actions to GPO management. These groups could also aid GPO management in the development of initiatives and recommendations for a diversity strategic plan similar to that identified in the GAO report.

In another effort to enhance employee involvement, the AEP Manager introduced GPO's Employee Mentoring Program in April 2008. The program is a formal six-month pilot with 11 mentors and protégés and is designed to enhance employee retention, job satisfaction, and cross-organizational communication through employees receiving teaching, guidance, counseling, and coaching from other GPO employees.

GPO also has very active employee involvement. As the GAO report emphasizes, employees should be empowered to address and identify diversity issues, recommend actions, and help develop initiatives to address concerns and create greater cultural and diversity awareness in the workplace for all employees. We recommend that GPO management evaluate its existing employee groups, identify whether employees' issues are fully represented and ensure that the groups are meeting the objectives as identified by GAO.

9. Diversity Training

GAO's ninth practice of training can help an organization's management and staff increase their awareness and understanding of diversity as well as help it develop concrete skills for assisting it with communicating and increasing productivity. Training can provide employees with an awareness of their differences—including cultural, work style, and personal presentation-and an understanding of how diverse perspectives can improve organizational performance. GAO also states that to increase employee effectiveness in a diverse environment, training should include teambuilding, communication styles, decision-making, and conflict resolution.

EEO officials informed us that GPO plans to adopt this leading practice. The OIG believes that officials from both EEO and Human Capital should work together to develop a diversity training curriculum that can be provided to all GPO employees.

Recommendation

2. The Public Printer should adopt all or a combination of the leading practices GAO recommends to create and maintain a positive work environment with qualified and diverse senior officials by taking the following steps:

    a. Continue to issue to all employees an annual policy statement on his personal commitment to equal opportunity and diversity.

b. Link diversity to GPO's strategic plan.
c. Include the development of diversity management in its strategic plan.

d. Develop a data gathering and tracking system for workforce data that will help the agency eliminate identified barriers.

e. Develop a written plan for attracting a supply of qualified, diverse applicants for employment, identifying quantitative and qualitative performance measures that can track data on its workforce to evaluate the effectiveness of the Agency's diversity management efforts as well as track the return on investment in such areas as diversity training and recruitment.

f. Ensure that managers are responsible for diversity in their business units and that awards are based partly on a manager's success in achieving diversity-related goals.

g. Identify, develop, and select candidates for new appointments who have the potential to be future leaders from a diverse pool of qualified candidates.

h. Empower employees to get involved in diversity management by forming employee task forces, councils, and boards that identify issues and recommend actions to the diversity strategic plan.

i. Develop a diversity training program for managers and employees that increases awareness and understanding of diversity as well as help develop concrete skills to assist in communicating and increasing productivity.

Management's Response. Concur. Implementation of the recommendation will require the Public Printer's review and approval (see Appendix J).

Evaluation of Management's Response. While GPO management concurred with the recommendation, they did not provide details regarding what actions the Agency plans to take to implement the recommendation. As a result, pending receipt of details related to implementation, the recommendation is considered unresolved. The OIG will work with GPO management to review any proposed actions to implement the recommendation.

Appendix A. Objectives, Scope, and Methodology

Objectives

The overall objective of the audit was to conduct a review of the diversity office within the GPO at the request of the Subcommittee on Federal Workforce, Postal Service, and the District of Columbia, Committee on Oversight and Government Reform, House of Representatives. The Subcommittee expressed concern about the under representation of women and minorities in the senior-level positions at the legislative branch agencies. The GPO OIG was one of five legislative branch agencies jointly conducting this review. The other legislative branch agencies participating in the review are the Library of Congress, Government Accountability Office, Architect of the Capitol, and U.S. Capitol Police. Participating agencies will issue a consolidated report to Congress by September 2008.

The specific audit objectives were to:

- Identify and assess the diversity program at GPO to determine if it is yielding the desired results, that of creating a more diverse population of women and minorities in top leadership positions (SLS).

- Evaluate the accuracy and completeness of the complaints and discrimination data being reported to the Congress.

- Assess to what degree the diversity offices are independent of the GPO's General Counsel and the Public Printer

Scope and Methodology

To be consistent in our scope and methodology in reporting each particular agency's position to the three specific objectives, we followed a uniform audit guide provided to each participating OIG by the Library of Congress OIG. To address the audit objectives, we:

1. Assessed the responses that the EEO Director provided in the: (1) Self-Assessment Checklist in MD-715 which identifies the effectiveness of the GPO diversity programs; and (2) Data Collection Instrument for Leading Diversity Management Practices which gauges the agency's progress in following leading diversity management practices as of January 1, 2008.

2. Evaluated the accuracy and completeness of GPO's complaint and discrimination data for Fiscal Year 2007.

3. Assessed the current independence of GPO's EEO Director and the diversity programs with the Public Printer and GPO's General Counsel.

We also interviewed officials from the Offices of the General Counsel and Human Capital to determine whether policies and procedures related to EEO were implemented and followed. Human Capital officials also provided workforce profile reports and documentation on recruiting applicants for Agency leadership programs.

Management Controls Reviewed

We reviewed management controls related to EEO areas, including complaint and discrimination reports as well as the reporting of data for workforce profile reports to ensure these practices are contained in GPO Instruction 825.18A.

Audit Field Work

We performed field work from April through August 2008 at the GPO Central Office in Washington, D.C. We performed the audit in accordance with generally accepted government auditing standards.

Appendix B. Assessment of Whether GPO Practiced the Essential Elements of EEOC Management Directive 715

	Essential Element	Generally Following	Not Following
1.	Demonstrated Commitment from Leadership	X	
2.	Integration of EEO into the Strategic Mission		X[19]
3.	Management and Program Accountability		X[20]
4.	Proactive Prevention		X[21]
5.	Efficiency	X	
6.	Responsiveness and Legal Compliance	X	

[19] Although GPO followed the four parts of Element B, the previous strategic plan did not address EEO.
[20] Although GPO followed portions of Element C, it did not include the portions for business unit managers developing EEO plans and EEO and Human Capital officials identifying any systemic barriers in past promotions, training, and awards.
[21] Because the data that Human Capital official provided was limited, the AEP Program Manager could not conduct an annual self-assessment to monitor the progress and identify areas where barriers may operate to exclude certain groups.

Appendix C. White and Blue Collar Workforce Profile by Grade, Race, and Sex (As of January 28, 2008)

Grade	Total Employees			White		Black		Hispanic		Asian / Pacific Islander		American Indian	
WHITE COLLAR WORKFORCE													
	All	Men	Women	Men	Women	Men	Women	Men	Women	Men	Women	Men	Women
SLS	26	23	3	22	1		2	1					
15	79	56	23	42	12	11	6	1		1	5	1	
14	95	60	35	46	24	8	10	3	1	3			
13	207	108	99	69	54	28	39	2	1	8	4	1	1
12	303	128	175	79	72	45	91		2	4	8		2
11	80	28	52	17	12	9	38	2	1		1		
10	4	1	3				3	1					
9	77	20	57	10	13	9	43			1			1
8	15	1	14		2	1	12						
7	95	15	80	8	19	6	56	1	3		2		
6	60	12	48	2	7	8	40	1	1	1			
5	91	49	42	13	10	31	29	5	3				
4	13	4	9	2	6	2	3						
3	8	6	2	2	2	4							
2	4	3	1	1	1	2							
0	6	4	2	2	2	1				1			
Subtotal	**1163**	**518**	**645**	**315**	**237**	**165**	**372**	**17**	**12**	**19**	**20**	**2**	**4**
BLUE COLLAR WORKFORCE													
Subtotal	**1100**	**789**	**311**	**296**	**57**	**473**	**250**	**9**		**7**	**4**	**4**	
GPO #	**2263**	**1307**	**956**	**611**	**294**	**638**	**622**	**26**	**12**	**26**	**24**	**6**	**4**

Source: GPO Office of Human Capital

Appendix D. Assessment of Whether GPO Exemplifies GAO's Leading Practices for Diversity Management

	Leading Diversity Practices[22]	Not Yet Adopted					Level of Adoption	
		Do not anticipate adopting	No decision	Will adopt	Plan under development	Written plan complete	Partially adopted	Fully adopted
1.	**Top leadership commitment –** a vision of diversity demonstrated and communicated throughout an organization by top-level.						X[23]	
2.	**Diversity as part of an organization's strategic plan –** a diversity strategy and plan that are developed and aligned with the organization's strategic plan.		X					
3.	**Diversity linked to performance –** the understanding that a more diverse and inclusive work environment can yield greater productivity and help improve individual and organizational performance.		X					
4.	**Measurement –** a set of quantitative and qualitative measures of the impact of various aspects of an overall diversity program.		X					
5.	**Accountability –** the means to ensure that leaders are responsible for diversity by linking their performance assessment and compensation to the progress of diversity initiatives.		X					
6.	**Succession planning –** an ongoing, strategic process for identifying and developing a diverse pool of talent for an organization's potential future leaders.				X[24]			
7.	**Recruitment –** the process of attracting a supply of qualified, diverse applicants for employment.		X					
8.	**Employee involvement –** the contribution of employees in driving diversity throughout an organization.		X					
9.	**Diversity training –** organizational efforts to inform and educate management and staff about diversity.		X					

[22] GAO report GAO-05-09, "Diversity Management Expert-Identified Leading Practices and Agency Examples," January 2005.

[23] Based on the Public Printer's April 8, 2008, letter on equal opportunity and diversity.

[24] The Human Capital Office did not have a written plan. However, GPO has made progress in the last five years to create a diverse pool of qualified candidates at the Grade 15 level and the implementation of the LDR program.

Appendix E. Public Printer's April 8, 2008 Letter on Equal Opportunity and Diversity

GPO U.S. GOVERNMENT PRINTING OFFICE
KEEPING AMERICA INFORMED

Robert C. Tapella
Public Printer

April 8, 2008

To All GPO Employees:

As Public Printer I want to emphasize my personal commitment to equal opportunity and diversity. It is imperative that we treat fairly all employees, applicants for employment, and customers of the U.S. Government Printing Office (GPO). Employment actions must be based upon merit principles and made without regard to an individual's race, color, religion, national origin, sex, age, mental/physical disability or sexual orientation.

Since becoming Public Printer at GPO, I have made it clear that I will not tolerate any form of discrimination in the workplace. I firmly believe that every GPO employee is entitled to work in an environment that is free of discrimination and harassment. I am committed to ensuring that every individual in GPO enjoys that right without regard to non-merit factors. This environment is necessary for accomplishing our goal of attracting, hiring, developing and retaining a quality diverse workforce that achieves our mission and meets the expectations of our citizens and the visitors we serve.

It is the policy of GPO to provide equal employment opportunity for all persons in its workforce, as well as applicants for employment and to prohibit discrimination in all aspects of its personnel policies, program practices and operations. Every GPO manager and supervisor is responsible for ensuring that we achieve that goal. I expect a "zero tolerance" approach to this important area. I take any confirmed violations of this policy very seriously. Employees who violate the law will be held accountable for their conduct. I encourage every level of management to maintain a high level of awareness regarding these matters and to foster a steadfast commitment to equal opportunity for all persons. I expect managers and supervisors to respond to complaints swiftly and appropriately, as they will be held accountable for taking steps to eliminate such behavior and to ensure that the work environment is one where employees are treated fairly, respectfully and with dignity.

As Public Printer, I will vigorously pursue these goals and I encourage all employees to fully support our commitment in principle and in action to ensure that our equal employment opportunity programs are successful. Each of you plays a part in creating and sustaining a workplace that will provide all employees with a working environment free from discrimination where individual differences are respected and valued.

Sincerely,

732 North Capitol Street, NW Washington, DC 20401 202-512-1000 rtapella@gpo.gov

Appendix F. Summary of Leading Practices GPO Followed (From PricewaterhouseCoopers[25] Study and EEOC Management Directive 715[26])

	Diversity Program Characteristics	Following	Generally Following	Not Following
1.	Diversity Program housed separate from the EEO office?			X
2.	Agency has a diversity action or strategic plan?			X
3.	Agency is conducting targeted recruitment and outreach efforts to attract potential under represented minority employees?		X	
4.	Mentoring Program?	X		
5.	Includes awareness events (for example, special emphasis functions)?	X		
6.	Includes a diversity council?			X
7.	Agency encourages the development of formally or informally constituted groups representing specific categories of employees such as women, African Americans, or gays and lesbians?		X	
8.	Includes focus on conflict management (for example, alternative dispute resolution or mediation)?	X		
9.	Diversity training required for managers and supervisors?			X
10.	Diversity training included in employee orientation?			X
11.	Have administered attitude survey as part of assessment?	X		
12.	Diversity element in supervisors/managers performance plans?			X
13.	Are management/personnel policies, procedures and practices examined at regular intervals to assess whether there are hidden impediments to equal opportunity?		X	
14.	Does the EEO Director have the authority and funding to ensure implementation of agency EEO action plans?	X		
15.	The agency tracks the race, national origin and sex of applicants for both permanent and temporary employment?			X
16.	The agency tracks the rates of selections for promotions by race, national origin and sex?			X
17.	The agency tracks the rates of training opportunities (hours per year) by race, national origin and sex?			X
18.	The agency tracks the rates of performance incentives (monetary awards, step increases) by race, national origin and sex?			X
19.	The agency tracks the rates of complaints by race, national origin and sex to see if a particular group has more complaints about promotions, disciplinary actions, performance appraisals, or awards?	X[27]		
20.	The agency tracks the rates of both voluntary and involuntary separations from employment by race, national origin and sex?			X

[25] "A Changing Workforce: Understanding Diversity Programs in the Federal Government" December 2001.
[26] This table will be included in the consolidated report of the five Legislative Branch agencies to Congress.
[27] The EEO Office uses this information in their semiannual meetings with business units that began in October 2007.

Appendix G. Accuracy and Completeness of EEO Data[28]

Tracking and Reporting the Number and Status of Discrimination Complaints

GPO's EEO Office uses EEONET, a case management system built to assist EEO managers and counselors in managing all aspects of information and program management related to EEO complaints and resolutions. Built to support the EEOC reporting requirements, EEONET allows automated generation of reports required by EEOC as well as a variety of other reports and documentation that can be customized to user and management requirements. The data in EEONET are supported by the manual files kept as well as a monthly report that is kept to ensure the data is accurate when it is entered into the system. GPO's EEO office is required to submit annually EEOC Form 462 report. EEOC incorporates the data along with the other agencies and report it to Congress. Although the format between "No Fear Act" and EEOC's 462 are somewhat different, the data collected are the same. One key difference is that the "No Fear Act" reporting reflects comparative data for the previous 5 years; EEOC Form 462 report includes activity that occurred during the preceding fiscal year.

No.	Discrimination Complaints	Yes	No
1	Does the agency have a system of management controls in place to ensure the timely, accurate, complete and consistent reporting of EEO complaint data?	X	
2	Does the agency use a complaint tracking system that allows identification of the location and status of complaints, and length of time elapsed at each stage of the agency's complaint resolution process?	X	
3	Does the agency's tracking system identify the issues and bases of the complaints, the aggrieved individuals/complainants, the involved management officials and other information to analyze complaint activity and trends?	X	
4	Is the agency statutorily mandated to follow the No Fear Act reporting requirements?		X
4a	Does the agency follow the No Fear Act reporting format?		X
4b	Does the agency post its No Fear Act (or similar) data on its web site?		X

[28] This table will be included in the consolidated report of the five Legislative Branch agencies to Congress.

Appendix H. Independence of the Diversity Office[29]

Independence

No.		Yes	No
1	Has the agency placed the EEO Director in a direct reporting relationship with the head of the agency?	X	
2	Does the EEO Director have a regular and effective means of informing the agency head and other top management officials of the effectiveness, efficiency and compliance (with agency regulations or EEOC Directives, if applicable) of the agency's EEO program?	X	
3	Is the EEO investigative and decision making process separate from the personnel function?	X	
4	Are the legal sufficiency reviews done by a unit separate from the personnel function?	X	
5	Does the agency offer Alternative Dispute Resolution or mediation?	X	

[29] This table will be included in the consolidated report of the five Legislative Branch agencies to Congress.

Appendix I. Acronyms Used in the Report

AEP	Affirmative Employment Program
CCPD	Counseling and Complaints Processing Division
EEO	Equal Employment Opportunity
EEOC	Equal Employment Opportunity Commission
EEONET	Equal Employment Opportunity Network
FWP	Federal Women's Program
FY	Fiscal Year
GAO	Government Accountability Office
GEM	GPO Employee Mentoring Program
GPO	Government Printing Office
GS	General Schedule
HEP	Hispanic Employment Program
LDR	Leadership, Development, and Recruitment Program
MD	Management Directive
OIG	Office of Inspector General
PG	Printing Office Grade
SES	Senior Executive Service
SLS	Senior Level Service

Appendix J. Management's Response

U.S. GOVERNMENT PRINTING OFFICE
KEEPING AMERICA INFORMED

memorandum

DATE: September 10, 2008

REPLY TO ATTN OF: Director, Equal Employment Opportunity

SUBJECT: Revised Draft Report on Audit of Diversity Management Programs at the GPO

TO: Assistant IG for Audits and Inspection

This is in response to your memorandum dated September 9, 2008, requesting comment on the above subject report. I fully concur with the recommendations outlined in the above subject report. However, it would require the Public Printer's review and approval before implementation.

Please contact me or Juanita M. Flores at (202) 512-2014 if you have any questions.

Juanita M. Flores

NADINE L. ELZY

U.S. GOVERNMENT PRINTING OFFICE
KEEPING AMERICA INFORMED
WASHINGTON, DC 20401

Memorandum

HUMAN CAPITAL OFFICE

DATE: September 10, 2008

REPLY TO
ATTN OF: Chief Human Capital Officer

SUBJECT: Draft Report on Audit of Diversity Management Programs at the GPO

TO: Assistant IG for Audits and Inspection

This is in response to your September 9, 2008 memorandum requesting comments on the revised draft report on the Audit of Diversity Management Program at the GPO. After a thorough review, we note that the changes made as a result of the September 5 meeting between the IG, EEO and Human Capital managers have greatly improved the report.

As far as the two recommendations are concerned, our office concurs with each of them. Thank you for the opportunity to review the draft. I am sure the report will have a positive impact to create a more diverse GPO in the future.

William T. Harris

Appendix K. Status of Recommendations

Recommendation No.	Resolved	Unresolved	Open/ECD*	Closed
1		X		
2		X		

*Estimated Completion Date.

Appendix L. Report Distribution

Government Printing Office

Deputy Public Printer
Chief of Staff
Chief Management Officer
Chief Financial Officer
Chief Information Officer
Chief Technology Officer
Director, Congressional Relations
Director, Library Services and Content Management
Director, Public Relations
Director, Publication and Information Sales
General Counsel
Managing Director, Customer Services
Managing Director, Official Journals of Government
Managing Director, Plant Operations

Major Contributors to the Report

Joseph J. Verch Jr., Supervisory Auditor

United States Government Accountability Office

GAO

Report to the Ranking Member, Committee on Financial Services, U.S. House of Representatives

April 2013

DIVERSITY MANAGEMENT

Trends and Practices in the Financial Services Industry and Agencies after the Recent Financial Crisis

GAO-13-238

April 2013

DIVERSITY MANAGEMENT

Trends and Practices in the Financial Services Industry and Agencies after the Recent Financial Crisis

GAO Highlights

Accountability * Integrity * Reliability

Highlights of GAO-13-238, a report to the Ranking Member, Committee on Financial Services, U.S. House of Representatives

Why GAO Did This Study

As the U.S. workforce has become increasingly diverse, many private- and public-sector entities recognize the importance of recruiting and retaining minorities and women for management-level positions to improve their business. The 2007-2009 financial crisis has renewed questions about commitment within the financial services industry (e.g., banking and securities) to workforce diversity. The Dodd-Frank Act required that eight federal financial agencies and the Federal Reserve Banks implement provisions to support workforce and contractor diversity. GAO was asked to review trends and practices since the beginning of the financial crisis. This report examines (1) workforce diversity in the financial services industry, the federal financial agencies, and Reserve Banks, from 2007 through 2011 and (2) efforts of the agencies and Reserve Banks to implement workforce diversity practices under the Dodd-Frank Act, including contracting. GAO analyzed federal datasets and documents and interviewed industry representatives and officials from the federal financial agencies and Reserve Banks.

What GAO Recommends

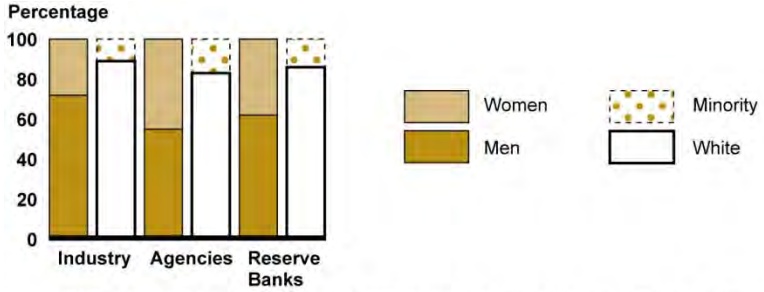
Each agency and Reserve Bank should include in its annual OMWI report to Congress efforts to measure the progress of its diversity practices. The agencies and Reserve Banks agreed to include this information in the annual OMWI reports. Additionally, some agencies and the Reserve Banks described steps they have taken or plan to take to address the recommendation.

View GAO-13-238. For more information, contact Daniel Garcia-Diaz at (202) 512-8678 or GarciaDiazD@gao.gov.

What GAO Found

Management-level representation of minorities and women in the financial services industry and among federal financial agencies and Federal Reserve Banks (Reserve Banks) has not changed substantially from 2007 through 2011. Industry representation of minorities in 2011 was higher in lower-level management positions—about 20 percent—compared to about 11 percent of senior-level manager positions. Industry representation of women at the overall management level remained at about 45 percent. Agency representation of minorities at the senior management level in 2011 ranged from 6 percent to 17 percent and from 0 percent to 44 percent at the Reserve Banks. Women's representation ranged from 31 to 47 percent at the agencies and from 15 to 58 percent at the Reserve Banks. Officials said the main challenge to improving diversity was identifying candidates, noting that minorities and women are often underrepresented in both internal and external candidate pools.

Senior Management-Level Diversity, 2011



Source: GAO analysis of financial services industry EEOC data and agency and Reserve Bank reports.

In response to the requirements in the Dodd-Frank Wall Street and Consumer Protection Act (Dodd-Frank Act), in 2011 federal financial agencies and Reserve Banks began to report annually on the recruitment and retention of minorities and women and other diversity practices. They all have established Offices of Minority and Women Inclusion (OMWI) as required. Many agencies and Reserve Banks indicated they had recruited from minority-serving institutions and partnered with organizations focused on developing opportunities for minorities and women, and most described plans to expand these activities. Some used employee surveys or recruiting metrics to measure the progress of their initiatives, as suggested by leading diversity practices, but OMWIs are not required to include this type of information in the annual reports to Congress. Better reporting of measurement efforts will provide Congress, agency officials, and other stakeholders additional insights on the effectiveness of diversity practices and demonstrate how agencies and Reserve Banks are following a leading diversity practice. Most federal financial agencies and Reserve Banks are in the early stages of implementing the contracting requirements required under the act. For example, most now include a provision in contracts for services requiring contractors to make efforts to ensure the fair inclusion of women and minorities in their workforce and subcontracted workforce and have established ways to evaluate compliance. The proportion of an agency's dollars awarded or a Reserve Bank's dollars paid to minority- or woman-owned businesses reported in 2011 OMWI reports ranged between 3 percent and 38 percent.

Contents

Tables

Figures

Abbreviations

AACSB	Association to Advance Collegiate Schools of Business
CFPB	Bureau of Consumer Financial Protection, known as the Consumer Financial Protection Bureau
CPS	Current Population Survey
Dodd-Frank Act	Dodd–Frank Wall Street Reform and Consumer Protection Act
EEO	equal employment opportunity
EEO-1	Employer Information Report
EEOC	Equal Employment Opportunity Commission
FAR	Federal Acquisition Regulation
FDIC	Federal Deposit Insurance Corporation
Federal Reserve Board	Board of Governors of the Federal Reserve System
FHFA	Federal Housing Finance Agency
FSOC	Financial Stability Oversight Council
HERA	Housing and Economic Recovery Act of 2008
MWOB	minority- and women-owned business
MBA	Master of Business Administration
MD-715	EEOC Management Directive 715
NAICS	North American Industry Classification System
NCUA	National Credit Union Administration
NPO	National Procurement Office
OCC	Office of the Comptroller of the Currency
OMWI	Office of Minority and Women Inclusion
Reserve Banks	Federal Reserve Banks
SBA	Small Business Administration
SBS	security-based swap
SEC	Securities and Exchange Commission
Treasury	Departmental Offices of the Department of the Treasury

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

April 16, 2013

The Honorable Maxine Waters
Ranking Member
Committee on Financial Services
House of Representatives

Dear Ms. Waters:

As the U.S. workforce has become increasingly diverse, many private and public-sector organizations have recognized the importance of recruiting and retaining minorities and women for key positions to improve their business or organizational performance. Studies have associated a diversity of perspectives in organizations with innovation. However, congressional hearings have raised questions about diversity in the workforce of the financial services industry, which provides services that are essential to the continued growth and economic recovery of the country. During hearings on the financial services industry between 2004 and 2010, congressional members and witnesses expressed concern about the level of inclusion of women and minorities in the industry, particularly in key management-level positions.[1] The 2007-2009 financial crisis has renewed concerns about commitment within the financial services industry to workforce diversity and the number of federal contracting opportunities available to minority- and women-owned businesses. The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) included provisions requiring selected federal financial agencies and Federal Reserve Banks (Reserve Banks)

[1]GAO has conducted prior work on the challenges faced in the financial sector for promoting and retaining a diverse workforce. See GAO, *Financial Services Industry: Overall Trends in Management-Level Diversity and Diversity Initiatives, 1993-2004*, GAO-06-617 (Washington, D.C.: June 1, 2006) and *Financial Services Industry: Overall Trends in Management-Level Diversity and Diversity Initiatives, 1993-2008,* GAO-10-736T (Washington, D.C.: May 12, 2010).

each to establish an Office of Minority and Women Inclusion (OMWI).[2] The act required that these agencies and Reserve Banks establish the new diversity and inclusion offices to replace existing diversity programs by January 2011 and to begin addressing a number of other requirements in the act.[3]

This report updates our previous work by discussing changes in management-level diversity or diversity practices used in this industry since the beginning of the financial crisis in 2007. It also reviews the implementation of requirements in section 342 of the Dodd-Frank Act on workforce diversity. Specifically, our objectives were to discuss (1) what available data show about how the diversity of the financial services industry workforce and how diversity practices by the industry have changed from 2007 through 2011; (2) what available data show about how diversity in the workforces of the federal financial agencies and the Reserve Banks has changed from 2007 through 2011; (3) how these federal financial agencies and Reserve Banks are implementing workforce diversity practices under section 342 of the Dodd-Frank Act, including the extent to which their workforce diversity practices have changed since the financial crisis; and (4) the status of federal financial agencies' and Reserve Banks' implementation of the contracting provisions of the Dodd-Frank Act related to the inclusion of women and minorities.

To describe how diversity in the financial services industry and how the diversity practices it uses have changed from 2007 through 2011, we analyzed 2007-2011 workforce data from the Equal Employment Opportunity Commission's (EEOC) Employer Information Report (EEO-1) and from the Current Population Survey (CPS) produced by the Bureau of

[2]Pub. L. No. 111-203 § 342,124 Stat.1376,1441-1443 (2010).The federal agencies required to meet the workforce diversity provisions in section 342 of the Dodd-Frank Act include the Departmental Offices of the Department of the Treasury (Treasury), the Federal Deposit Insurance Corporation (FDIC), the Federal Housing Finance Agency (FHFA), the Board of Governors of the Federal Reserve System (Federal Reserve Board), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), the Securities and Exchange Commission (SEC), and the Bureau of Consumer Financial Protection, commonly known as the Consumer Financial Protection Bureau (CFPB). Throughout the report we refer to these as either federal financial agencies or agencies.

[3]CFPB had until January 21, 2012, to establish its OMWI and begin addressing the other requirements of the act.

the Census and the Bureau of Labor Statistics. Through a review of documentation, electronic testing, and interviews with knowledgeable officials, we found these data sufficiently reliable for our use. We conducted a literature review to identify academic and industry studies on financial services workforce diversity, and we interviewed 10 industry representatives on these issues.

To review changes to the representation of women and minorities in the workforces of the agencies and Reserve Banks, we analyzed data the agencies submitted to EEOC from 2007 through 2011 in annual Equal Employment Opportunity Program Status Reports required by EEOC's MD-715 and analyzed EEO-1 reports provided by the 12 Reserve Banks.[4] We assessed the reliability of these data by conducting electronic testing, reviewing agency documentation, and interviewing agency officials. We determined that the data were sufficiently reliable for our use. We reviewed agency and Reserve Bank documentation of efforts to respond to the Dodd-Frank Act requirements, including annual OMWI reports to Congress. Additionally, we interviewed agency and Reserve Bank officials on changes in the inclusion of women and minorities in their workforces and any changes in the practices they used to further workforce diversity goals.

To determine the extent to which agencies and Reserve Banks are implementing the requirements of the Dodd-Frank Act regarding the inclusion of women and minorities in contracting, we reviewed annual OMWI reports submitted to Congress and interviewed officials on their efforts in this area. We collected and reviewed agency documentation of procedures developed to address the act's requirements, such as policy manuals, contract provisions related to promoting a diverse workforce, process workflows, and technical assistance materials.

We conducted this performance audit from January 2012 through April 2013 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe

[4]The race/ethnicity categories in EEOC data include White, Black, Hispanic, Asian, and other races. All non-White categories in EEOC data are considered racial/ethnic minorities in this report.

that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The financial services industry is a major source of employment in the United States. EEOC data we obtained and analyzed showed that financial services firms we reviewed for this work employed more than 2.9 million people in 2011. We defined the financial services industry to include the following sectors:

- depository credit institutions, which include commercial banks, thrifts (savings and loan associations and savings banks), and credit unions;
- holdings and trusts, which include investment trusts, investment companies, and holding companies;
- nondepository credit institutions, which extend credit in the form of loans and include federally sponsored credit agencies, personal credit institutions, and mortgage bankers and brokers;
- the securities sector, which is composed of a variety of firms and organizations that bring together buyers and sellers of securities and commodities, manage investments, and offer financial advice; and
- the insurance sector, including carriers and insurance agents that provide protection against financial risks to policyholders in exchange for the payment of premiums.

Financial Services Industry and Diversity

We previously conducted work on the challenges faced in the financial sector for promoting and retaining a diverse workforce, focusing on private-sector firms.[5] In 2010, we reported that overall diversity at the management level in the financial services industry did not change substantially from 1993 through 2008 and that diversity in senior positions was limited. We also found that without a sustained commitment among financial services firms to overcoming challenges to recruiting and retaining minority candidates and obtaining "buy-in" from key employees, limited progress would be possible in fostering a more diverse workplace.

[5]See GAO-06-617 and GAO-10-736T.

In a 2005 report, we defined diversity management as a process intended to create and maintain a positive work environment that values individuals' similarities and differences, so that all can reach their potential and maximize their contributions to an organization's strategic goals and objectives.[6] We also identified a set of nine leading diversity management practices that should be considered when an organization is developing and implementing diversity management. They are (1) commitment to diversity as demonstrated and communicated by an organization's top leadership; (2) the inclusion of diversity management in an organization's strategic plan; (3) diversity linked to performance, making the case that a more diverse and inclusive work environment could help improve productivity and individual and organizational performance; (4) measurement of the impact of various aspects of a diversity program; (5) management accountability for the progress of diversity initiatives; (6) succession planning; (7) recruitment; (8) employee involvement in an organization's diversity management; and (9) training for management and staff about diversity management.

Diversity Requirements under Section 342 of the Dodd-Frank Act

Section 342 of the Dodd-Frank Act required specific federal financial agencies and Reserve Banks each to establish, by January 21, 2011, an OMWI, responsible for matters relating to diversity in management, employment, and business activities.[7] Table 1 describes the affected agencies.

Table 1: Federal Financial Agencies Subject to Dodd-Frank Act Section 342

Agency	Function
Bureau of Consumer Financial Protection (CFPB)	Commonly known as the Consumer Financial Protection Bureau, writes rules to implement federal consumer financial law across banks and nonbanks; supervises for consumer protection purposes banks, thrifts, and credit unions with over $10 billion in assets and their affiliates, as well as nonbank mortgage-related firms, private student lenders, payday lenders, and certain other larger consumer financial companies; and enforces federal consumer financial law with respect to supervised entities and other nonbank entities.

[6]GAO, *Diversity Management: Expert-Identified Leading Practices and Agency Examples*, GAO-05-90 (Washington, D.C.: Jan. 14, 2005).

[7]Pub. L. No. 111-203. § 342, 124 Stat. 1376, 1541-1544 (2010). CFPB had until January 21, 2012, to comply with the requirements.

Agency	Function
Federal Deposit Insurance Corporation (FDIC)	Regulates FDIC-insured state-chartered banks that are not members of the Federal Reserve System, as well as federally insured state savings banks and thrifts; insures the deposits of all banks and thrifts that are approved for federal deposit insurance; and resolves all failed insured banks and thrifts and may resolve certain bank holding companies and nonbank financial companies.
Federal Housing Finance Agency (FHFA)	Supervises and regulates Fannie Mae, Freddie Mac, and the 12 Federal Home Loan Banks and their Office of Finance. Acts as conservator for Fannie Mae and Freddie Mac.
Board of Governors of the Federal Reserve System (Federal Reserve Board)	Regulates state-chartered banks that opt to be members of the Federal Reserve System, bank holding companies and certain subsidiaries, thrift holding companies, securities holding companies, Edge and agreement corporations, U.S. branches of foreign banks, any firm that is designated as systemically significant by the Financial Stability Oversight Council (FSOC), and payment, clearing, and settlement systems designated as systemically significant by FSOC, unless regulated by SEC or the Commodity Futures Trading Commission.
National Credit Union Administration (NCUA)	Charters and supervises federally chartered or insured credit unions and operates the National Credit Union Share Insurance Fund, which insures savings in federal and most state-chartered credit unions.
Office of the Comptroller of the Currency (OCC)	Charters and regulates national banks and federal thrifts and U.S. federal branches of foreign banks.
Securities and Exchange Commission (SEC)	Regulates securities exchanges, broker-dealers, investment companies, investment advisers, nationally recognized statistical rating organizations, security-based swap (SBS) dealers, major SBS participants, and SBS execution facilities.
Departmental Offices of the Department of the Treasury (Treasury)	The Department of the Treasury is organized into two major components: the departmental offices and the operating bureaus. The departmental offices are primarily responsible for the formulation of policy and management of the department as a whole, and include domestic finance, economic policy, international affairs, and others.

Source: GAO review of agency documentation.

The act's diversity provisions also apply to the Reserve Banks. The Federal Reserve System consists of a central governmental agency, the Board of Governors, in Washington, D.C., and 12 regional Reserve Banks. The 12 Reserve Banks are each responsible for a particular geographic area or district of the United States. They are located in Atlanta, Boston, Chicago, Cleveland, Dallas, Kansas City, Minneapolis, New York, Philadelphia, Richmond, San Francisco, and St. Louis. Unlike the Federal Reserve Board, the Reserve Banks are not federal agencies. Each Reserve Bank is a federally chartered corporation with a board of directors and member banks who are stockholders in the Reserve Bank. Under the Federal Reserve Act, Reserve Banks are subject to the general supervision of the Federal Reserve Board.[8]

[8]Federal Reserve Act, 63 Cong. Ch. 6, 38 Stat. 251-275 (Dec. 23, 1913).

The act's diversity provisions require the director of each OMWI to develop standards for (1) equal employment opportunity and the racial, ethnic and gender diversity of the workforce and senior management for the agency; (2) increased participation of minority- and women-owned businesses in the programs and contracts of the agency, including standards for coordinating technical assistance to such businesses; and (3) assessing the diversity policies and practices of entities regulated by the agency. It also provides that each OMWI director advise his or her agency on the impact of agency policies and regulations on minority- and women-owned businesses.[9]

The act also outlines steps the specific agencies and Reserve Banks should take to seek workforce diversity at all levels of their organizations. Among other things, these steps include recruiting from colleges serving primarily minority populations, sponsoring and recruiting at job fairs in urban communities, and advertising positions in newspapers and magazines oriented toward minorities and women.

In addition, the act provides that each OMWI director develop and implement standards and procedures to ensure, to the maximum extent possible, the fair inclusion and utilization of minorities, women, and minority- and women-owned businesses in all business and activities of the agency at all levels, including in procurement, insurance, and all types of contracts. Agency procedures for reviewing and evaluating applicable contract proposals and for hiring service providers should include a component that gives consideration to applicant diversity, to the extent consistent with applicable laws.[10] Additionally, the act mandates that the

[9]For purposes of the act, minority means any Black American, Native American, Hispanic American, or Asian American. Minority-owned business means a business (i) more than 50 percent of the ownership or control of which is held by one or more minority individuals; and (ii) more than 50 percent of net profit and loss of which accrues to one or more minority individuals. Women-owned business means a business (i) more than 50 percent of the ownership or control of which is held by one or more women; (ii) more than 50 percent of the new profit or loss of which accrues to one or more women; and (iii) a significant percentage of senior management positions are held by women.

[10]Section 342 applies to all contracts of an agency for services of any kind, including the services of financial institutions, investment-banking firms, mortgage banking entities, underwriters, accountants, investment consultants, and providers of legal services. It also includes all contracts for all business and activities of an agency, at all levels, including contracts for the issuance or guarantee of any debt, equity, or security; the sale of assets; the management of assets of the agency; the making of equity investments by the agency; and the implementation of programs to address economic recovery.

OMWI director develop procedures to determine whether contractors, or subcontractors when applicable, have made a good faith effort to include minorities and women in their workforces. It requires that each OMWI director recommend that contracts be terminated if they determine that an agency contractor, and as applicable, a subcontractor has failed to make a good faith effort to include minorities and women in their workforce. Upon receipt of such a recommendation, the head of an agency may terminate the contract, make a referral to an office in the Department of Labor, or take other appropriate action.

Finally, the act requires each OMWI to submit to Congress an annual report detailing the actions taken by the agency and the OMWI to comply with the provisions in section 342. The annual reports are required to include, among other things, annual amounts paid to contractors, including the percentage of the amounts that were paid to minorities, women, and minority- and women-owned businesses; any challenges in contracting with qualified minority- and women-owned businesses; any challenges in hiring qualified minority and women employees; and any other information, findings, conclusions, and recommendations for legislative or agency action as the OMWI director determines appropriate.

Industry Diversity Levels Remained about the Same from 2007 through 2011

Diversity has remained about the same at the management level in terms of the representation of both minorities and women, while industry representatives noted the continued use of leading diversity practices and some challenges. According to EEOC data, the representation of minorities at the management level stood at 19 percent in 2011. The representation of women in management remained at about 45 percent, according to EEOC data. The nine leading diversity practices that we previously identified in 2005 remain relevant today, according to industry representatives with whom we spoke. Industry representatives also noted some challenges, such as the difficulty in recruitment because of a limited supply of diverse candidates.

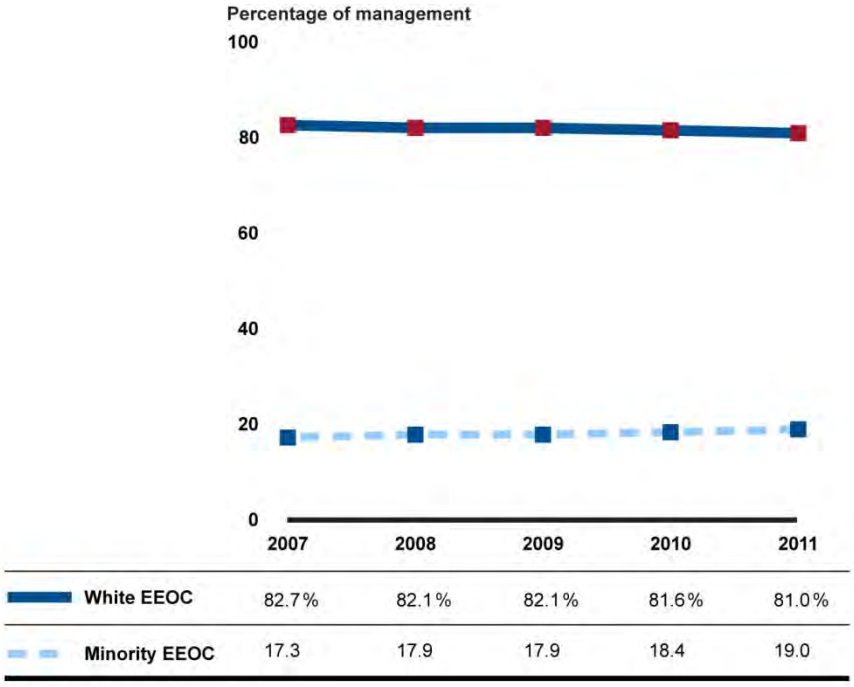
Diversity in the Financial Services Industry Remained about the Same at the Management Level from 2007 through 2011

At the overall management level, the representation of minorities increased from 17.3 percent to 19 percent from 2007 through 2011 according to EEOC data we obtained, which are reported by financial services firms (see fig. 1).[11] While this is not a substantial increase, it shows a continued upward trend from our 2006 report, in which data showed that management-level representation by minorities increased from 11.1 percent to 15.5 percent from 1993 through 2004.[12]

[11]EEOC compiles EEO-1 data from the reports it collects annually from private employers with 100 or more employees or federal contractors with 50 or more employees. Similar to our 2006 report, we obtained data from EEOC for private employers with 100 or more employees. Consequently, the analysis included in this report may not match the analysis found in EEOC's website, which would also include federal contractors with 50 or more employees. The financial services industry EEO-1 data analysis provided in this section of the report includes workforce information from the 12 Federal Reserve Banks, as they are considered part of the financial services industry. We provide a separate analysis of the 12 Federal Reserve Banks' workforce later in the report because they were also covered by the Dodd-Frank Act provisions.

[12]GAO-06-617.

Figure 1: Percentage of White and Minority Managers in the Financial Services Industry, 2007-2011

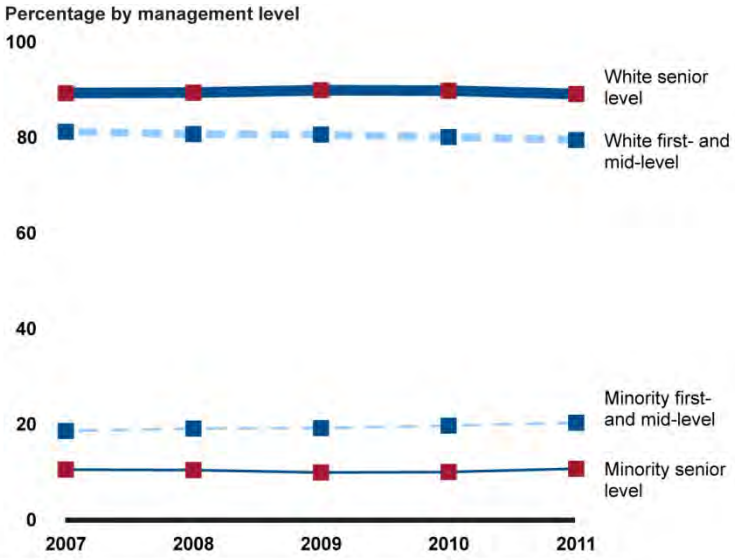


	2007	2008	2009	2010	2011
White EEOC	82.7%	82.1%	82.1%	81.6%	81.0%
Minority EEOC	17.3	17.9	17.9	18.4	19.0

Source: GAO analysis of EEOC data.

The representation of minorities varied among management positions, which EEOC splits into two categories: (1) first- and mid-level officials and managers and (2) senior-level officials and managers. In 2011, the representation of minorities among first- and mid-level managers stood at 20.4 percent, about 1 percentage point higher to the representation of minorities among all management positions, according to EEOC data (see fig. 2). In contrast, at the senior management level, representation of minorities was 10.8 percent in 2011, about 8 percentage points below their representation among all management positions; yet representation of minorities in first- and mid-level management positions consistently increased from 18.7 percent to 20.4 percent over the 5-year period. First- and mid-level management positions may serve as an internal pipeline in an organization through which minority candidates could move into senior management positions.

Figure 2: Percentage of Whites and Minorities in First- and Mid-Level Management and Senior Management Positions in the Financial Services Industry, 2007-2011

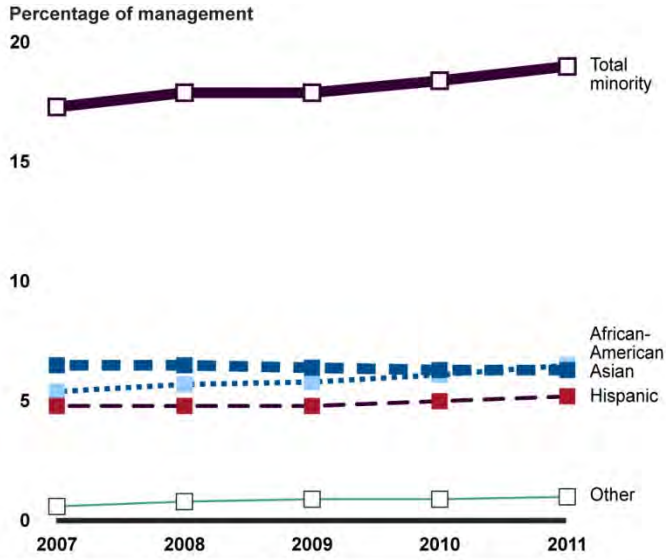


	2007	2008	2009	2010	2011
White senior level	89.4%	89.5%	90.0%	89.9%	89.2%
White first- and mid-level	81.3	80.8	80.7	80.2	79.6
Minority senior level	10.6%	10.5%	10.0%	10.1%	10.8%
Minority first- and mid-level	18.7	19.2	19.3	19.8	20.4

Source: GAO analysis of EEOC data.

Similar to the total representation of minorities across all management positions, specific races/ethnicities have not changed significantly, but EEOC data show slight variations of representation for specific races/ethnicities. For example, the representation of African Americans decreased from 6.5 percent in 2007 to 6.3 percent in 2011, according to EEOC data (see fig. 3). In contrast, representation of most other races/ethnicities increased, and the highest increase was in the representation of Asians, from 5.4 percent to 6.5 percent over the same time period.

Figure 3: Percentage of Specific Races/Ethnicities in the Financial Services Industry in Overall Management Positions, 2007-2011

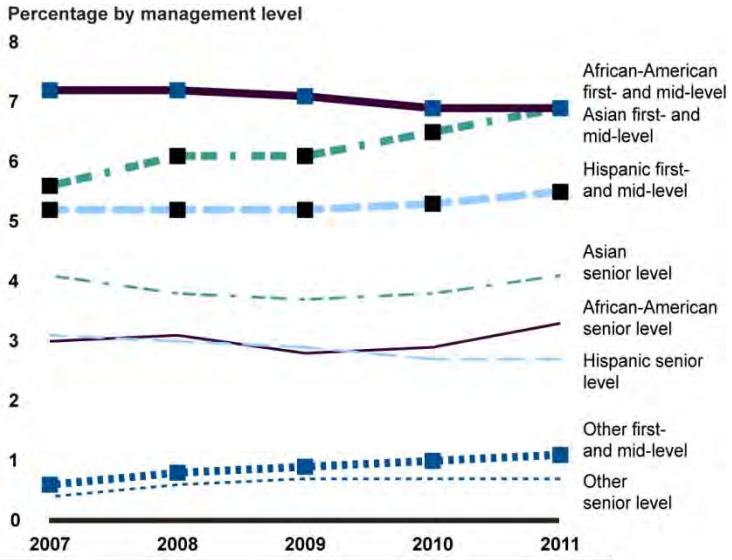


	2007	2008	2009	2010	2011
Total minority	**17.3%**	**17.9%**	**17.9%**	**18.4%**	**19.0%**
African-American	6.5	6.5	6.4	6.3	6.3
Hispanic	4.8	4.8	4.8	5.0	5.2
Asian	5.4	5.7	5.8	6.1	6.5
Other	0.6	0.8	0.9	0.9	1.0

Source: GAO analysis of EEOC data.

From 2007 to 2011, the representation of African Americans went down in both management levels, while the representation of other specific races/ethnicities either increased or remained stable (see fig. 4). At the senior management level, the representation of Asians remained stable at about 4.1 percent from 2007 through 2011. However, the representation of African Americans in senior management positions decreased from 3.1 percent to 2.7 percent, and the representation of Hispanics increased from 3 percent to 3.3 percent. Among first- and mid-level management positions, the representation of Asians increased from 5.6 percent to 6.9 percent and the representation of Hispanics increased from 5.2 percent to 5.5 percent, while the representation of African Americans decreased from 7.2 percent to 6.9 percent.

Figure 4: Percentage of Specific Races/Ethnicities in the Financial Services Industry at Various Management Levels, 2007-2011



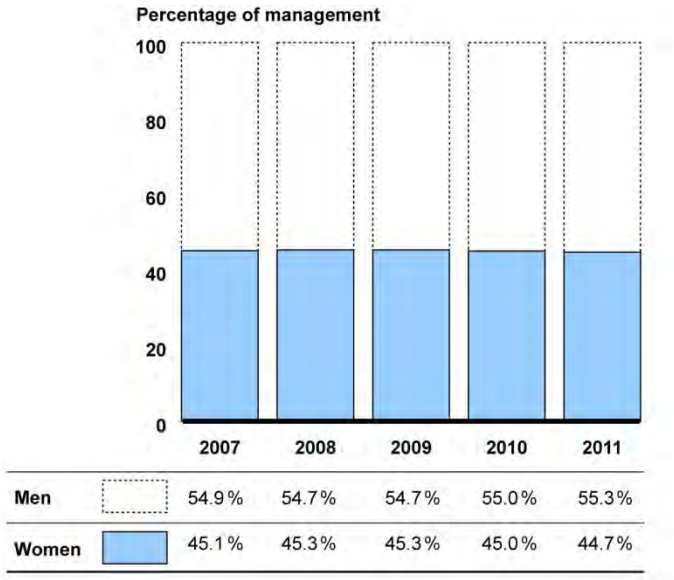
	Total minority senior level	**10.6 %**	**10.5%**	**10.0 %**	**10.1 %**	**10.8%**
	African-American senior level	3.1	3.0	2.9	2.7	2.7
	Hispanic senior level	3.0	3.1	2.8	2.9	3.3
	Asian senior level	4.1	3.8	3.7	3.8	4.1
	Other senior level	0.4	0.6	0.7	0.7	0.7
	Total minority first- and mid-level	**18.7 %**	**19.2%**	**19.3 %**	**19.8 %**	**20.4%**
	African-American first- and mid-level	7.2	7.2	7.1	6.9	6.9
	Hispanic first- and mid-level	5.2	5.2	5.2	5.3	5.5
	Asian first- and mid-level	5.6	6.1	6.1	6.5	6.9
	Other first- and mid-level	0.6	0.8	0.9	1.0	1.1

Source: GAO analysis of EEOC data.

Over the same 5-year period, the representation of women at the management level remained at about 45 percent in EEOC data, which show a slight decrease from 45.1 percent to 44.7 percent (see fig. 5). In

2006, we reported an increase with representation of women at about 42.9 percent in 1993 to about 45.8 percent in 2004.[13]

Figure 5: Percentage of Men and Women in Management Positions in the Financial Services Industry, 2007-2011

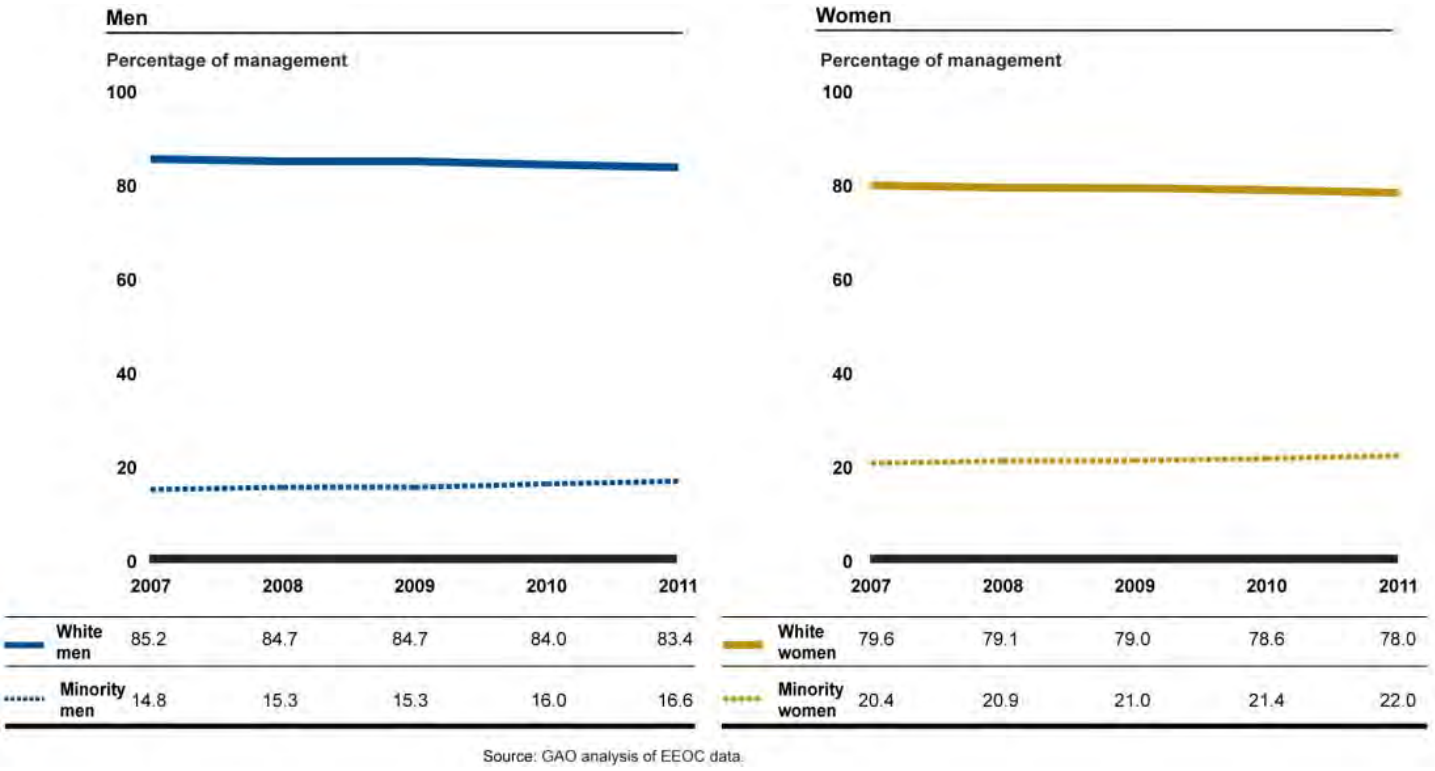


Source: GAO analysis of EEOC data.

Among all women in management positions, EEOC data showed that the representation of minority women increased, from 20.4 percent to 22 percent over the same 5-year period (see fig. 6). In addition, EEOC data show that the representation of minority men increased from 14.8 percent to 16.6 percent.

[13]GAO-06-617.

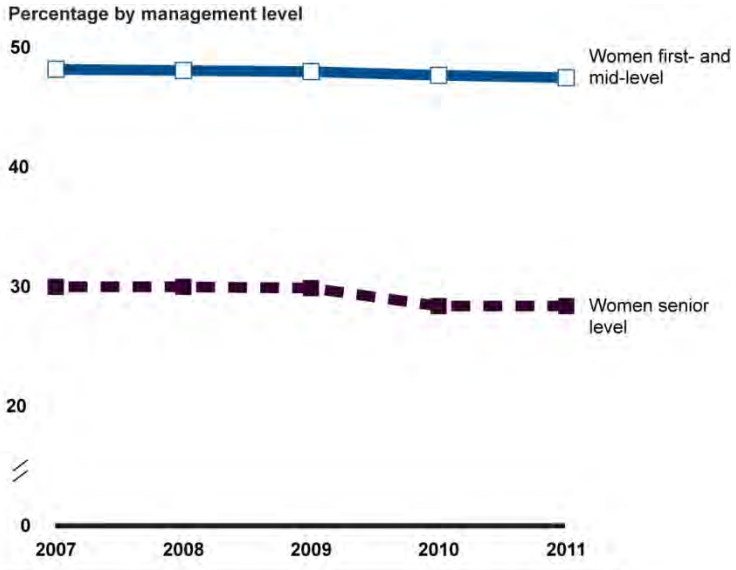
Figure 6: Percentage of White and Minority Men and White and Minority Women in Management Positions in the Financial Services Industry, 2007-2011



Source: GAO analysis of EEOC data.

Among first- and mid-level management positions, the representation of women has been at about 48 percent, slightly higher than the representation of women among all management positions. In contrast, women represented about 29 percent of all senior management positions from 2007 through 2011—about 16 percentage points below the representation of women for all management positions, according to EEOC data (see fig. 7).

Figure 7: Percentage of Women in the Financial Services Industry by Management Level and Race/Ethnicity, 2007-2011



	2007	2008	2009	2010	2011
Women first- and mid-level	48.2%	48.1%	48.0%	47.7%	47.5%
White women first- and mid-level	78.8	78.2	78.1	77.7	77.1
Minority women first- and mid-level	21.2	21.8	21.9	22.3	22.9
Women senior level	30.0%	30.0%	29.9%	28.4%	28.4%
White women senior level	86.3	86.7	87.4	87.6	86.5
Minority women senior level	13.7	13.3	12.6	12.4	13.5

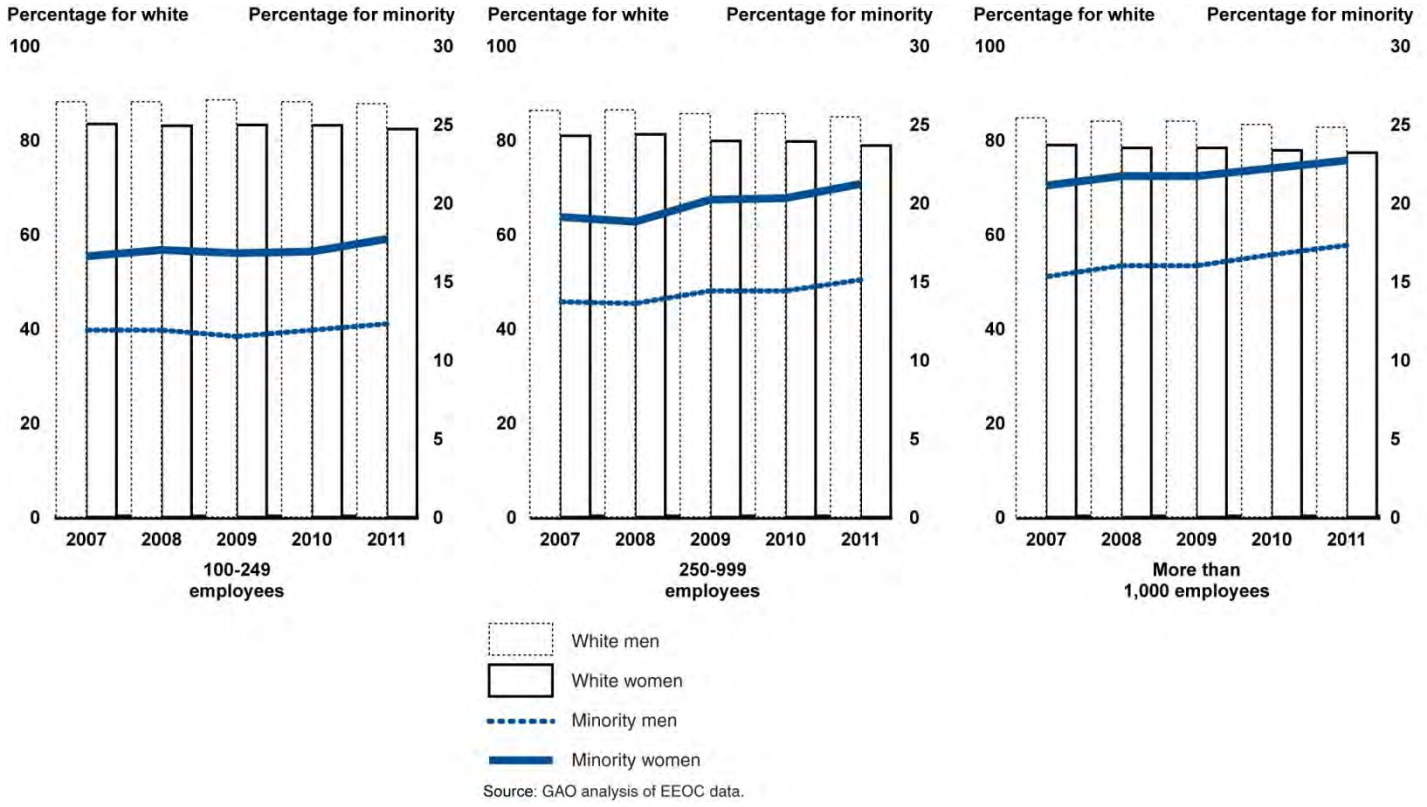
Source: GAO analysis of EEOC data.

Based on EEOC data, minority women had greater representation at the first and mid levels of management compared to the senior level over the 5-year period. As shown in figure 7, among female senior managers, representation of minority women remained at about 13 percent over the 5-year period. In contrast, among female first- and mid-level managers, the proportion of minority women increased during the same period from 21.2 percent to 22.9 percent.

The representation of minorities increases for both women and men as the firm size increases (see fig. 8). For example, in 2011 the representation of minorities at firms with 100-249 employees was about 18 percent among women and about 12 percent among men, while at firms with more than 1,000 employees, the representation of minorities

was about 23 percent among women and about 17 percent among men. For additional analysis of EEOC data by workforce position and industry sector, see appendix II.

Figure 8: Percentage of Whites/Minorities and Men/Women at Financial Services Firms of Different Sizes, 2007-2011



Source: GAO analysis of EEOC data.

A survey of the general population shows some similar trends in the representation of both women and minorities in the financial services industry. The CPS is administered by the Bureau of the Census for the Bureau of Labor Statistics and is a monthly survey of about 60,000 households across the nation. The CPS is used to produce official government figures on total employment and unemployment issued each month. According to the CPS data, from 2007 through 2011 the representation of women at the management level decreased from an estimated 49.1 percent to 47.3 percent. In addition, CPS data show a smaller increase from an estimated 14.1 percent to 15.1 percent in the

representation of minorities in management over the same 5-year period.[14]

Leading Diversity Practices Remain Relevant but Challenges Exist Regarding Recruitment and Other Issues

The nine leading diversity practices that we previously identified in 2005 are still relevant today, according to industry representatives with whom we spoke.[15] Some industry representatives highlighted practices among these nine that they considered the most important to foster diversity and inclusion in their organizations. For example, top leadership commitment drives the other eight leading diversity practices, according to 9 of 10 industry representatives. In addition, accountability helps to promote the implementation of the other leading diversity practices because an issue is more likely to be addressed if it is tracked, according to 2 industry representatives. Moreover, creating awareness of the benefits of diversity for an organization among management and employees is important because it increases commitment to further the diversity goals of the organization, according to 7 industry representatives whom we interviewed.[16] However, 1 industry representative told us there are still some firms that do not see the importance of diversity. In addition, 2 industry representatives said these 9 leading diversity practices should be expanded beyond workforce management to include, for example, an organization's contracting efforts.

[14]We determined the CPS-estimated minority percentages of management positions within the financial services industry cannot be precisely measured. However, CPS-estimated minority percentages were included in this report to provide some more context. Since many of the percentage estimates have wide confidence intervals, we encourage the reader to interpret the CPS-estimated minority percentages in this report with caution. Please see appendix I for the estimated minority percentages and standard errors.

[15]As previously discussed the nine leading diversity practices are (1) commitment to diversity as demonstrated and communicated by an organization's top leadership; (2) the inclusion of diversity management in an organization's strategic plan; (3) diversity linked to performance, making the case that a more diverse and inclusive work environment could help improve productivity and individual and organizational performance; (4) measurement of the impact of various aspects of a diversity program; (5) management accountability for the progress of diversity initiatives; (6) succession planning; (7) recruitment; (8) employee involvement in an organization's diversity management; and (9) training for management and staff about diversity management. See GAO-05-90.

[16]This relates to leading practice diversity linked to performance, which refers to the understanding that a more diverse and inclusive work environment can yield greater productivity and help improve individuals' and organization performance, while employee involvement refers to the contribution of employees in driving diversity throughout an organization. See GAO-05-90.

Some industry representatives also noted that measuring the impact of various diversity practices is an important practice but that it can also be challenging; for example, it can be difficult to link specific practices to diversity outcomes and it can be a long-term process. According to some industry representatives, financial services organizations may measure the effectiveness of their diversity practices by assessing attrition, recruiting, and promotion rates, which are similar to measures we had previously reported.[17] For example, a financial services organization may measure the proportion of certain minority groups or women in its workforce or among its promotions to determine the effectiveness of its practices. Further, financial services firms may use surveys to gather employee perspectives on workforce diversity issues in the organization, such as perceived fairness in the promotion process or factors that affect an employee's decision to remain with the firm, among other topics.

Additional diversity practices identified by some industry representatives that can support the leading diversity practices include the following:

- *Sponsor individuals*. Sponsorship of women within an organization where an executive acts as a guide to help women navigate the organization and expand their networks is an important diversity practice, according to three industry representatives. This sponsorship practice goes beyond the mentoring programs we previously reported in 2006, as a sponsor acts as an advocate to help the individual advance within the organization.[18]

- *Address biased perceptions.* One industry representative told us about an effort to combat unconscious bias in promotions. They described a promotion system designed to address biased perceptions, such as a view of leaders as being typically male. According to the industry representative, the firm that employed this diversity practice gathered complete and objective evaluations of employees and trained its managers to recognize and address these perceptions. The result was that the firm promoted greater numbers of women into management.

No industry representatives that we contacted reported changes to diversity practices as a result of the challenges faced by many firms

[17]GAO-06-617 and GAO-10-736T.

[18]GAO-06-617.

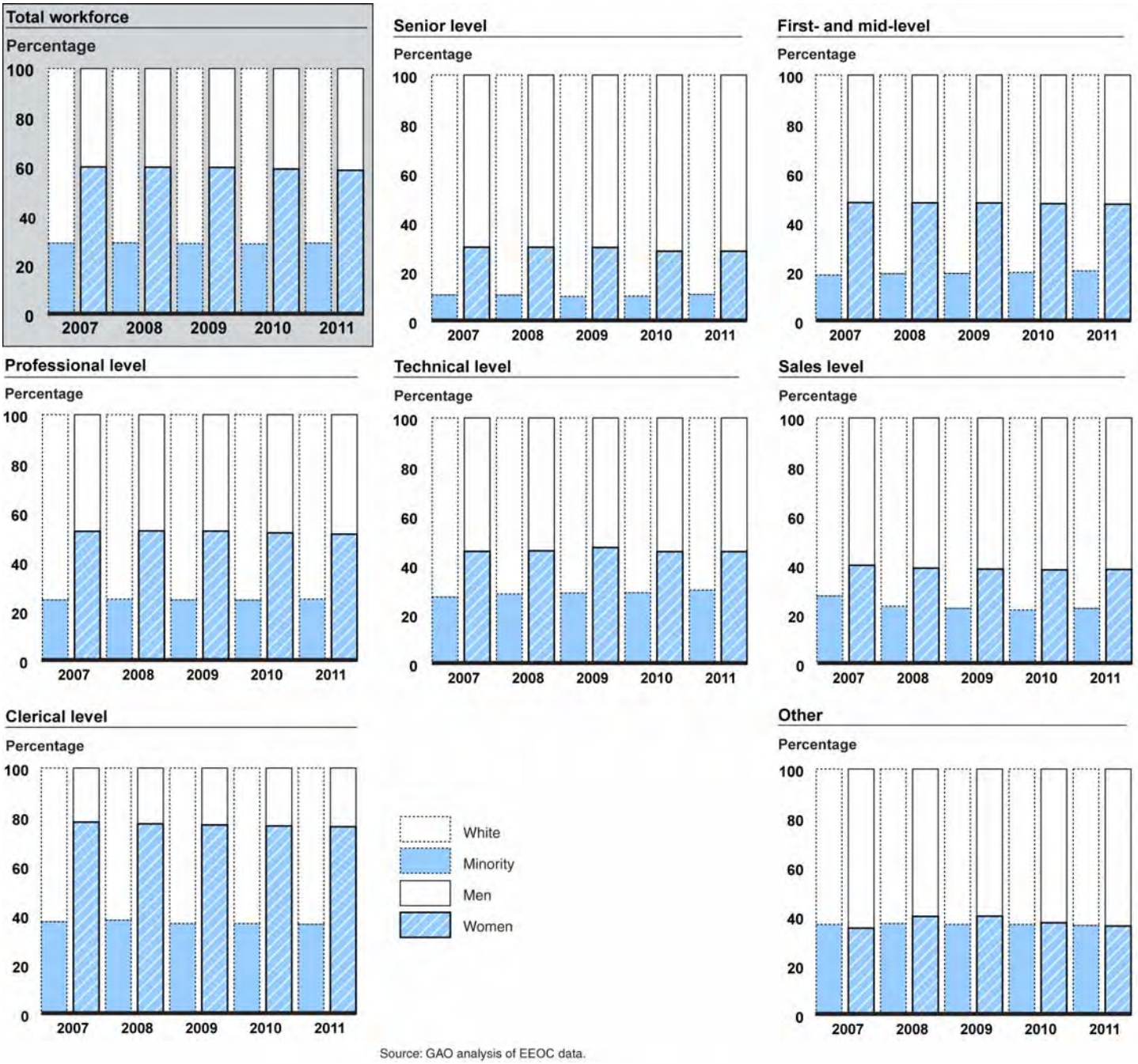
during the financial crisis. Although representation of minorities and women has remained about the same from 2007 through 2011, according to some industry representatives, the industry continues to be focused on diversity. However, three industry representatives did cite specific instances where funding was scaled back as a result of the recent financial crisis. One industry representative told us that investment in training programs was reduced across the organization, but when a measureable impact on employees was identified at this organization, steps were taken to address the impact.

Some industry representatives cited challenges to achieving a diverse workforce in general. We have previously reported some of these challenges, which can affect some of the leading diversity practices.[19] Six industry representatives said that diversity recruitment is difficult because the supply (or "pipeline") of minority and women candidates is limited. This has been a consistent challenge that we previously reported in 2006 and 2010.[20] Available data indicate that for the internal pool of potential candidates for some management positions, representation of women varied, while representation of minorities was higher in every nonmanagement category compared to management positions (see fig. 9). For example, in 2011 the representation of women was greater in professional positions (about 51 percent) compared to sales positions (about 38 percent). In addition, the representation of minorities was higher in all nonmanagement positions than at the management level in 2011, but especially higher in technical and clerical positions at more than 29 percent in both types of positions. Further analysis of diversity in various workforce positions can be found in appendix II.

[19]GAO-06-617 and GAO-10-736T.

[20]GAO-06-617 and GAO-10-736T.

Figure 9: Percentage of Whites/Minorities and Men/Women in Various Financial Services Industry Workforce Positions, 2007-2011



Source: GAO analysis of EEOC data.

Note: The following are descriptions of the job categories in EEO-1 data from EEOC: (1) "Executive/Senior Level Officials and Managers," includes individuals who reside in the highest levels of organizations and plan, direct, and formulate policies, set strategy, and provide the overall direction of enterprises/organizations for the development and delivery of products or services, within the parameters approved by boards of directors or other governing bodies; (2) "First/Mid-Level Officials and Managers," includes individuals who receive directions from Executive/Senior Level management, and oversee and direct the delivery of products, services, or functions at group, regional, or divisional levels of organizations; (3) "professionals" include occupations requiring either college graduation or experience of such kind and amount as to provide a comparable background; (4) "technicians" include occupations requiring a combination of basic scientific knowledge and manual skill that can be obtained through 2 years of post-high school education; (5) "sales workers" include occupations engaging wholly or primarily in direct selling; (6) "office and clerical" includes all clerical-type work regardless of level of difficulty, where the activities are predominantly nonmanual; and (7) the category "other" includes craft workers, operatives, laborers, and service workers.

In recent years, representation in business graduate programs, a potential source of future managers in the financial industry, has remained stable for women and has increased slightly for minorities, but representation is still low for both women and minorities when compared to the overall representation of students in the university system.[21] To assess one possible external pool of candidates for financial services firms, we obtained data from the Association to Advance Collegiate Schools of Business (AACSB) on the number of students enrolled in Master of Business Administration (MBA) degree programs in AACSB member schools in the United States from 2007 through 2011 as well as the number of students in the university system.[22] According to AACSB data, the representation of women remained constant over this period, while the representation of minorities increased. For example, the representation of women among MBA students remained at about 37 percent over the 5-year period, while representation of women was slightly higher in the overall university system at about 41 percent. In contrast, as table 2 shows, the representation of minorities increased among MBA students from about 26 percent in 2007 to about 29 percent in 2011. However, when compared to the university system, representation of minorities in the overall university system was slightly higher from about 29 percent in 2007 to 34 percent in 2011.

[21]We refer to overall representation of students from undergraduate, graduate, and doctoral programs as the university system. These data exclude specialized graduate programs, such as Master of Economics. In addition, these overall percentages only represent enrolled students for which race/ethnicity or gender were indicated.

[22]AACSB, the world's largest accreditation association for business schools, conducts an annual survey called "Business School Questionnaire" of all its member schools. Participation in this survey is voluntary.

Table 2: Percentage of Students Enrolled in MBA Degree Programs at AACSB Member Schools in the United States by Race/Ethnicity, 2007-2011

Year	Total enrolled	White	Total minority	African American	Hispanic	Asian	Other
2007	100%	74%	26%	7%	6%	12%	0%
2008	100	73	27	8	6	12	0
2009	100	73	27	8	7	12	0
2010	100	72	28	9	7	11	1
2011	100	71	29	9	7	11	2

Source: GAO analysis of AACSB International data.

Note: The "other" category includes Native American, and updated race/ethnicity categories implemented in 2011 to include "two or more races" and "Native Hawaiian or Other Pacific Islander." Percentages may not always add exactly due to rounding. In addition, these ratios only represent MBA enrolled students for whom race/ethnicity was indicated.

Some industry representatives stated that the negative perception of the industry could also limit the external pipeline of potential candidates, which can make recruitment challenging. Multiple industry representatives discussed the need to take a new approach to diversity recruiting as a result of the negative image many potential candidates may have about the financial services industry following the recent financial crisis. For example, to counter negative perceptions that may have resulted from the foreclosure crisis or the Occupy Wall Street movement, one industry representative told us that it explains to prospective employees the social contributions financial services firms make through microfinance or economic and community development.

In addition to these difficulties with recruiting, two industry representatives highlighted maintaining accountability as a particular challenge for financial services firms.[23] For example, an industry representative said it is difficult to promote results in diversity by linking diversity management with managers' performance ratings because this practice may not provide enough incentive to many managers. Another industry representative told us that recognizing and compensating managers and employees for their diversity efforts can result in increased commitment to foster workforce diversity and an increase in diversity at firms.

[23]Accountability refers to the means to ensure that leaders are responsible for diversity by aligning their performance assessment and compensation to the progress of diversity initiatives. See GAO-05-90.

Agency and Reserve Bank Workforce Diversity Varied, and Officials Reported Difficulty Identifying Diverse Candidates

Since the financial crisis, senior management-level minority and gender diversity at the federal financial agencies and Reserve Banks has varied across individual entities.[24] The representation of minorities at the senior management-level increased slightly overall at both the agencies and Reserve Banks. In addition, the representation of women at the senior management-level increased slightly overall for both the agencies and Reserve Banks. Agency and Reserve Bank officials identified key challenges to increasing workforce diversity overall and at the senior management-level, including limited representation of minorities and women among internal and external candidate pools.

Senior Management-Level Representation of Minorities and Women Varied at Agencies and Reserve Banks, with Slight Changes Overall

Senior management-level representation of minorities and women varied across individual federal financial agencies and the 12 Reserve Banks. The agencies included FDIC, the Federal Reserve Board, NCUA, OCC, and Treasury. Complete data for this period were not available for CFPB, FHFA, and SEC, and we excluded these agencies from our analysis of changes in senior management-level diversity from 2007 through 2011, but provide recent data when available. Data for each agency are provided in appendix IV. CFPB assumed responsibility for certain consumer financial protection functions in July 2011 and has not yet reported workforce information to EEOC.[25] However, we received recent employment profile data from CFPB as of May 2012.[26] FHFA, which was established in July 2008, started reporting workforce data for 2010; while our analysis provides 2010 and 2011 data for FHFA, our analysis across the agencies excludes FHFA from aggregated totals. SEC reported data for 2007 through 2011, but revised how it reported officials and managers during the 5-year period; while our analysis provides 2011 senior

[24]Our analysis of employment data in this section of the report differs from how EEOC typically reports data. While EEOC reports on individual equal employment opportunity groups, we report on minorities as a group. Additional data and figures supporting this section of the report are in appendixes III and IV.

[25]On July 21, 2010, the Consumer Financial Protection Act established CFPB as an independent bureau within the Federal Reserve System to be headed by a director. Effective July 21, 2011, CFPB assumed responsibility for certain consumer financial protection functions formerly the responsibilities of the Board of Governors of the Federal Reserve System, the Comptroller of the Currency, the Director of the Office of Thrift Supervision, FDIC, the Federal Trade Commission, NCUA, and the Secretary of the Department of Housing and Urban Development.

[26]CFPB provided to us workforce diversity data for all employees, senior officials, and supervisors as of May 19, 2012.

management-level data for SEC, we excluded SEC from our senior management-level trend analysis.

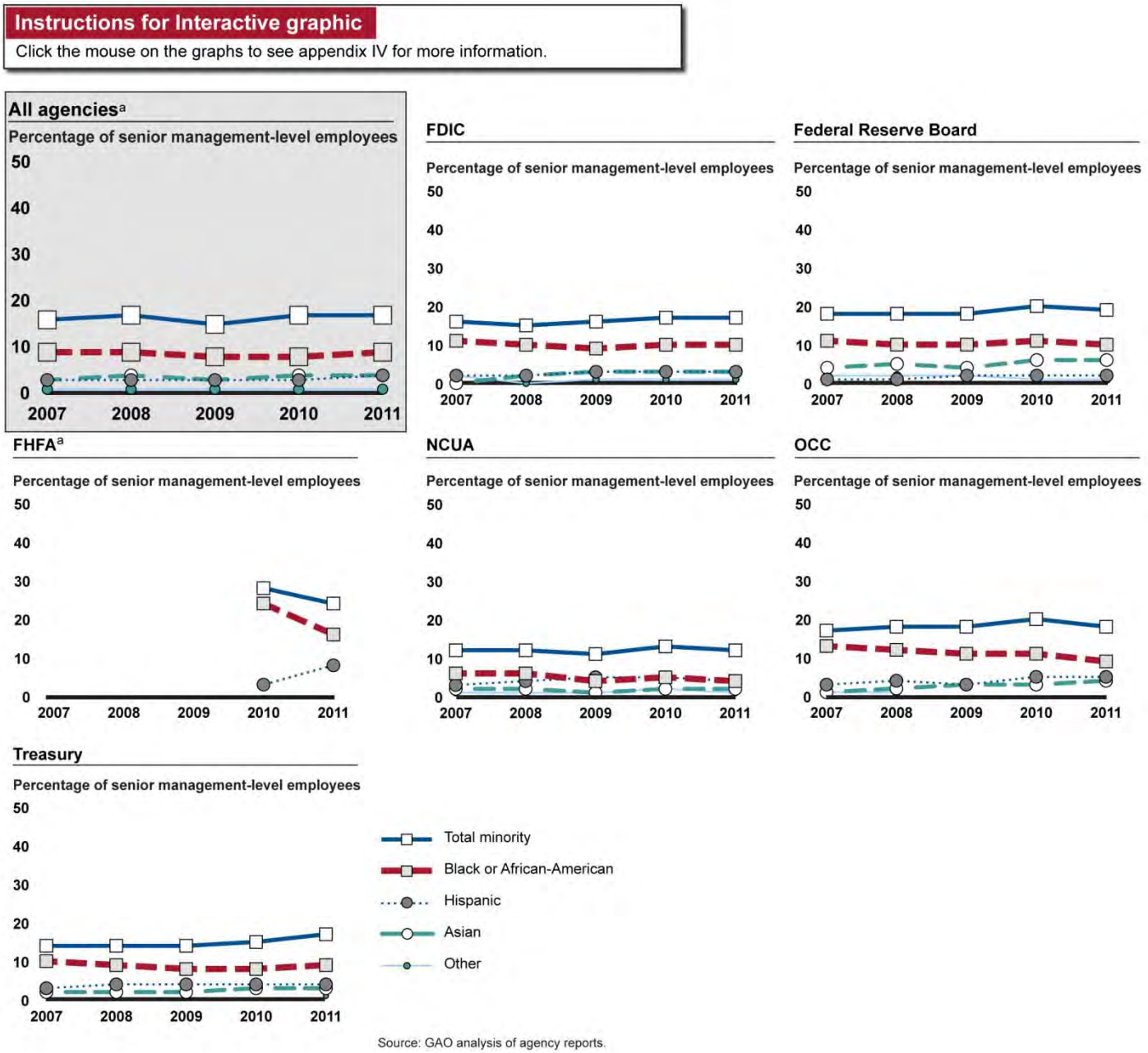
In our review of agency reports, we found that from 2007 through 2011, the representation of minorities among senior management-level employees, when aggregated across FDIC, the Federal Reserve Board, NCUA, OCC, and Treasury, increased slightly, from 16 to 17 percent for the agencies combined (see fig. 10).[27] From 2007 through 2011, three agencies—FDIC, the Federal Reserve Board, and Treasury—showed an increase in the representation of minorities at the senior management-level, by between 1 and 3 percentage points. Two agencies—NCUA and OCC—experienced no percentage point change in their representation of minorities at the senior management-level from 2007 through 2011.[28] In 2011, the representation of minorities among senior management-level employees of these agencies, FHFA, and SEC ranged from 11 percent at SEC to 24 percent at FHFA. Additionally, CFPB employment data showed about 28 percent representation of minorities among senior officials as of May 2012.[29]

[27]Federal financial agencies provided us reports they issued according to EEOC Management Directive 715, known as MD-715 reports. This directive does not apply to the Federal Reserve Banks, as they are not federal agencies. Our analysis of the representation of minorities and women at the senior management level for agencies reviewed the numbers of employees the agencies reported as "Executive/Senior Level" from 2007 through 2011. Though the MD-715 reports allow for this category to cover Grades 15 and above, agencies have discretion to decide which positions are included in this senior level versus those the agencies include at lower levels of management. Therefore, comparisons of a given management level between the agencies do not necessarily involve the same set of managers at each agency. Figures in our analysis are rounded to the nearest percent.

[28]Percentage changes in the representation of minorities among senior management-level employees from 2007 through 2011 for NCUA and OCC were zero when rounded to the nearest percent. The representation of minorities among senior management-level employees was 12 percent at NCUA in 2007 and 2011, and at OCC, 17 percent in 2007 and 18 percent in 2011.

[29]CFPB identified these employees as Executive/Senior Officials.

Figure 10: Percentage of Minorities among Senior Management-Level Employees at Six Federal Financial Agencies, 2007-2011



Source: GAO analysis of agency reports.

Notes: Percentages are rounded to the nearest percent.

For our analysis, we reviewed the numbers of employees the agencies reported according to race/ethnicity and gender in table A3 of their MD-715 reports from 2007 through 2011. These data

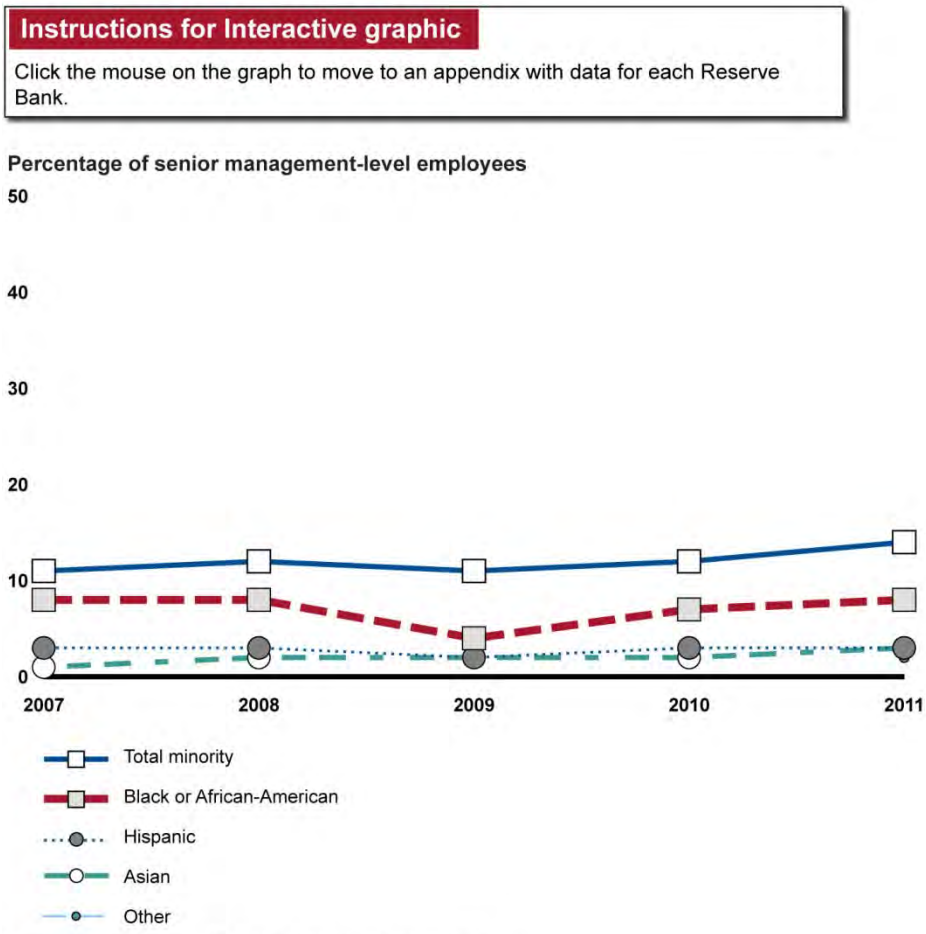
are based on information self-reported by employees to each agency and there were some differences in reporting across the agencies. In some years, some agencies reported all employees—permanent and temporary—in their A3 tables while others reported permanent employees only. We considered employees reported by agencies in the category "Executive/Senior Level" as senior management-level employees. Though the MD-715 report guidelines instruct agencies to identify employees Grades 15 and above who have supervisory responsibility in this category, agencies have discretion to include employees who have significant policymaking responsibilities but do not supervise employees. As a result, the composition of the "Executive/Senior Level" category may vary among the different agencies and does not necessarily involve the same set of managers at each agency.

[a]Our trend analysis for "all agencies" excludes CFPB, FHFA, and SEC. CFPB assumed responsibility for certain consumer financial protection functions in July 2011 and has not yet reported workforce information to EEOC. FHFA was established in 2008 and started reporting workforce data for 2010. SEC revised how it reported officials and managers between 2007 and 2011. While our analysis includes 2011 management-level data for SEC, we excluded SEC from our trend analysis.

In our review of EEO-1 reports provided by the Reserve Banks, we found that the representation of minorities among senior management-level employees in aggregate across the 12 Reserve Banks increased from 11 percent to 14 percent from 2007 through 2011 (see fig.11).[30] The population of senior management-level employees at each bank in 2011 ranged from 9 employees at the Reserve Banks of Chicago, Dallas, and Minneapolis, to 59 employees at the Reserve Bank of New York, and the population of minority senior management-level employees at each bank ranged from zero employees at the Reserve Bank of Cleveland to 7 employees at the Reserve Bank of New York. Specific information on each Reserve Bank is provided in appendix IV.

[30]Reserve Banks provided us reports they issued to EEOC according to form EEO-1. Our analysis of senior management-level representation for the Reserve Banks included employees the banks reported as "Executive/Senior Officials and Managers." Figures in our analysis are rounded to the nearest percent.

Figure 11: Percentage of Minorities among Senior Management-Level Employees at the 12 Reserve Banks, 2007-2011



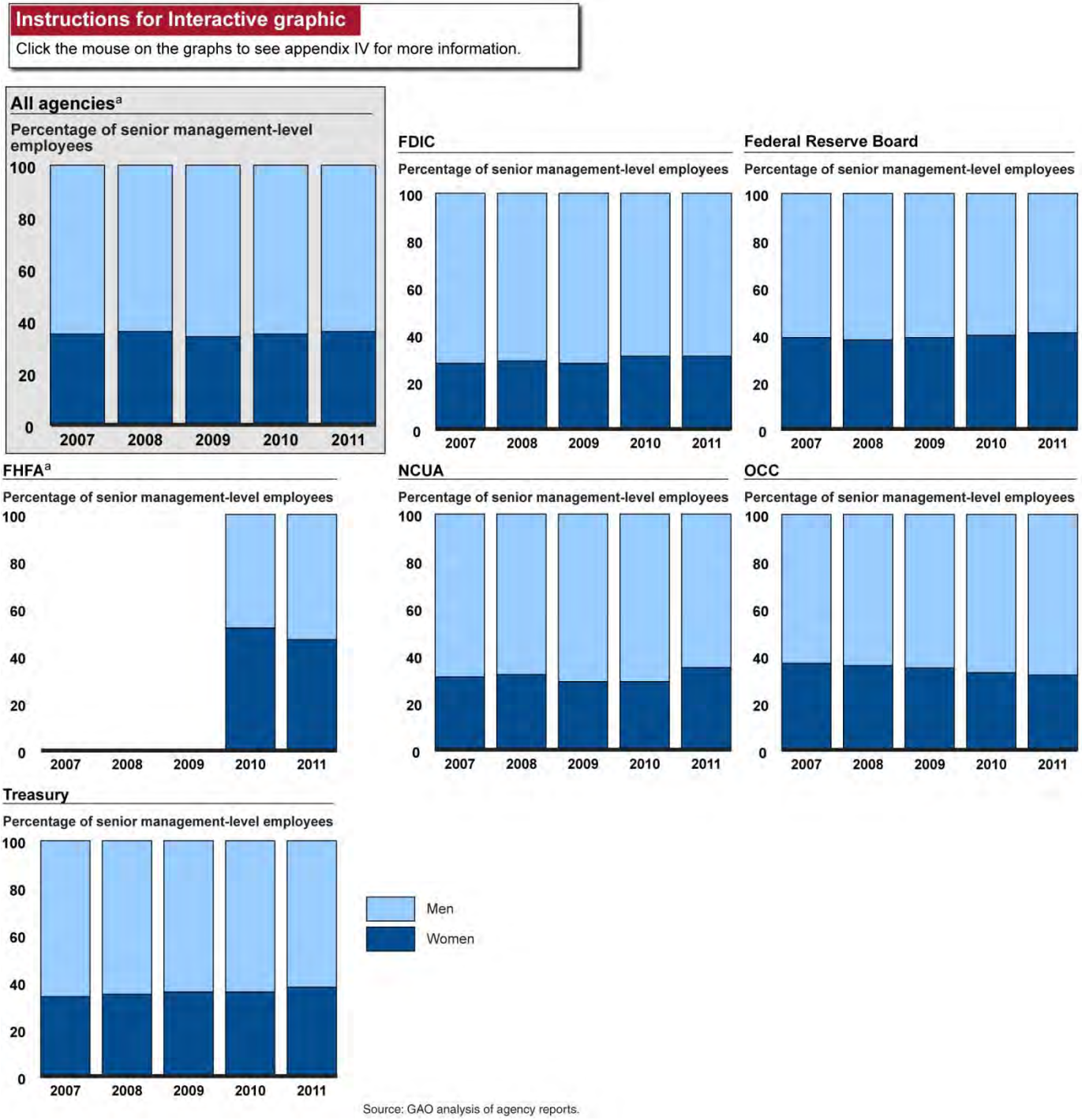
Source: GAO analysis of EEO-1 reports provided by Reserve Banks.

Notes: Data are rounded to the nearest percent.

Reserve Bank data are presented in aggregate because the population of senior management-level employees at most Reserve Banks is generally small and the gain or loss of one employee can result in a large percentage point change in the representation of minorities. Specific information on each Reserve Bank is provided in appendix IV.

In general, the representation of women at the senior management-level increased slightly since the beginning of the financial crisis in 2007 at agencies, but representation percentages varied for each entity. In our review of agency reports, we found that from 2007 through 2011, the representation of women at the senior management-level increased slightly from 34 to 36 percent across FDIC, the Federal Reserve Board, NCUA, OCC, and Treasury, in aggregate (see fig. 12). Changes varied by agency, from a decrease of 5 percentage points at OCC to an increase of 5 percentage points at NCUA. Four of the five agencies—FDIC, the Federal Reserve Board, NCUA, and Treasury—showed an increase of between 3 and 5 percentage points in the representation of women at the senior management-level from 2007 through 2011. In 2011, the representation of women among senior management-level employees ranged among the agencies from 31 percent at FDIC to 47 percent at FHFA. Additionally, CFPB employment data showed the representation of women among senior officials at about 35 percent as of May 2012.

Figure 12: Percentage of Women among Senior Management-Level Employees at Six Federal Financial Agencies, 2007-2011



Source: GAO analysis of agency reports.

Notes: Percentages are rounded to the nearest percent.

For our analysis, we reviewed the numbers of employees the agencies reported according to race/ethnicity and gender in table A3 of their MD-715 reports from 2007 through 2011. These data are based on information self-reported by employees to each agency and there were some differences in reporting across the agencies. In some years, some agencies reported all employees—permanent and temporary—in their A3 tables while others reported permanent employees only. We considered employees reported by agencies in the category "Executive/Senior Level" as senior management-level employees. Though the MD-715 report guidelines instruct agencies to identify employees Grades 15 and above who have supervisory responsibility in this category, agencies have discretion to include employees who have significant policymaking responsibilities but do not supervise employees. As a result, the composition of the "Executive/Senior Level" category may vary among the different agencies and does not necessarily involve the same set of managers at each agency.

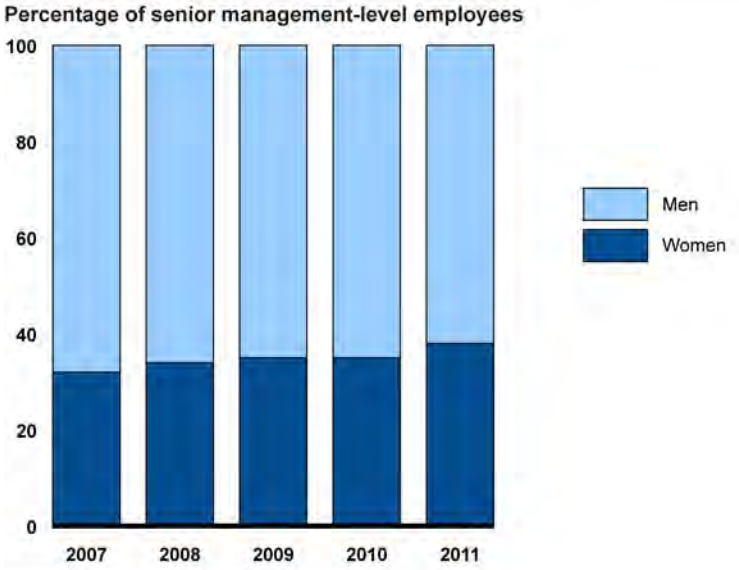
[a]Our trend analysis for "all agencies" excludes CFPB, FHFA, and SEC. CFPB assumed responsibility for certain consumer financial protection functions in July 2011 and has not yet reported workforce information to EEOC. FHFA was established in 2008 and started reporting workforce data for 2010. SEC revised how it reported officials and managers between 2007 and 2011. While our analysis includes 2011 management-level data for SEC, we excluded SEC from our trend analysis.

In our review of EEO-1 reports provided by the Reserve Banks, we found that from 2007 through 2011, the representation of women at the senior management-level increased from 32 percent to 38 percent for the Reserve Banks, in aggregate (see fig. 13). As mentioned previously, the population of senior management-level employees at each bank in 2011 ranged from nine employees at the Reserve Banks of Chicago, Dallas, and Minneapolis, to 59 employees at the Reserve Bank of New York. The population of women among senior management-level employees at each bank in 2011 ranged from two employees at the Reserve Bank of Boston to 25 employees at the Reserve Bank of New York. Specific information on each Reserve Bank is provided in appendix IV.

Figure 13: Percentage of Women among Senior Management-Level Employees at the 12 Reserve Banks, 2007-2011

Instructions for Interactive graphic

Click the mouse on the graph to move to an appendix with data for each Reserve Bank.



Source: GAO analysis of Reserve Bank reports.

Notes: Data are rounded to the nearest percent.

Reserve Bank data are presented in aggregate because the population of senior management-level employees at most Reserve Banks is generally small and the gain or loss of one employee can result in a large percentage point change in the representation of women. Specific information on each Reserve Bank is provided in appendix IV.

Several agencies reported on existing diversity practices related to retaining and promoting employees to build management-level diversity. For example, according to agency reports, some Treasury offices conduct formal mentoring programs, and the Federal Reserve Board has customized mentoring programs within its divisions, which in conjunction with a leadership exchange program sponsored by the Federal Reserve System, provide employees opportunities to develop new skills and experiences. Further, OCC reported having development programs for employees within its bank supervision division that provide leadership and development opportunities to staff, and agency-sponsored employee network groups implemented mentoring circles to assist in the career development and retention of the agency's workforce.

Several Reserve Banks identified practices targeted to improve management-level diversity, including changes to hiring practices and mentoring programs. For example, officials from several Reserve Banks we contacted said their organizations revised their hiring policies to open all management-level positions to external applicants in addition to current employees as a way to build management-level diversity by hiring diverse, experienced candidates from outside the organization. Additionally, the Reserve Banks of Dallas and New York began piloting new mentoring programs in 2011, and each planned to expand its program based on initial feedback its OMWI had received. These banks and several others with existing mentoring programs reported that mentoring programs were important to retaining and developing minorities and women within their organizations. Later in this report, we provide additional information on the agencies' and Reserve Banks' recruitment practices as part of their efforts to implement section 342 of the Dodd-Frank Act.[31]

[31]Among other things, the act outlines steps the specific agencies and Reserve Banks should take to seek workforce diversity at all levels of their organizations. These steps include recruiting from colleges serving primarily minority populations, sponsoring and recruiting at job fairs in urban communities, and advertising positions in newspapers and magazines oriented toward minorities and women.

Total Workforce Minorities and Women Representation Varied but Decreased Slightly Overall

Based on our analysis of minority and gender diversity at all levels from 2007 through 2011, workforce diversity varied at the federal financial agencies and Reserve Banks, with slight decreases in aggregate. Specifically, the representation of minorities decreased slightly from 31 percent to 30 percent from 2007 through 2011 across FDIC, the Federal Reserve Board, NCUA, OCC, SEC, and Treasury, in aggregate. Additionally, CFPB employment data showed the representation of minorities of all agency employees at about 33 percent as of May 2012. Three agencies—NCUA, OCC, and SEC—showed a 1 percentage point or greater increase in the overall representation of minorities during the 5-year period, according to agency reports. In 2011, the representation of minorities at the agencies ranged from 25 percent at NCUA to 44 percent at the Federal Reserve Board. Our analysis of EEO-1 reports provided by the Reserve Banks for 2007 through 2011 showed that the representation of minorities across the Reserve Banks declined slightly in aggregate, from 38 percent to 36 percent. The Reserve Banks of Minneapolis and New York showed a 2 percentage point increase in the overall representation of minorities working at Reserve Banks, the Reserve Bank of Boston showed no percentage point change, and the remaining nine banks showed decreases of 1 to 8 percentage points. In 2011, the representation of minorities at the Reserve Banks ranged from 16 percent at the Reserve Bank of Kansas City to 53 percent at the Reserve Bank of San Francisco.

Similarly, we found that overall gender diversity varied at individual agencies and Reserve Banks, and generally declined slightly from 2007 through 2011. The overall representation of women in the workforce aggregated across FDIC, the Federal Reserve Board, NCUA, OCC, SEC, and Treasury declined slightly from 47 percent to 45 percent over the 5-year period. Additionally, CFPB employment data showed the representation of women of all agency employees at about 49 percent as of May 2012. Two agencies—NCUA and SEC—showed no percentage point change in the representation of women during the 5-year period; OCC showed a decrease of about 1 percentage point, and the other three agencies—FDIC, the Federal Reserve Board, and Treasury—experienced decreases of 2 percentage points. In 2011, the representation of women among all employees at the agencies ranged from 42 percent at FDIC to 48 percent at SEC and Treasury. The overall representation of women across the Reserve Banks, in aggregate, declined from 49 percent to 45 percent from 2007 through 2011. All Reserve Banks showed declines in the representation of women among all employees during the 5-year period, ranging from a 1 percentage point decrease at the Reserve Bank of New York to a 7 percentage point

decrease at the Reserve Bank of Cleveland. For example, in 2007, 827 of the Reserve Bank of Cleveland's 1,568 employees were women, and in 2011, 500 of the bank's 1,094 employees were women; the bank's workforce changed from having around 53 percent women employees to about 46 percent women employees. In 2011, the overall representation of women at Reserve Banks ranged from 40 percent at the Reserve Banks of Philadelphia and Richmond to 53 percent at the Reserve Bank of Minneapolis. See appendix III for additional information on the overall workforce representation for the agencies and Reserve Banks.

According to officials from five Reserve Banks and the Federal Reserve Board, consolidation of check processing and other operations, some of which occurred since the financial crisis, had eliminated many administrative and service worker positions. Since these positions are often held by minorities and women, these consolidations affected overall employment diversity at affected Reserve Banks. In response to declines in the use of paper checks and greater use of electronic payments, the Reserve Banks took steps beginning in 2003 to reduce the number of locations where paper checks were processed. In 2001, the Federal Reserve System employed around 5,500 people in check processing functions across 45 locations, and in 2008, around 2,800 employees supported check processing functions across 18 locations. By 2010, one paper check processing site remained in Cleveland, along with an electronic check processing site in Atlanta. As of January 2013, approximately 480 employees supported check processing functions across the Federal Reserve System. The Federal Reserve System is projected to complete its consolidation of check processing functions in 2013.

Officials Reported Difficulty Identifying Diverse Candidates as the Main Challenge to Building Workforce Diversity

OMWI officials described challenges to building workforce diversity both at the management level and overall. Four agencies—FDIC, the Federal Reserve Board, FHFA, and OCC—and three Reserve Banks—the Reserve Banks of Chicago, Minneapolis, and St. Louis—cited underrepresentation of minorities and women within internal candidate pools as a challenge to building management-level diversity, as many management-level positions are filled through promotions or internal hiring processes. Additionally, the Reserve Banks of Dallas, Minneapolis, Philadelphia, and San Francisco said low turnover was a challenge to increasing their management-level diversity profiles because it limited opportunities to increase organizational diversity through hiring and promotion.

Federal financial agencies and Reserve Banks identified other challenges to building workforce diversity generally. The Reserve Banks of Atlanta, Boston, Chicago, Kansas City, and St. Louis cited competition from the private sector for recruiting diverse candidates as a challenge. In addition, FHFA and the Reserve Banks of Cleveland, Philadelphia, and San Francisco cited limited representation of minorities within external candidate pools as another challenge. The Federal Reserve Board and the Reserve Banks of Chicago and Kansas City reported that the availability of external candidates could be an issue in particular for hiring certain specialized positions, such as economists, which would involve a small candidate pool with limited representation of minorities. Additionally, three Reserve Banks identified geographic impediments to their national recruitment efforts, explaining that it is difficult to attract candidates from outside their region. For example, the Reserve Banks of Kansas City and St. Louis said it was difficult to recruit candidates lacking ties to the central United States, and the Reserve Bank of San Francisco cited difficulty recruiting from the eastern United States. Further, several agencies and Reserve Banks identified other challenges to building workforce diversity. For example, Treasury cited budget constraints on hiring and the Reserve Bank of Cleveland cited time constraints on recruitment practices as challenges. Additionally, NCUA cited as a challenge establishing tracking systems to help identify barriers to recruiting, hiring, and retaining minorities.

Dodd-Frank Requirements Are Being Implemented, but Enhanced Reporting of Efforts to Measure Progress Is Needed

Federal financial agencies and Reserve Banks have begun implementing key requirements of section 342 of the Dodd-Frank Act. First, all agencies and Reserve Banks have established OMWIs. Most agencies and all of the Reserve Banks used existing policies to establish standards for equal employment opportunity required by the act. Although many agencies and Reserve Banks had been using recruitment practices required by the act prior to its enactment, the majority of OMWIs have expanded these or initiated other practices. In addition to meeting requirements regarding their diversity policies, the federal financial agencies have taken preliminary steps to develop procedures for assessing the diversity policies and practices of entities they regulate, as required under the act. Finally, nearly all the agencies and all of the Reserve Banks are reporting annually on their diversity practices. While many OMWIs have implemented or are planning efforts to measure and evaluate the progress of their diversity and inclusion activities, information on such efforts is not yet reported consistently across the OMWI annual reports. Such information could enhance their efforts to report on measuring outcomes and the progress of their diversity practices.

Agencies and Reserve Banks Have Established Offices of Minority and Women Inclusion and Diversity Standards

All federal financial agencies and all Reserve Banks have established an OMWI. Six of the seven agencies that existed when the Dodd-Frank Act was enacted established OMWIs by January 2011, pursuant to the time frame established in the act. Additionally, SEC formally established its OMWI in July 2011, following House and Senate Appropriations Committees' approvals of the agency's request to create an OMWI.[32] SEC selected an OMWI director in December 2011, who officially joined the office in January 2012. CFPB, which assumed responsibility for certain consumer financial protection functions in July 2011, established its OMWI in January 2012 and its OMWI director officially joined the agency in April 2012.[33]

Many agencies and most of the Reserve Banks established their OMWIs as new, separate offices. Four of eight agencies and 9 of 12 Reserve Banks established their OMWIs separate from other offices, including four banks that refocused existing diversity offices as their OMWIs. Three agencies—FDIC, the Federal Reserve Board, and OCC—and three banks—the Reserve Banks of Atlanta, Kansas City, and Philadelphia—established their OMWIs within existing offices of equal employment opportunity (EEO) or diversity. FHFA established its OMWI and then merged its EEO function into that office. OMWI officials from several agencies with separate OMWIs said their staff worked with their EEO offices to address agency diversity issues. Similarly, many agency and Reserve Bank OMWI officials said they coordinated with other offices across their organizations, such as human resources, recruiting, procurement, and management, to support ongoing diversity and inclusion efforts organizationwide.

Federal financial agencies and Reserve Banks all have taken steps to staff their OMWIs. As of January 2013, the agencies had allocated

[32]SEC determined it could not use appropriated funds for the purpose of establishing an OMWI without first obtaining congressional approval. Its reprogramming request was approved by the House and Senate Appropriations Committees in July 2011.

[33]As mentioned previously, on July 21, 2010, the Consumer Financial Protection Act of 2010 established CFPB as an independent bureau within the Federal Reserve System to be headed by a director. Effective July 21, 2011, CFPB assumed responsibility for certain consumer financial protection functions formerly the responsibilities of the Board of Governors of the Federal Reserve System, the Comptroller of the Currency, the Director of the Office of Thrift Supervision, FDIC, the Federal Trade Commission, NCUA, and the Secretary of the Department of Housing and Urban Development. CFPB had until January 21, 2012, to establish its OMWI and begin addressing the other requirements of the act.

between 3 and 40 full-time equivalent positions to their OMWIs (see table 3), and all agencies had open positions they planned to fill among these allocated positions. FDIC had allocated 40 full-time equivalent positions to its combined OMWI/EEO office as of January 2013. Many of FDIC's OMWI staff, including eight EEO specialists, support the office's EEO functions, and OCC and FHFA also reported EEO specialists among their staff. The agency OMWIs included directors and analysts among their staff, as well as some positions specific to certain functions of the OMWIs. For example, four of the agencies—CFPB, FDIC, NCUA, and SEC—had allocated staff specifically to recruitment and outreach functions, and four of the agencies—NCUA, OCC, SEC, and Treasury—had allocated staff specifically to business and supplier diversity. Four agencies—the Federal Reserve Board, FHFA, NCUA, and OCC—had each allocated a position to help implement the Dodd-Frank Act requirement to review the diversity practices of regulated entities. Additionally, two of the agencies—CFPB and SEC—had attorney positions among their OMWI staff.

Table 3: OMWI Staffing Levels for Federal Financial Agencies, as of January 2013

Agency	Allocated	Filled
CFPB	4	3
Federal Reserve Board[a]	3	2
FDIC[a]	40	35
FHFA[a,b]	9	8
NCUA	6	5
OCC[a]	12	11
SEC[c]	9	8
Treasury	11	8

Source: GAO analysis of federal financial agency information.

[a]Totals for FDIC, FHFA, and OCC include EEO staff, as the OMWI offices for these agencies include both functions. The Federal Reserve Board also established its OMWI within an existing office, but it provided information for OMWI staff only and excluded the office's director position, as agency officials said additional funds for the director position were not allocated because the director's primary duties included overseeing EEO compliance, diversity, and inclusion.

[b]Totals for FHFA include part-time staff.

[c]In addition to these staff, SEC's OMWI is supported by two full-time contract positions, a program analyst and a recruitment coordinator.

The Reserve Banks had allocated between three and seven full-time equivalent positions to their OMWIs as of January 2013 (see table 4). Ten of the 12 Reserve Banks had filled all of these positions, while the

Reserve Banks of Cleveland and St. Louis each had one open position. The Reserve Bank OMWIs included directors and analysts among their staff. Few Reserve Banks designated specific OMWI functions to certain positions. Three banks, the Reserve Banks of Atlanta, Boston, and St. Louis, had each allocated one position to supplier or business diversity, and two other banks, the Reserve Banks of Chicago and Cleveland, had each allocated one position to help carry out the reporting functions of the OMWIs.

Table 4: OMWI Staffing Levels for Reserve Banks, as of January 2013

Reserve Bank	Allocated	Filled
Atlanta[a]	4.5	4.5
Boston	5	5
Chicago	7	7
Cleveland	4	3
Dallas[b]	4	4
Kansas City[b]	5	5
Minneapolis[b]	3	3
New York	5	5
Philadelphia[b]	3	3
Richmond	5	5
San Francisco	3	3
St. Louis	5	4

Source: GAO analysis of Reserve Bank information.

[a]Totals for the Reserve Bank of Atlanta include part-time staff.

[b]Totals for the Reserve Banks of Dallas, Kansas City, Minneapolis, and Philadelphia include full-time employees with shared duties that help support the OMWI.

Perspectives on the role of OMWIs varied across some Reserve Bank officials with whom we spoke. While several Reserve Bank officials said their OMWIs were involved in policy development with a commitment to improving the Reserve Bank's diversity efforts over time, officials from one Reserve Bank said their OMWI was compliance-focused and primarily analyzed the banks' human capital resources and recruiting functions for compliance with Dodd-Frank Act requirements. Reserve Bank of Dallas officials told us they considered the OMWI staff members as objective critics of the Reserve Bank's recruitment, procurement, and financial education efforts, and that bank management is responsible for fostering diversity and inclusion across the organization.

The act also required federal financial agency and Reserve Bank OMWIs to develop standards for equal employment opportunity and the racial, ethnic, and gender diversity of the workforce and senior management.[34] Six of eight agencies and most Reserve Banks indicated either their previously established equal employment opportunity standards or MD-715 requirements for agencies helped satisfy the Dodd-Frank Act requirement to establish equal employment opportunity standards with minimal changes, while two agencies and one Reserve Bank were still determining how to respond to the requirement. Treasury and CFPB planned to develop benchmarks of best practices as standards for diversity and inclusion. For example, Treasury officials said they planned to identify qualitative measures or indicators for assessing workforce diversity practices. Additionally, the Reserve Banks of Kansas City and San Francisco revised their diversity and inclusion policies pursuant to Dodd-Frank Act requirements. One agency established new standards separate from its existing equal employment opportunity policies as standards for the diversity of the workforce and senior management. Specifically, NCUA developed a diversity and inclusion strategic plan in response to a government-wide executive order that provides diversity standards and goals, which officials said the agency used to help establish expectations for staff.[35]

Agencies and Reserve Banks Are Implementing Recruitment Practices

OMWI Annual Reports to Congress and officials we contacted indicated that federal financial agencies and Reserve Banks have implemented various practices pursuant to the Dodd-Frank Act's requirements regarding diversity recruiting, outlined in table 5. Most agency and Reserve Bank OMWIs indicated that they had been conducting various diversity recruitment practices prior to the enactment of the Dodd-Frank Act—such as partnering with organizations focused on developing opportunities for minorities and women.

[34] Pub. L. No. 111-203. § 342(b)(2) (2010).

[35]Exec. Order 13583 (2011).

Table 5: Federal Financial Agency and Reserve Bank Implementation of Dodd-Frank Act Section 342 Diversity Recruitment Requirements

Section	Requirement	Agency and Reserve Bank implementation efforts
Sec. 342(f)(1)	Recruiting at historically black colleges and universities, Hispanic-serving institutions, women's colleges, and colleges that typically serve majority minority populations	Seven of eight agencies and all Reserve Banks reported on efforts to recruit from historically black colleges and universities and other minority-serving institutions. Additionally, a few Reserve Banks reported on regional diversity recruitment efforts that included recruiting from two California State University locations that serve Latino communities.
Sec. 342(f)(2)	Sponsoring and recruiting at job fairs in urban communities	All agencies and all Reserve Banks participated in diversity job fairs sponsored by minority-serving groups. These practices included participating in national job fairs sponsored by the National Urban League, National Black MBA Association, National Association of Black Accountants, National Society of Hispanic MBAs, Association of Latino Professionals in Finance and Accounting, Society for Women Engineers, National Association of Asian MBAs, and the Pacific Asian Consortium in Employment.
Sec. 342(f)(3)	Placing employment advertisements in newspapers and magazines oriented toward minorities and women	Five agencies and all Reserve Banks reported on efforts to place advertisements in minority- and women-serving publications. These included posting jobs in IMDiversity, Hispanic Business, EOE Journal, Diversity Life, Diversity Women, and Hispanic Life magazines.
Sec. 342(f)(4)	Partnering with organizations focused on developing opportunities for minorities and women to place talented young minorities and women in industry internships, summer employment, and full-time positions	Seven agencies and all Reserve Banks have partnerships with organizations for internship programs, including the Hispanic Association of Colleges and Universities, Washington Internships for Native Students, and INROADS, a nonprofit organization that trains and develops minority students for careers in business and industry.
Sec. 342(f)(6)	Any other mass media communications that the OMWI determines necessary	Two agencies and all Reserve Banks identified additional mass media communications to support their diversity recruiting efforts, including using social media networking sites such as Facebook and Twitter to reach diverse candidates. For example, CFPB created a recruitment website based on the agency's review of best practices for developing diverse applicant pools, and the Federal Reserve System (the Board and all the Reserve Banks) maintains a presence on the LinkedIn networking website.

Source: GAO summary of Dodd-Frank Act section 342 and information provided by federal financial agencies and Reserve Banks.

Note: Sec. 342(f)(5) pertains to partnering with inner-city high schools, girls' high schools, and majority-minority population high schools to establish or enhance financial literacy programs and provide mentoring and is not included in this list or addressed in this report.

The majority of agencies and Reserve Banks focused their recruitment efforts on attending job fairs and maintaining partnerships with minority-serving institutions and organizations. According to Federal Reserve Board and Reserve Bank officials, they collectively participate in and fund recruitment activities, including national career fairs, advertisements in diverse publications, and social media initiatives. The Reserve Bank of Chicago coordinates the Federal Reserve System's participation in national diversity recruitment events and oversees an internal training

initiative aimed at developing and retaining employees within the Federal Reserve System. In addition to participating in these efforts, Reserve Banks conduct some activities independently.

Some OMWIs indicated their diversity activities had changed due in part to recent efforts to satisfy section 342 requirements as well as broadening their approaches to diversity and inclusion. For example, some OMWIs indicated the scope of their diversity and inclusion practices had broadened to include persons with disabilities as well as the lesbian, gay, bisexual, and transgender community. Further, the majority of OMWIs reported on plans to improve or expand existing practices. For example, many OMWIs described plans to pursue new or further develop existing partnerships with organizations focused on developing opportunities for minorities and women, and some OMWIs described recent efforts to expand internship opportunities for minority students.

Some OMWI officials identified practices targeted to improve organizationwide diversity, which could eventually help build management-level diversity. These included targeted recruitment to attract minorities and women, training for hiring managers and other employees on diversity hiring practices, and expanded internship programs as a way to hire a greater number of female and minority interns.

- *Targeted recruitment.* All agencies and Reserve Banks with whom we spoke had participated in career fairs or partnerships with minority-serving organizations, as outlined in section 342 of the Dodd-Frank Act, to target diversity recruitment, and in several cases bolster recruitment of particular populations, such as Hispanics. The OMWIs at FDIC, FHFA, and SEC work with the agencies' hiring and recruitment staff to identify strategies for recruiting diverse candidates. Additionally, the Federal Reserve Board OMWI reported that including hiring managers at diversity career fairs had made their targeted recruitment activities more effective.

- *Training for hiring managers*. Some OMWIs reported they implemented practices to educate supervisors and hiring managers on diversity hiring practices. For example, the Reserve Bank of New York designed a training course to enhance cross-cultural interviewing skills of recruitment staff. OCC also provides diversity recruitment training to the agency's recruitment staff, and CFPB planned to

provide its hiring managers a toolkit with tips on diversity hiring practices.

- *Internship programs*. Many agencies and Reserve Banks implemented internship programs to build employment diversity by developing a more diverse pipeline of potential entry-level candidates. For example, the Reserve Bank of San Francisco reported that it expanded its internship program to support more interns and leveraged partnerships with organizations representing minorities and women to increase the diversity of the bank's internship program applicant pool.

Agencies Have Taken Preliminary Steps to Develop Procedures to Assess Diversity Policies and Practices of Regulated Entities

In response to section 342 of the Dodd-Frank Act, seven federal financial agencies have taken preliminary steps to respond to the requirement to develop standards for assessing the diversity policies and practices of entities they oversee. While these agencies have made initial progress, it is too soon to evaluate how effectively the agencies are responding to this requirement. The affected agencies include CFPB, FDIC, FHFA, the Federal Reserve Board, NCUA, OCC, and SEC.[36] In addition to this requirement under the Dodd-Frank Act, FHFA is also subject to the Housing and Economic Recovery Act of 2008 (HERA), under which it must assess its regulated entities' diversity activities and meet other provisions similar to those in section 342.[37]

[36]Although this report reviews eight federal agencies, this requirement does not apply to Treasury Departmental Offices, as the agency does not have regulated entities. Additionally, the requirement does not directly apply to the Reserve Banks. However, the Federal Reserve Board has delegated some of its supervisory responsibilities to the Reserve Banks—such as responsibility for examining bank and thrift holding companies and state member banks under rules, regulations, and policies established by the Federal Reserve Board. The scope of these delegated authorities does not include section 342 oversight of regulated entities at this time.

[37]Pub. L. No. 110-289 § 1116, 122 Stat. 2654, 2681-2683 (2008). Under HERA, FHFA's regulated entities must establish an OMWI and develop and implement standards and procedures to ensure, to the maximum extent possible, the inclusion and utilization of minorities and women, and minority- and women-owned businesses in all business and activities of the regulated entity at all levels, including in procurement, insurance, and all types of contracts. Additionally, each of its regulated entities must report annually to FHFA on actions taken pursuant to these requirements. Further, the act requires FHFA to take affirmative steps to seek diversity in its workforce at all levels, consistent with the demographic diversity of the United States.

In 2010, FHFA developed an agency regulation implementing HERA requirements, in part, to ensure that diversity is a component of all aspects of its regulated entities' business activities. The agency's regulated entities include Fannie Mae, Freddie Mac, Federal Home Loan Banks, and the Federal Home Loan Bank System's Office of Finance. HERA requires the agency's regulated entities to develop diversity policies and procedures, staff an OMWI, and report annually to FHFA on their OMWI activities, among other requirements.[38] In addition, FHFA has enforcement authority under HERA and FHFA's promulgated regulation to ensure its regulated entities have diversity standards in place. According to FHFA OMWI officials, the agency's response to HERA also satisfies the section 342 requirement.

According to OMWI officials, other agencies reviewed FHFA's regulation as a possible option for responding to the section 342 requirement; however, the enforcement authority included in FHFA's regulation is unique to the agency. They said that under the Dodd-Frank Act their agencies do not have enforcement authority to require regulated entities to implement diversity standards and practices.[39] Officials from the affected agencies also told us their OMWIs collaborated on initial steps to determine how to respond to these requirements by meeting periodically as a group, meeting with members of Congress, and performing outreach to industry participants and advocacy groups.

The agency OMWI directors began meeting periodically in 2011 and began in 2012 to explore the possibility of developing a uniform set of standards that agencies could use as a baseline for developing standards for assessing the diversity practices of their regulated entities. Agency OMWI officials said the working group aimed to develop a set of standards for review and feedback from industry participants. As part of these efforts, some OMWI directors of the affected agencies participated in meetings with members of Congress to explore issues involving collection and analysis of workforce diversity data. Some members of the working group also held meetings with industry and advocacy groups to

[38]Minority and Women Inclusion. 12 C.F.R. § 1207.1 -24 (Dec. 28, 2010).

[39]Pub. L. No. 111-203. § 342(b)(4) (2010). Even though section 342 provides for the development of standards for the assessment of diversity policies and practices of regulated entities, it further provides that nothing in the requirement may be construed to require any specific action based on the findings of the assessment.

understand industry views on developing standards for assessing diversity policies and practices. One OMWI reported that industry representatives discussed options for evaluating diversity with respect to a regulated entity's size, complexity, and market area.

OMWI officials told us responding to the requirement was a challenge for several reasons. Specifically, differences across regulated entities in terms of size, complexity, and market area made it challenging to develop a uniform standard. Determining the process and format for developing standards was also a challenge. OMWI officials also said they want to minimize adding a new regulatory burden to meet this provision. Therefore, the agencies would like to leverage existing information sources—data that regulated entities already provide—in evaluating the diversity activities of regulated entities. For example, to find ways to avoid duplicating existing data-collection efforts, CFPB and NCUA were working with EEOC for access to EEO-1 data for regulated entities. OCC officials said OCC had also considered using EEO-1 data, but some regulated entities had concerns about maintaining proprietary information, given the potential for Freedom of Information Act requests.[40]

Efforts to Report on Measuring Outcomes and Progress Could Be Enhanced

In addition to establishing an OMWI, the act required federal financial agencies and Reserve Banks to report annually on their diversity practices, and nearly all of the agencies and all the Reserve Banks have begun reporting annually on their diversity practices. As discussed earlier, the act required each OMWI to submit to Congress an annual report on the actions taken pursuant to section 342, including information on the percentage of amounts paid to minority-and women-owned contractors and successes and challenges in recruiting and hiring qualified minority and women employees, and other information as the OMWI director determines appropriate. Including more information on the outcomes and progress of their diversity practices could enhance the usefulness of these annual reports. Seven of eight agencies and all Reserve Banks issued annual reports in 2011. CFPB, which was created in July 2010 and assumed responsibility for certain consumer financial protection functions in July 2011, issued an agencywide semiannual report for 2011. Its OMWI

[40] 5 U.S.C. § 552. The Freedom of Information Act requires that federal agencies provide the public with access to government records and information on the basis of the principles of openness and accountability in government.

planned to issue an annual report for 2012 at the same time as the other agencies, in March 2013.

In their 2011 Annual OMWI Reports to Congress, several agencies and Reserve Banks reported on efforts to measure outcomes and progress of various diversity practices, which provide examples of the types of outcomes and measures of progress that could be helpful for OMWIs to include in their annual reports. Although the act requires information on successes and challenges, it does not specifically require reporting on effectiveness; however, the act provides some leeway to the federal financial agencies and the Reserve Banks to include "any other information, findings, conclusions, and recommendations for legislative or agency action, as the Director determines appropriate."[41] Measurement of diversity practices is one of the nine leading diversity management practices we previously identified. We have reported that quantitative measures—such as tracking employment demographic statistics—and qualitative measures—such as evaluating employee feedback survey results—could help organizations translate their diversity aspirations into tangible practice.[42]

The Federal Reserve Board reported that it tracks job applicant information to assess the diversity of applicant pools, candidates interviewed, and employees hired as a result of diversity recruiting efforts, and FDIC reported that it monitors participation and attrition rates and diversity characteristics of participants in a development program. SEC reported plans to develop standards for assessing its ongoing diversity and inclusion efforts and include them in a strategic plan. The Reserve Banks of Chicago, Philadelphia, Richmond, and San Francisco reported on the number of internships each bank supported and the ethnic and gender diversity of the interns. The Reserve Bank of Chicago also reported on the number of job offers extended and candidates hired from its internship program, as well as on the number of candidates successfully hired from a diversity career expo. Further, the Reserve Bank of Cleveland identified reporting tools developed to monitor the bank's inclusion in contracting efforts. In addition to using these measures, some OMWI officials said they used annual employee surveys as a measurement tool to gather information about the progress of their

[41]Pub. L. No. 111-203, § 342(e)(5) (2010).

[42]GAO-05-90.

diversity practices, including retention practices. For example, FDIC's annual employee survey includes specific questions related to diversity, and the agency uses responses to assess the effectiveness of policies and programs and outline action steps for improvement. OCC officials told us the government-wide federal employee viewpoint survey provided information on employee perspectives about diversity, and the agency measured its results against government-wide scores. Further, OMWI officials from the Reserve Bank of Minneapolis said exit surveys and employee declination surveys provided additional information for evaluating their retention and recruiting programs.

Federal financial agencies and Reserve Banks have focused their initial OMWI efforts on implementing section 342 of the Dodd-Frank Act. While many OMWIs have implemented or are planning efforts to measure and evaluate the progress of their diversity and inclusion activities, which is consistent with the leading diversity management practices, information on such efforts is not yet reported consistently across the OMWI annual reports. According to OMWI officials as well as industry representatives we interviewed, measuring the progress of diversity recruitment and retention practices is a challenging, long-term process. For example, NCUA officials told us measuring the progress of certain recruiting practices could be a challenge, as access to demographic information about job applicants might be limited. Additionally, FHFA officials told us that while measuring the progress of diversity practices was needed to identify best practices, such measurement needs to be efficient and meaningful. However, without knowledge of OMWI efforts to measure outcomes and the progress of their diversity practices, Congress lacks information that would help hold OMWIs accountable for achieving desired outcomes. In addition, increased attention to evaluation and measurement through annual reporting of these efforts could help the OMWIs improve management of their diversity practices. Reporting such information would provide an opportunity for the agencies and Reserve Banks to learn from others' efforts to measure their progress and indicate areas for improvement.

Procedures to Meet Dodd-Frank Inclusive Contracting Requirements Are Largely in Place

Section 342 of the Dodd-Frank Act requires federal financial agencies and Reserve Banks to develop procedures to ensure, to the maximum extent possible, the fair inclusion and utilization of women and minorities in contracting. Specifically, the act requires agency and Reserve Bank actions to ensure that its contractors are making efforts to include women and minorities in their workforce. Also, the act has requirements for actions to increase contracting opportunities for minority- and women-owned businesses (MWOB).[43] Most agencies and Reserve Banks have developed and included a provision in contracts for services requiring their contractors to make efforts to ensure the fair inclusion of women and minorities in their workforce and subcontracted workforces. The extent to which these agencies and Reserve Banks have contracted with MWOBs varied widely. These entities reported multiple challenges to increasing contracting opportunities for MWOBs and used various technical assistance practices to address these challenges.

Most Agencies and Reserve Banks Are Implementing Requirements Related to Inclusiveness in Contractor Workforces

To address the act's requirement to ensure the fair inclusion of women and minorities, to the maximum extent possible, in contracted workforces, agencies either have developed or are in the process of developing fair inclusion provisions in their contracts for services, and all Reserve Banks have done so. In addition, some agencies and all Reserve Banks have developed procedures to assess contractors' efforts for workforce inclusion of women and minorities.

Fair Inclusion Provision in Contracts

Five agencies—FDIC, FHFA, NCUA, OCC, and the Federal Reserve Board—and all Reserve Banks have created a fair inclusion provision and are using it in contracts for services. Section 342 of the Dodd-Frank Act requires agencies and Reserve Banks to develop procedures for review and evaluation of contract proposals for services and for hiring service providers that include a written statement that the contractor, and as applicable subcontractors, shall ensure, to the maximum extent possible, the fair inclusion of women and minorities in the workforce of the contractor and, as applicable, subcontractors. The act does not specify

[43]For purposes of the act, minority-owned business means a business for which more than 50 percent of the ownership is held by one or more minority individuals and more than 50 percent of net profit and loss of the business accrues to one or more minority individuals. Women-owned business means a business for which more than 50 percent of the ownership is held by one or more women, more than 50 percent of the net profit or loss of the business accrues to one or more women, and a significant percentage of senior management positions are held by women.

the elements to be included in the written statement and provides that each OMWI director prescribe the form and content of the statement.

CFPB, SEC, and Treasury are each in the process of developing a fair inclusion provision. CFPB is developing procurement procedures to address the requirements of the act and required more time because its OMWI office was established in January 2012. SEC is subject to the Federal Acquisition Regulation (FAR) and is currently developing its inclusive contract provision.[44] While CFPB and SEC develop inclusion statements pursuant to the act, both agencies have been using the equal employment opportunity statement contained in the FAR in executed contracts. Treasury has developed its fair inclusion provision to add to future contracts. It has issued a notice of proposed rulemaking in the Federal Register for public comments on this change to its contracting procedures as required under the law. The comment period ended on October 22, 2012. Treasury received eight comments which included, among other things, suggestions to make the fair inclusion provision applicable to all contracts regardless of the dollar amount of the contract and to better specify the documentation required of contractors to demonstrate that they have met the requirements of the fair inclusion provision. Treasury is currently reviewing the public comments and considering changes to the proposed rule.

The fair inclusion provisions we reviewed contained the following:

- *Equal employment opportunity statement:* Fair inclusion provisions include a commitment by the contractor to equal opportunity in employment and contracting and, to the maximum extent possible consistent with applicable law, the fair inclusion of women and minorities in the contractor's workforce.

[44]The FAR is the primary regulation for use by all federal executive agencies in their acquisition of supplies and services with appropriated funds. Two federal financial agencies subject to the contracting provisions in section 342 of Dodd-Frank are also governed by the FAR because they receive appropriated funds: SEC and Treasury. The other agencies included in this report are not legally required to follow the FAR because they do not receive appropriated funds. However, according to CFPB, FDIC, FHFA, and OCC these agencies choose to adhere to part or all of this regulation. According to NCUA, it used the FAR as guidance when establishing its contracting procedures. The Federal Reserve Board described their procurement policy as consistent with the FAR.

- *Documentation:* To enforce the fair inclusion provision, agencies require contractors to provide documentation of their efforts to include women and minorities in the contractor's workforce, such as a written affirmative action plan; documentation of the number of employees by race, ethnicity, and gender; information on subcontract awards, including whether the subcontractor is an MWOB; and any other actions describing the contractor's efforts toward the inclusion of women and minorities.

- *Contract amount threshold:* Agencies apply the fair inclusion provision to contracts exceeding a certain dollar amount. For two agencies subject to the act, this threshold is any amount over $150,000. For three agencies subject to the act, this threshold is any amount over $100,000. The Reserve Bank fair inclusion provisions we reviewed did not generally include a dollar-amount threshold.

None of the officials from five agencies that have implemented a fair inclusion provision required by the act described to us receiving an adverse reaction from contractors, but officials from a majority of the Reserve Banks we spoke with described resistance or concerns from some contractors. OCC stated that smaller businesses had expressed confusion about the requirement because the businesses are too small to report workforce demographics to EEOC. Eight Reserve Banks described contractors expressing some disagreement or concern at the inclusion of the language in contracts. According to some Reserve Bank officials, contractors were concerned that accepting the fair inclusion provision would trigger other federal requirements for their businesses, or subject the contractor to meeting hiring or subcontracting targets.[45] Some Reserve Banks described explaining the limited scope of the provision to concerned contractors. Other Reserve Banks described modifying the language in the fair inclusion provision, for example, in one case, changing a phrase regarding the contractor's efforts to include women and minorities from "to the maximum extent possible" to read "to the maximum extent required by law." Other Reserve Banks described occurrences where, in response to a contractor's concern, they excluded the fair inclusion language from contracts for a procurement with a small dollar amount or because the vendor provided a service critical to the

[45]As previously discussed, the Reserve Banks are not federal agencies.

Reserve Bank and alternate vendors were not available.[46] Finally, one Reserve Bank described declining a contract and seeking an alternate vendor that accepted the provision.

Procedures to Assess Contractors' Inclusion Efforts

Some agencies and all Reserve Banks have developed procedures to assess contractors' efforts toward workforce inclusion of women and minorities. Section 342 of the Dodd-Frank Act requires the 8 federal financial agencies in the act and 12 Reserve Banks to develop procedures to determine whether a contractor and, as applicable, a subcontractor, has failed to make a good faith effort to include minorities and women in their workforces. Good faith efforts include any actions intended to identify and remove barriers to employment or to expand employment opportunities for minorities and women in the workplace, according to the policies some agencies have developed. For example, recruiting minorities and women or providing these groups job training may be considered good faith efforts for diversity inclusion. Contractors must certify that they have made a good faith effort to include women and minorities in their workforces, according to most policies we reviewed. At the same time, contractors may provide documentation of their inclusion efforts such as workforce demographics, subcontract recipients, and the contractor's plan to ensure that women and minorities have opportunities to enter and advance within its workforce. Agencies and Reserve Banks plan to conduct a review of each contractor's certifications and documentation annually, once in a 2-year period, or at other times deemed necessary, such as when contracts are executed or renewed, to make a determination of whether the contractor made a good faith effort to include women and minorities in its workforce. Failure to make a good faith effort may result in termination of the contract, referral to the Office of Federal Contract Compliance Programs, or other appropriate action.[47] Four agencies and all Reserve Banks have established good faith effort

[46]According to one Reserve Bank, there are certain types of contracts from which the fair inclusion provision would be automatically excluded. For example, the Reserve Bank of Chicago would not include the provision in a new contract with a vendor that has an existing contract with the National Procurement Office of the Federal Reserve System because in that previous contract the vendor had already agreed to make efforts to include women and minorities in its workforce.

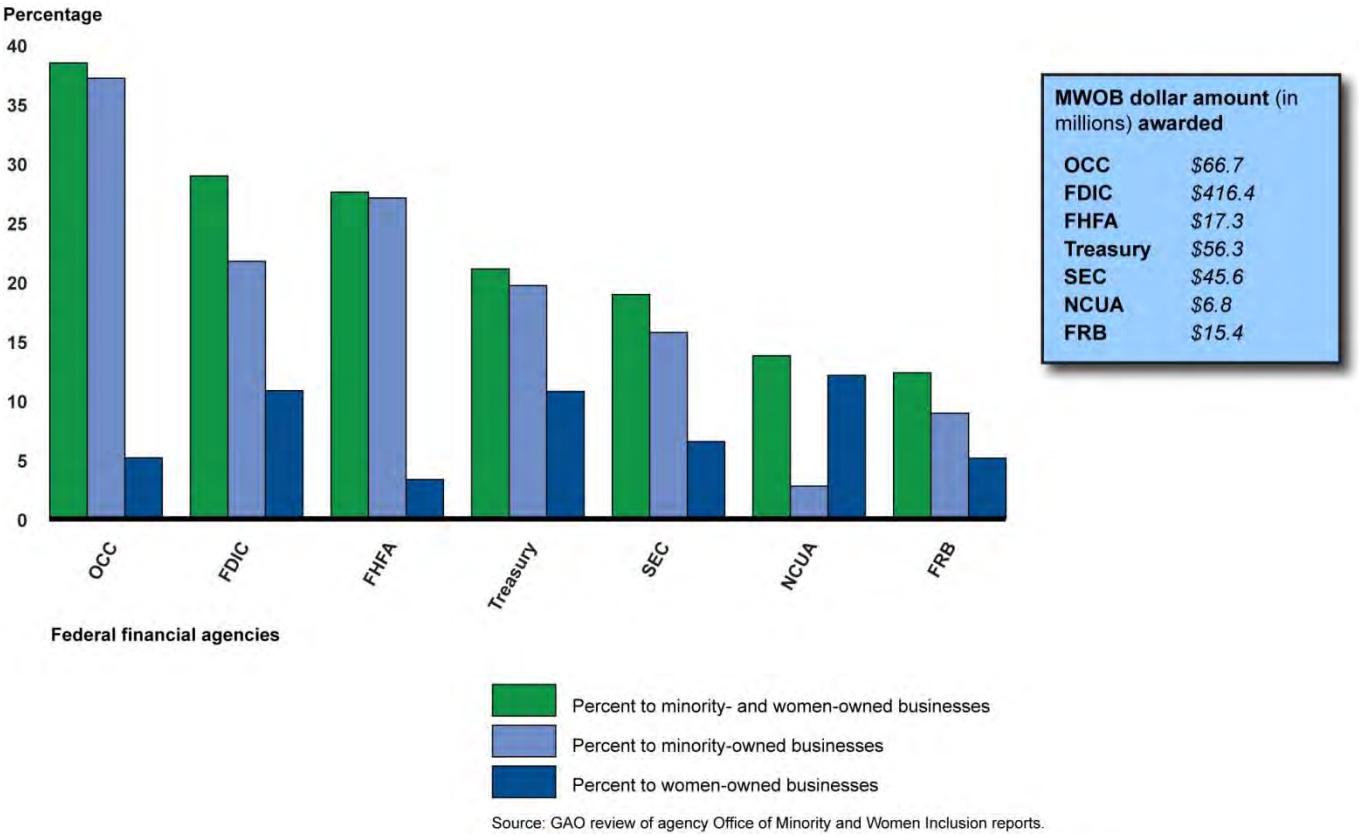
[47]The Office of Federal Contract Compliance Programs enforces, for the benefit of job seekers and wage earners, the contractual promise of affirmative action and equal employment opportunity required of those who do business with the federal government.

determination procedures, and four agencies have yet to implement such procedures.

Levels of Contracting with Minority- and Women-Owned Businesses Varied by Agency and Reserve Bank

In 2011, the proportion of a federal financial agency's contracting dollars awarded to businesses owned by minorities or women varied, ranging between 12 percent and 38 percent according to the OMWI reports of the agencies (see fig. 14).[48] Seven federal financial agencies awarded a total of about $2.4 billion for contracting for external goods and services in fiscal year 2011, with FDIC awarding about $1.4 billion of this amount.

Figure 14: Dollar Amount and Percentage of Total Awarded to Minority- and Women-Owned Businesses (MWOB) by Agency, 2011



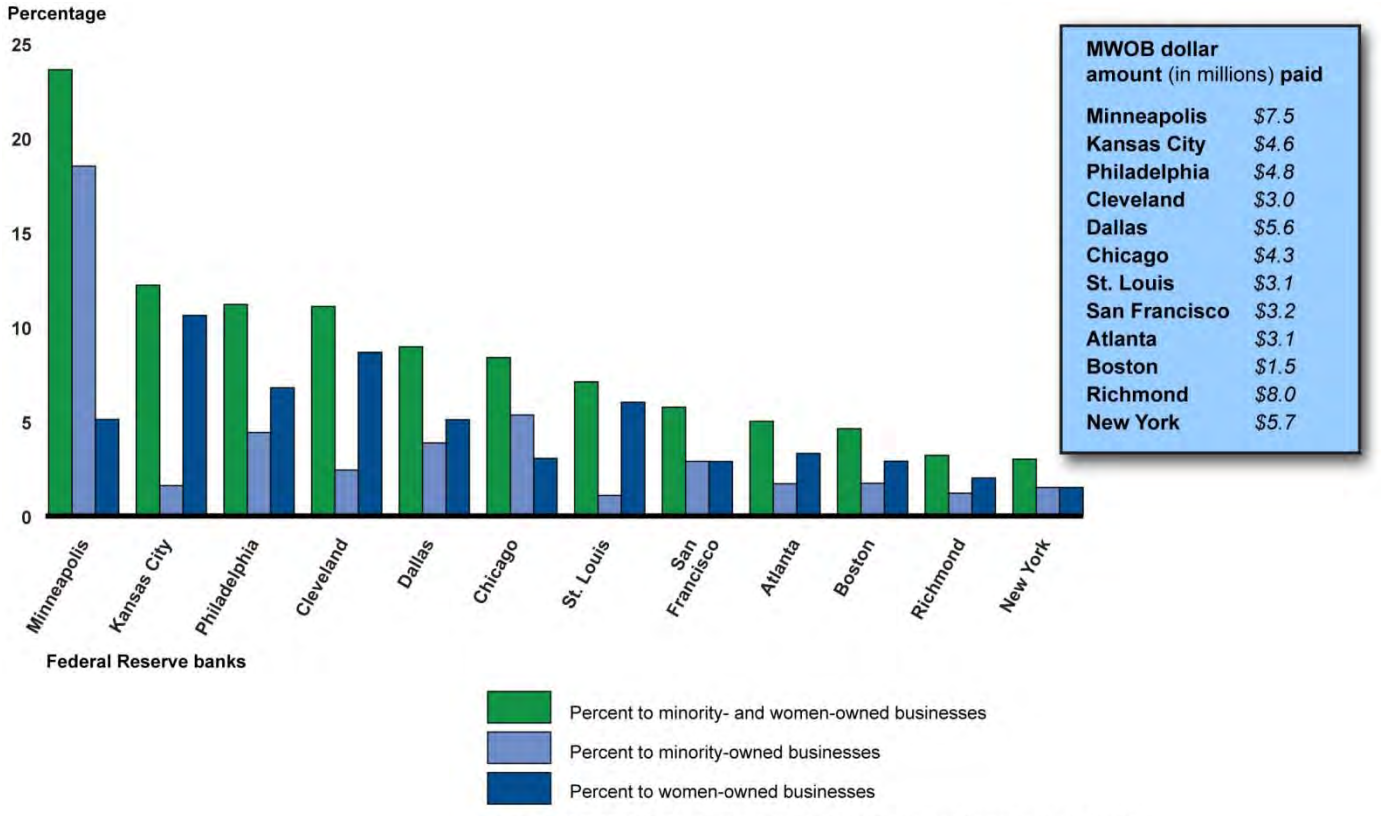
Source: GAO review of agency Office of Minority and Women Inclusion reports.

[48]The act does not set a standard that the federal agencies or Reserve Banks must meet in making contracting awards to MWOBs.

Note: CFPB was not required to issue an OMWI report to Congress in 2011. Percentages of dollar amounts awarded to minority-owned businesses and women-owned businesses displayed separately may not be mutually exclusive for all agencies and do not always total to the combined percent to minority- and women-owned business category. Some businesses are both minority- and women-owned and may be counted by agencies under both categories.

Similarly, according to Reserve Bank OMWI reports, Reserve Bank contracting dollars paid to businesses owned by minorities or women ranged between 3 percent and 24 percent in 2011 (see fig. 15). Reserve Banks paid about $897 million in fiscal year 2011 in contracting.

Figure 15: Dollar Amount and Percentage of Total Paid to Minority- and Women-Owned Businesses (MWOB) by Reserve Bank, 2011



Source: GAO review of Federal Reserve Bank Office of Minority and Women Inclusion reports.

Note: Reserve Banks reported amounts paid to contractors in OMWI reports rather than amounts awarded as reported by agencies.

Among federal financial agencies, OCC awarded the largest proportional amount of contracting dollars to MWOBs—about 38 percent (almost $67 million). OCC officials told us that its contract needs tend to be for

services for which there is often a pool of MWOB suppliers and most of OCC's 2011 contract dollars were spent on computer related services. The Federal Reserve Board awarded the smallest proportion of its contracting dollars to MWOBs, with about 12 percent going to such businesses. According to the Federal Reserve Board, a significant amount of its procurement is for economic data, which are generally not available from MWOBs. Although federal agencies are not generally required to report on MWOBs, most are required to report on certain small business contracting goals, including goals for women and small disadvantaged businesses (which include minority-owned businesses).[49] In a 2012 report, we found that 35 percent of funds all federal agencies obligated to small businesses in 2011 were obligated to minority-owned small businesses and 17 percent were obligated to women-owned businesses.[50]

Among Reserve Banks, the Reserve Bank of Minneapolis paid the largest proportion of its contracting dollars to MWOBs with about 24 percent going to such businesses (18.5 percent to minority-owned businesses and about 5 percent to women-owned businesses). According to the Reserve Bank of Minneapolis, almost half of its MWOB contract dollars were paid for software and related technology integration services from minority-owned firms. All other Reserve Banks paid under 13 percent of contracting dollars to MWOBs, with the Reserve Bank of New York awarding the smallest percentage of its contracting dollars to such businesses (3 percent). The Reserve Bank of New York described its commitment to increasing diversity in its pool of potential contractors through its outreach efforts to us and in its 2011 OMWI report. For example, the Reserve Bank of New York held an event with its primary

[49]The Small Business Administration (SBA) negotiates goals with federal agencies for contract dollars awarded to small businesses to meet statutory government-wide goals. 15 U.S.C. § 664(g) sets forth a statutory goal for 23 percent of all aggregated federal contracting dollars to be awarded to small businesses. These include current goals for 5 percent of all prime contract and subcontract dollars to be awarded to small disadvantaged businesses and 5 percent of all prime contract and subcontract dollars to be awarded to women-owned small businesses. SBA also negotiates goals for the award of contract dollars to service-disabled veteran-owned and HUBZone small businesses.

[50]See GAO, *Government Contracts: Federal Efforts to Assist Small Minority Owned Businesses*, GAO-12-873 (Washington, D.C.: Sept. 28, 2012). We analyzed data from the Federal Procurement Data System—Next Generation. Minority designations are self-reported, and some businesses are both minority- and women-owned and may be counted under both categories.

contractors and small firms to identify potential partnerships and an event that provided small firms consultation on business plans and credit applications to increase the capacity of the small firms.

Agencies and Reserve Banks Report Challenges to Increasing Contracting Opportunities and Have Offered Technical Assistance to Minority- and Women-Owned Businesses

Seven federal financial agencies included in this report and all 12 Reserve Banks identified challenges in increasing contracting opportunities for MWOBs. Section 342 of the Dodd-Frank Act requires federal financial agencies and Reserve Banks to include in their annual OMWI report a description of the challenges they may face in contracting with qualified MWOBs. As a new agency, CFPB has not been required to complete an annual OMWI report and did not identify any contracting challenges to us. In interviews with us and in the 2011 OMWI reports to Congress, the remaining agencies and all Reserve Banks discussed a number of common challenges to increasing contracting with MWOBs, including the following:

- *Limited capacity of MWOBs:* Some agencies and Reserve Banks stated that reporting or other requirements under federal contracts were often too great a burden for MWOBs or that MWOBs needed to build capacity to meet federal contracting requirements. Some agencies and Reserve Banks also stated that at times the need for goods or services is not scaled to the capacity of MWOBs. For example, some agencies and Reserve Banks faced challenges identifying MWOBs that can meet procurement needs on a national scale.

- *Developing staff or procedures to meet contracting requirements of the act:* According to some agencies, new OMWIs require additional staff or staff development, or procedures to meet the requirements of the act, including providing technical assistance to increase opportunities for MWOBs, identifying qualified MWOBs in the marketplace, and incorporating the use of a fair inclusion provision in contracts and good faith effort determination processes, which we discussed earlier, into established procurement processes.

- *MWOB classification challenges:* Multiple agencies and Reserve Banks described difficulty identifying and classifying suppliers as diverse entities. Some Reserve Banks noted that no central agency is responsible for certifying MWOBs. Some agencies and Reserve Banks also discussed a need for new procedures or information systems to identify and classify diverse ownership of businesses.

- *Availability:* Some agencies and Reserve Banks noted that specialized services are often only available from a limited pool of suppliers that may not include MWOBs.

- *Centralized procurement:* Reserve Banks may use the National Procurement Office (NPO), the centralized procurement office for the 12 Reserve Banks, to contract for some goods and services.[51] When a Reserve Bank procures through the NPO, access to MWOBs may be limited because the NPO procures for volume discounts with larger contractors. However, the Reserve Bank of Richmond, in its 2011 OMWI report, described efforts to work with existing large contractors to increase subcontracting with smaller, diverse firms.

- *No MWOB bids:* In some cases, agencies and Reserve Banks found that potentially eligible MWOB applicants decided not to bid without explanation.

Other challenges were described on a limited basis by one agency or Reserve Bank. For example, NCUA explained that MWOBs are not familiar with the agency. According to NCUA, to address this issue it increased its outreach budget and attendance to MWOB events and published an online guide on doing business with the agency. According to FDIC, in some cases MWOBs do not have relationships with large federal contractors for subcontracting opportunities. To address this problem, FDIC emphasizes to larger firms the importance of subcontracting with MWOBs and has negotiated increases in MWOB subcontracting participation with large contractors. FDIC participated in procurement events where small and large contractors could meet and match capabilities. The Reserve Bank of Chicago stated that MWOBs have a hard time standing out in highly competitive industries, such as staff augmentation services. Finally, according to the Reserve Bank of Richmond, MWOBs may have incorrect perceptions that Reserve Banks are subject to federal procurement rules that they cannot meet.

To counter challenges MWOBs may face in accessing federal contracting opportunities, all agencies and Reserve Banks described providing various specific forms of technical assistance to MWOBs, which they described in discussions with us and in 2011 OMWI reports to Congress.

[51]The NPO, housed in the Reserve Bank of Richmond, conducts research and negotiates, manages, and administers contracts on behalf of the 12 Reserve Banks, but the purchases are made by the individual Reserve Bank that chooses to use the contract.

No agency or Reserve Bank stood out as coordinating technical assistance better than others, although some agencies pointed to longstanding efforts at FDIC to provide technical assistance to MWOBs as model practices. Section 342 of the Dodd-Frank Act requires federal financial agencies and Reserve Banks to develop standards for coordinating technical assistance to MWOBs. These activities included developing and distributing literature, such as manuals and brochures describing contracting procedures and resources to prospective contractors. Most agencies also established websites that function as informational portals on doing business with agencies and act as an agency entry point to prospective contractors. Agencies and Reserve Banks described outreach activities to MWOBs, including conducting expert panels, hosting meetings and workshops, and exhibiting at trade shows and procurement events. Some of these outreach activities have been coordinated with SBA. For example, FDIC has partnered with SBA to develop a technical assistance program for small businesses, including MWOBs, on money management. OCC worked with SBA to create a technical assistance workshop that they conducted in 2012 with women-owned small businesses. Some agencies have included SBA representatives in supplier diversity events they sponsor. Even prior to the passage of the Dodd-Frank Act, the Federal Reserve Board had participated in SBA procurement fairs and used SBA information and events to market its procurement opportunities among diverse suppliers. Treasury has participated in SBA outreach events and created a mentor-protégé program to assist small businesses with contracting opportunities.[52]

Agencies and Reserve Banks also provide one-on-one technical assistance, which is intended to meet the specific needs of a prospective MWOB contractor. According to Treasury, they coordinate with SBA to leverage SBA's knowledge of one-on-one technical assistance practices

[52]A mentor-protégé program is an arrangement in which mentors—businesses, typically experienced prime contractors—provide technical, managerial, and other business development assistance to eligible small businesses, or protégés. Overall, mentor-protégé programs seek to enhance the ability of small businesses to compete more successfully for federal government contracts by furnishing them with assistance to improve their performance. See GAO, *Mentor-Protégé Programs Have Policies that Aim to Benefit Participants but Do Not Require Postagreement Tracking*, GAO-11-548R (Washington, D.C.: June 15, 2011) and *Small Business Contracting: Opportunities to Improve the Effectiveness of Agency and SBA Advocates and Mentor-Protégé Programs*, GAO-11-844T (Washington, D.C.: Sept. 15, 2011).

with MWOBs. FHFA and SEC have created dedicated e-mail addresses and telephone lines for MWOBs to reach their OMWIs, and SEC has established monthly vendor outreach days when MWOBs can speak one-on-one with SEC's supplier diversity officer and small-business specialist. Some Reserve Banks described conducting one-on-one meetings with prospective contractors in 2011, some of which were held during procurement events. Finally, FDIC offered its database of MWOBs to the OMWIs and some agencies described using or planning to use it to identify potential contractors for outreach regarding procurement opportunities. According to FDIC, it sends an updated version of the database to the agencies each quarter.

Conclusion

Across financial services firms, federal financial agencies, and Reserve Banks, available data showed the representation of minorities and women varied, and there was little overall change in workforce diversity from 2007 through 2011. Our findings suggest the overall diversity of the financial services industry has generally remained steady following the financial crisis. Since 2011, federal financial agencies and Reserve Banks have taken initial steps to respond to the Dodd-Frank Act's requirements to promote workforce diversity, and OMWIs have begun reporting on both planned and existing diversity practices, in addition to reporting on workforce demographic statistics according to EEOC requirements. While many OMWIs have implemented or are planning efforts to measure and evaluate the progress of their diversity and inclusion activities, a leading diversity management practice, information on these efforts is not reported consistently across the OMWI annual reports. Although the act requires information on successes and challenges, it does not specifically require reporting on measurement; however, the act provides that the federal financial agencies and the Reserve Banks can include additional information determined appropriate by the OMWI director. Measurement of diversity practices is one of the nine leading diversity management practices we have previously identified. Reporting on these efforts as part of annual OMWI reporting would provide Congress, other OMWIs, and the financial services industry with potentially useful information on the ongoing implementation of diversity practices. Such information could be helpful industrywide, as management-level diversity at federal financial agencies, Reserve Banks, and the broader financial services industry continues to be largely unchanged. Without information on OMWI efforts to report outcomes and the progress of diversity and inclusion practices, Congress lacks information that would help hold agencies accountable for achieving desired outcomes or whether OMWI efforts are having any impact.

Recommendations for Executive Action

To enhance the availability of information on the progress and impact of agency and Reserve Bank diversity practices, we are recommending to CFPB, FDIC, the Federal Reserve Board, FHFA, NCUA, OCC, SEC, Treasury, and the Reserve Banks that each OMWI report on efforts to measure the progress of its employment diversity and inclusion practices, including measurement outcomes as appropriate, to indicate areas for improvement as part of their annual reports to Congress.

Agency Comments and Our Evaluation

We provided drafts of this report to CFPB, the Federal Reserve Board, FDIC, FHFA, NCUA, OCC, SEC, Treasury, and each of the Federal Reserve Banks for review and comment. We received written comments from each of the agencies and a consolidated letter from all of the Reserve Banks. Their comment letters are reproduced in appendixes V through XIII. The agencies and Reserve Banks generally agreed with our recommendation. CFPB, Federal Reserve Banks, FDIC, FHFA, NCUA, OCC, and SEC provided technical comments, which we incorporated as appropriate. We also provided a draft of the report to EEOC for comment. EEOC is not subject to the requirements of section 342 of the act but did provide technical comments, which we incorporated as appropriate.

With respect to our recommendation that each OMWI report on efforts to measure the progress of its employment diversity and inclusion practices, including measurement outcomes as appropriate, to indicate areas for improvement as part of their annual reports to Congress, all the federal financial agencies and Reserve Banks indicated that they plan to implement the recommendation:

- the OMWI Director of CFPB explained that its OMWI was the newest of such offices because the agency was created with the enactment of the Dodd-Frank Act and that it planned to include measurement information in future reports;
- the OMWI Director of the Federal Reserve Board stated that the recommendation was consistent with its ongoing practices and that it would look for additional ways to report on diversity practices;
- FDIC's OMWI Director agreed with the recommendation and stated that it will include efforts to measure the progress of its diversity practices in its annual reports to Congress;

- the Acting Associate Director of FHFA's OMWI stated that it would include measurement information in its 2013 OMWI report to Congress;
- the Executive Director of NCUA said the agency will work toward reporting on its efforts to measure the progress of workforce diversity and practices;
- the Comptroller of the Currency stated that OCC had a well-developed diversity and inclusion program through which the agency measures its progress and that OCC has included additional metrics in its 2013 OMWI report to Congress;
- SEC's OMWI Director noted that the agency plans to incorporate measurement information on its diversity and inclusion practices in its future OMWI reports to Congress;
- Treasury's OMWI Director agreed with our recommendation and stated that it was consistent with the agency's efforts to use more than demographic representation to measure the progress of diversity and inclusion efforts; and
- the Federal Reserve Banks' OMWI directors noted that the banks currently include some measurement information in annual reports and said that they will consider additional ways to measure and report on Reserve Banks' diversity practices.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution of this report until 30 days from the report date. At that time, we will send copies of this report to the appropriate congressional committees; the Chairman, Board of Governors of the Federal Reserve; Director, Bureau of Consumer Financial Protection, commonly known as the Consumer Financial Protection Bureau; Chair, Equal Employment Opportunity Commission; Chairman, Federal Deposit Insurance Corporation; Acting Director, Federal Housing Finance Agency; Chairman, National Credit Union Association; Comptroller, Office of the Comptroller of the Currency; Chairman, Securities and Exchange Commission; Secretary, Department of the Treasury; and to the Directors of the Offices of Minority and Women's Inclusion for the Federal Reserve Banks; and other interested parties. We will make copies available to others upon request. The report will also be available at no charge on our website at http://www.gao.gov.

If you or your staffs have any questions about this report, please contact me at (202) 512-8678 or garciadiazd@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs are listed on the last page of this report. GAO staff who made major contributions to this report are listed in appendix XIV.

Sincerely yours,

Daniel Garcia-Diaz
Director, Financial Markets and Community Investment

Appendix I: Objectives, Scope, and Methodology

The objectives for this report were to examine (1) what available data show about how the diversity of the financial services industry workforce and how diversity practices taken by the industry have changed from 2007 through 2011; (2) what available data show about how diversity in the workforces of the federal financial agencies and the Federal Reserve Banks (Reserve Banks) has changed from 2007 through 2011; (3) how these federal financial agencies and Reserve Banks are implementing workforce diversity practices under section 342 of the Dodd-Frank Act, including the extent to which their workforce diversity practices have changed since the financial crisis; and (4) the status of federal financial agencies' and Reserve Banks' implementation of the contracting provisions of the Dodd-Frank Act related to the inclusion of women and minorities.

To describe how diversity in the financial services industry has changed since the beginning of the 2007-2009 financial crisis, we analyzed 2007-2011 workforce data from the Equal Employment Opportunity Commission's (EEOC) Employer Information Report (EEO-1). EEO-1 is data annually submitted to EEOC generally by private-sector firms with more than 100 employees.[1] We obtained EEO-1 data on October 2012, from the finance and insurance industry categorized under the North American Industry Classification System (NAICS) code 52 for these industries from 2007 through 2011. EEO-1 data were specifically obtained from the EEOC's "officials and managers" category by gender, race/ethnicity, firm size, and industry sectors.[2] The EEO-1 "officials and managers" category was further divided into two management-level categories of first- and mid-level managers and senior-level managers

[1]Federal contractors with 50 or more employees are also required to submit to EEOC annual reports showing the composition of their workforce; however, we did not include these firms in our analysis. Accordingly, our EEO-1 analysis presented in this report may not match the EEO-1 data presented on EEOC's website. As required under the Civil Rights Act of 1964, EEOC collects periodic reports from public and private employers and unions and labor organizations that indicate the composition of their work forces by sex and by racial/ethnic category. Key among these reports is the EEO-1.

[2]EEOC defines the job category of "officials and managers" as occupations requiring administrative and managerial personnel, who set broad policies, exercise overall responsibility for execution of these policies, and direct individual departments or special phases of a firm's operation.

and then analyzed by gender, race/ethnicity, and firm size.[3] To understand the potential internal candidate pools available for management positions in the financial industry, we obtained EEO-1 data under NAICS code 52 for all positions, including nonmanagement positions, by gender and race/ethnicity. To determine the reliability of the EEO-1 data that we received from EEOC, we interviewed knowledgeable EEOC officials and reviewed relevant documents provided by agency officials and obtained on its website. We also conducted electronic testing of the data. We determined that the EEO-1 data were sufficiently reliable for our purposes.

To corroborate the results of the EEO-1 data, we used an additional source of workforce diversity data from the Current Population Survey (CPS), a monthly survey of households the Bureau of the Census administers on behalf of the Bureau of Labor Statistics. CPS data provide information on labor force characteristics and demographic data, among other topics. Similar to the EEO-1 "officials and managers" job category, we used the CPS "management occupations" category—unlike EEO-1, CPS does not split its management into two levels—for our discussion of management-level diversity within the financial services industry. However, the statistics from these two sources are not exactly comparable. We determined the CPS-estimated percentages of minorities in management positions within the financial services industry could not be precisely measured.[4] See table 6 for the estimated percentages and standard errors. The standard errors for the minority percentages were greater than the standard errors for the white percentages, and they were relatively large compared to the estimated percentage for minorities. However, CPS minority percentages were included in this report for additional context. To determine the reliability of CPS data, which we

[3]In 2007, EEOC subdivided the "officials and managers' category into two subcategories. The first one, "Executive/Senior Level Officials and Managers," includes individuals who reside in the highest levels of organizations and plan, direct, and formulate policies, set strategy, and provide the overall direction of enterprises/organizations for the development and delivery of products or services, within the parameters approved by boards of directors or other governing bodies. The second category, "First/Mid-Level Officials and Managers," includes individuals who receive directions from Executive/Senior Level management and oversee and direct the delivery of products, services, or functions at group, regional, or divisional levels of organizations.

[4]We used monthly averages over 3 months—July, August, and September—from the Basic Monthly CPS for each year and then calculated the estimated percentages, as EEOC's EEO-1 reports are collected over this period of time every year.

obtained from a publicly accessible federal statistical database, we gathered and reviewed relevant documentation from the Bureau of the Census website, conducted electronic testing, and determined the standard errors of the CPS estimates. We determined that the CPS data were sufficiently reliable for our purposes.

Table 6: Estimated Percentages and Standard Errors for Race/Ethnicity in Management Positions in the Financial Services Industry Using the Current Population Survey (CPS), 2007-2011

Year	Race/ethnicity	Percentage	Standard errors
2007	White	85.9%	1.7%
2007	Minority	14.1	4.5
2008	White	85.9	1.7
2008	Minority	14.1	4.5
2009	White	83.1	1.9
2009	Minority	16.9	4.5
2010	White	86.0	1.8
2010	Minority	14.0	4.7
2011	White	84.9	1.8
2011	Minority	15.1	4.6

Source: GAO analysis of CPS data.

To gather information on a potential external pipeline of diverse candidates for management positions in the financial industry, we obtained demographic data on minority and female students enrolled in undergraduate, Master of Business Administration (MBA), and doctoral degree programs from 2007 through 2011 from the Association to Advance Collegiate Schools of Business (AACSB). We focused on MBA programs as a source of potential future managers and senior executives. Financial services firms compete for minorities in this pool with one another and with firms from other industries. We combined this information with undergraduate and doctoral degree programs to provide information on the overall diversity of the university system. AACSB conducts an annual voluntary survey called “Business School Questionnaire” of all its member schools. In 2011, AACSB updated its survey to include two additional race/ethnicity categories to include “two or more races” and “Native Hawaiian or Other Pacific Islander.” For consistency purposes, we combined these two additional categories along with the representation of Native Americans into an “other” category. To determine the reliability of the AACSB data, we interviewed a knowledgeable AACSB official and reviewed relevant documents

provided by the official and obtained on its website. We determined that the data from AACSB were sufficiently reliable for our purposes.

To determine how diversity practices in the financial services industry have changed since the beginning of the financial crisis, we conducted a literature review of relevant studies that discussed diversity best practices within the financial services industry from 2007 through 2011. In addition, we interviewed 10 selected industry representatives to determine whether the nine leading diversity practices we previously identified are relevant today and how diversity practices changed since 2007. We also reviewed documents produced by these industry representatives. These representatives were selected based on their participation in our previous work, suggestions from federal agencies we interviewed for this report, as well as the type of industry representative—such as an industry association or private firm.[5]

To describe diversity in the workforces of the federal financial agencies and Reserve Banks, we analyzed data we received from agencies and banks. To review changes in the representation of minorities and women in the workforces of federal financial agencies, we obtained from the agencies annual Equal Employment Opportunity Program Status Reports from 2007 through 2011, required under U.S. EEOC Management Directive 715 and known as MD-715 reports.[6] We obtained data from seven of the eight federal agencies required to meet the workforce diversity provisions in section 342 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act). These included the Departmental Offices of the Department of the Treasury, the Federal Deposit Insurance Corporation, the Federal Housing Finance Agency (FHFA), the Board of Governors of the Federal Reserve System, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission. The Bureau of

[5]In our 2006 report we selected industry representatives based on a variety of criteria including whether they had received public recognition of their diversity programs or on the type of sector (such as securities or commercial banking) they were involved in. GAO-06-617.

[6]EEOC collects a variety of data on workforce diversity from federal agencies, including information pursuant to a management directive it issued in 2003 that included policy guidelines and standards for establishing and maintaining affirmative employment programs. This directive does not apply to the Federal Reserve Banks, as they are not federal agencies. EEOC MD-715 (2003).

Consumer Financial Protection, commonly known as the Consumer Financial Protection Bureau (CFPB), was created in July 2010 and assumed responsibility for certain consumer financial protection functions in 2011; workforce diversity data for the agency to show trends from 2007 through 2011 were unavailable.[7] Additionally, our trend analysis excluded FHFA, as the agency was created in 2008 and did not report on diversity employment statistics for 2007, 2008, or 2009. Further, our senior management-level trend analysis excluded SEC, as the agency revised how it reported officials and managers during the 5-year period. To review changes in the representation of minorities and women in the workforces of Reserve Banks, we obtained from banks their annual EEO-1 reports from 2007 through 2011.[8] For agencies and Reserve Banks, we reviewed workplace employment data by occupational categories, distributed by race/ethnicity and gender.[9] In our analyses, we considered all categories other than white as race/ethnic minorities and analyzed trends in diversity

[7]On July 21, 2010, the Consumer Financial Protection Act established CFPB as an independent bureau within the Federal Reserve System to be headed by a director. Effective July 21, 2011, CFPB assumed responsibility for certain consumer financial protection functions formerly the responsibilities of the Board of Governors of the Federal Reserve System, the Comptroller of the Currency, the Director of the Office of Thrift Supervision, FDIC, the Federal Trade Commission, NCUA, and the Secretary of the Department of Housing and Urban Development.

[8]We obtained annual EEO-1 reports from all 12 Reserve Banks, which are located in Atlanta, Boston, Chicago, Cleveland, Dallas, Kansas City, Minneapolis, New York, Philadelphia, Richmond, San Francisco, and St. Louis.

[9]These data are organized in table A3 of each MD-715 report and as part of the consolidated employer information reports for Reserve Bank EEO-1 data. For both data sets, race and ethnicity categories included Hispanic or Latino, White, Black or African American, Asian American, Native Hawaiian or Other Pacific Islander, American Indian or Alaskan Native, and Two or More Races. Our analysis included as an Other category: Native Hawaiian or Other Pacific Islander, American Indian or Alaskan Native, and Two or More Races.

at both the senior management-level and agency- and bankwide.[10] We analyzed senior management-level and overall diversity trends across all agencies and all Reserve Banks, as well as diversity trends for each agency when trend information was available.

To assess the reliability of MD-715 and EEO-1 data we received from agencies and Reserve Banks, we interviewed EEOC officials on both types of data as well as agency officials on MD-715 data and Reserve Bank officials on EEO-1 data about how the data are collected and verified as well as to identify potential data limitations. We found that while agencies and banks rely on employees to provide their race and ethnicity information, agencies and banks had measures in place to verify and correct missing or erroneous data prior to reporting them and officials with whom we spoke generally agreed these data were generally accurate. Based on our analysis, we concluded that the MD-715 and EEO-1 data were sufficiently reliable for our purposes.

To assess how federal financial agencies and Reserve Banks are implementing workforce diversity practices under section 342 of the Dodd-Frank Act, we reviewed agency and bank documentation of efforts to respond to the act's requirements. Sources included annual Office of Minority and Women Inclusion (OMWI) reports to Congress by agencies and banks, annual agency MD-715 reports, and other documentation provided to us by agency and bank OMWI officials. Additionally, we gathered testimonial information from agency and Reserve Bank OMWI officials on changes in the inclusion of women and minorities in their workforces and any changes in the practices used to further workforce diversity goals. Through our review of agency and Reserve Bank documentation and interviews with OMWI officials, we assessed agency

[10]We defined senior management-level as employees reported in the most senior job category by federal financial agencies and Reserve Banks. For agency MD-715 data, we considered senior management-level as officials and managers reported as "Executive/Senior Level," in each agency's A3 data tables. For Reserve Bank EEO-1 data, we considered senior management-level as "Executive/Senior Officials and Managers," reported by each Reserve Bank. Our analysis of agencywide data included all job categories reported by each agency: Executive/Senior Level, Mid-level, First-level, and Other Officials and Managers, Professionals, Technicians, Sales Workers, Administrative Support Workers, Craft Workers, Operatives, Laborers and Helpers, and Service Workers. Our analysis of bankwide data included all job categories reported by each Reserve Bank: Executive/Senior Officials and Managers, First/Mid Officials and Managers, Professionals, Technicians, Sales Workers, Administrative Support Workers, Craft Workers, Operatives, Laborers and Helpers, and Service Workers.

and Reserve Bank efforts to measure and report on the progress of their diversity practices, as measurement was one of the nine leading diversity practices we previously identified.

To determine the extent to which agencies and Reserve Banks are implementing the requirements of the Dodd-Frank Act regarding the inclusion of women and minorities in contracting, we reviewed 2011 OMWI reports submitted to Congress and interviewed officials on their efforts in this area. We also reviewed OMWI reports to determine the dollar amount and percentage of total contracts federal financial agencies reported awarding to minority- and women-owned businesses (MWOB), and the dollar amount and percentage of total contracts Reserve Banks reporting paying MWOBs in 2011. We verified these figures and our presentation of the information with each agency and Reserve Bank, and we determined that these data were sufficiently reliable for our purposes. We interviewed agency officials on their efforts to coordinate with the Small Business Administration and other federal agencies to provide technical assistance to minority- and women-owned businesses. We collected and reviewed agency documentation of procedures developed to address the act's requirements, such as policy manuals, process workflows, and technical assistance materials. We also collected and reviewed examples of fair inclusion provisions used in agency and Reserve Bank contracts as required in section 342 of the Dodd-Frank Act.

We conducted this performance audit from January 2012 to March 2013 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

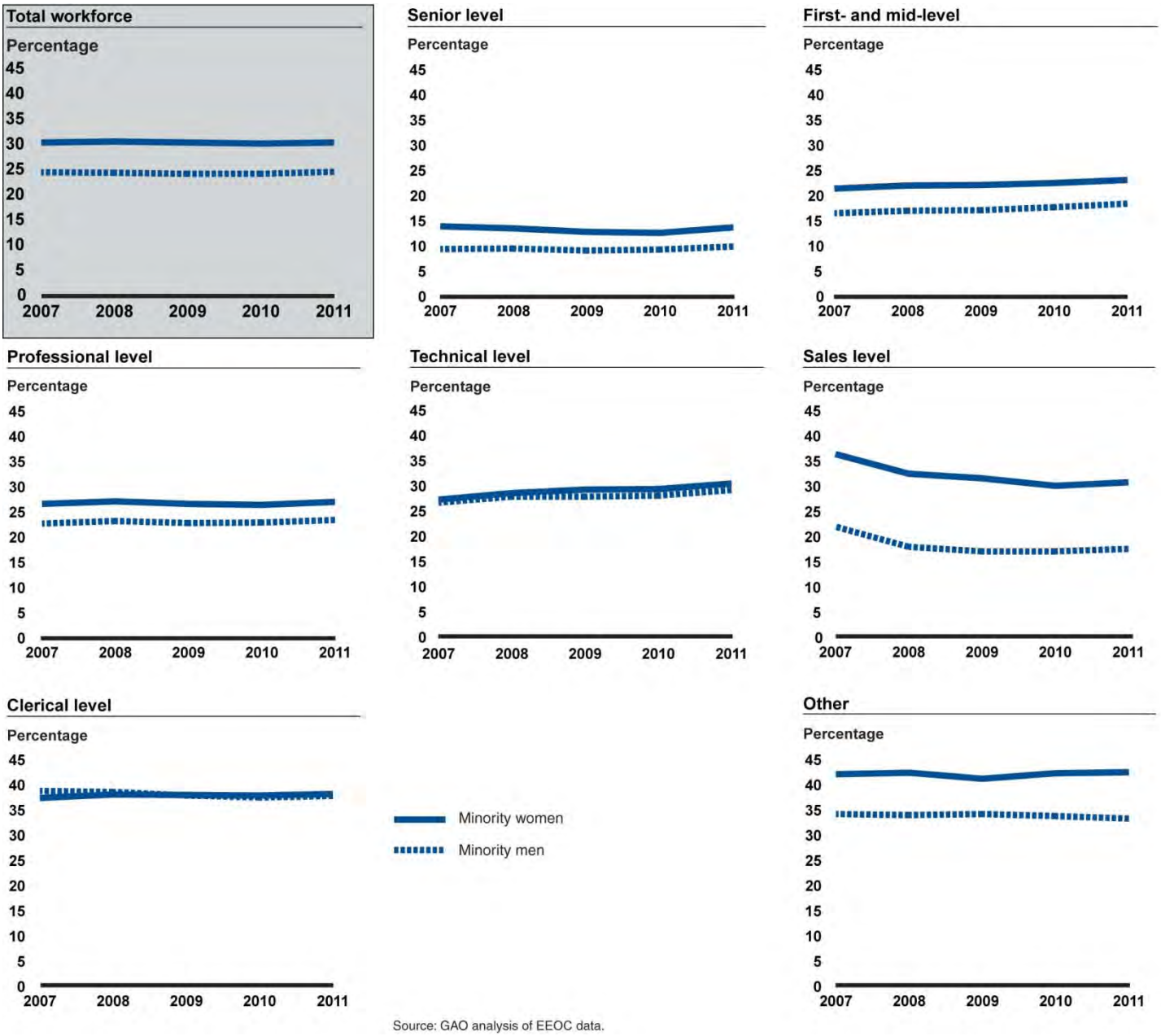
Appendix II: Additional Analysis of the Financial Services Industry

This appendix provides additional detailed analysis of EEOC data on the financial services industry by workforce position and industry sector from 2007 through 2011.

Analysis by Workforce Positions

The representation of minorities by gender was below 45 percent across all the positions throughout the same 5-year period (see fig. 16). For example, in sales positions, the representation of minorities was higher among women (about 31 percent) than among men (about 17 percent). Similarly, at the professional level, the representation of minority women was about 27 percent, compared to about 23 percent for minority men.

Figure 16: Percentage of Minority Women and Minority Men in Various Industry Workforce Positions in the Financial Services Industry, 2007-2011



Source: GAO analysis of EEOC data.

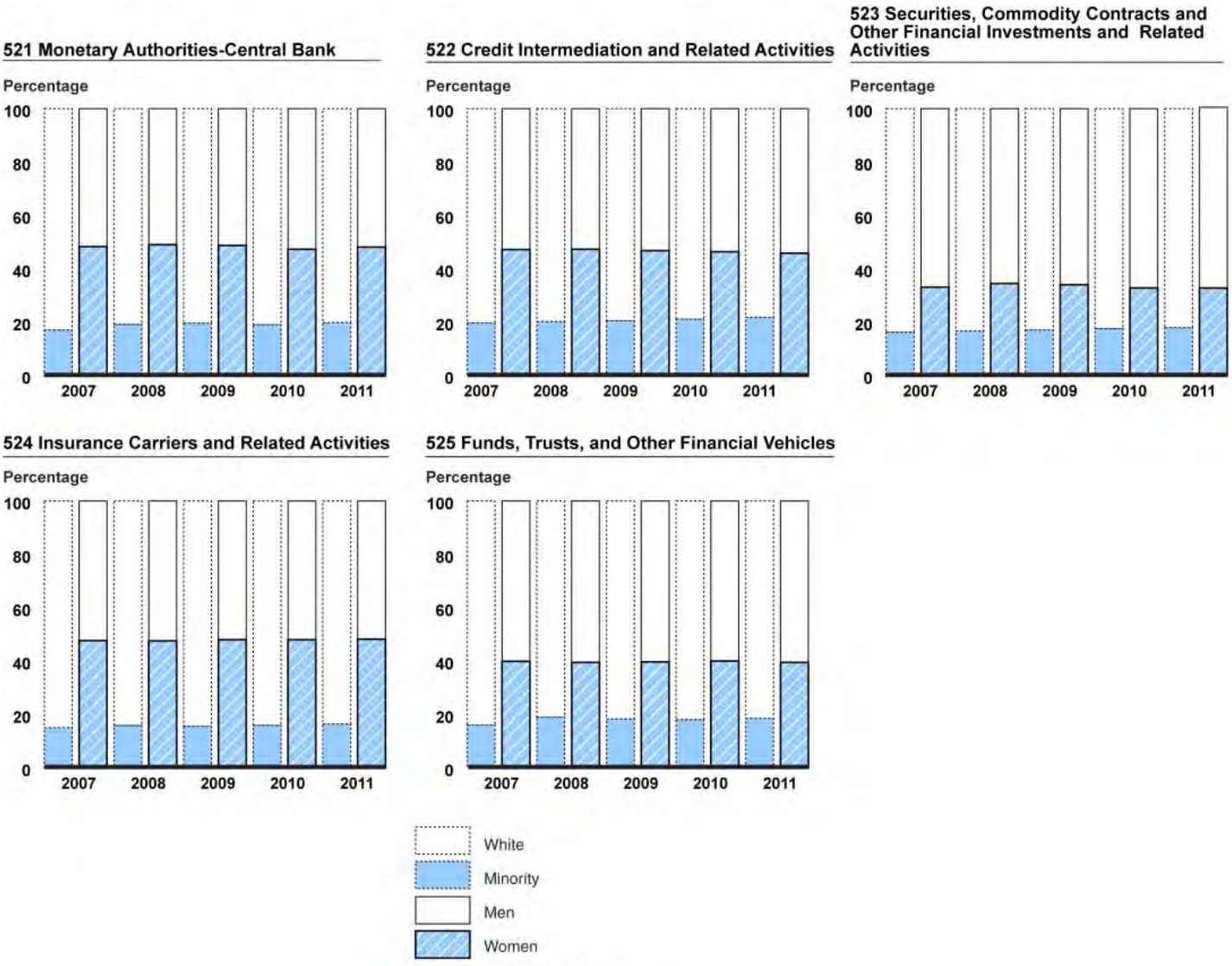
Note: The category "other" includes craft workers, operatives, laborers, and service workers.

Analysis by Industry Sectors

Diversity remained about the same across all industry sectors in terms of both the representation of women and minorities.[1] From 2007 through 2011, the representation of women decreased slightly in most industry sectors and remained below 50 percent in all sectors (see fig. 17). The "insurance carriers and related activities" sector was the only sector that showed an increase in the representation of women, from 47.7 percent to 48.2 percent. In contrast, the representation of minorities increased across all sectors. Specifically, from 2007 through 2011 the representation of minorities in the "monetary authorities-central bank" sector increased from 17 percent to 19.8 percent, and the "funds, trusts, and other financial vehicle" sector increased from 16 percent to 18.5 percent.

[1]These industry sectors under the financial services industry are split according to the NAICS.

Figure 17: Percentage of Whites/Minorities and Men/Women in Various Sectors of the Financial Services Industry, 2007-2011



Source: GAO analysis of EEOC data.

Note: Industry sector numbers are defined as follows: Sector 521, Monetary Authorities-Central Bank; Sector 522, Credit Intermediation and Related Activities; Sector 523, Securities, Commodity Contracts, and Other Financial Investments and Related Activities; Sector 524, Insurance Carriers and Related Activities; Sector 525, Funds, Trusts, and Other Financial Vehicles.

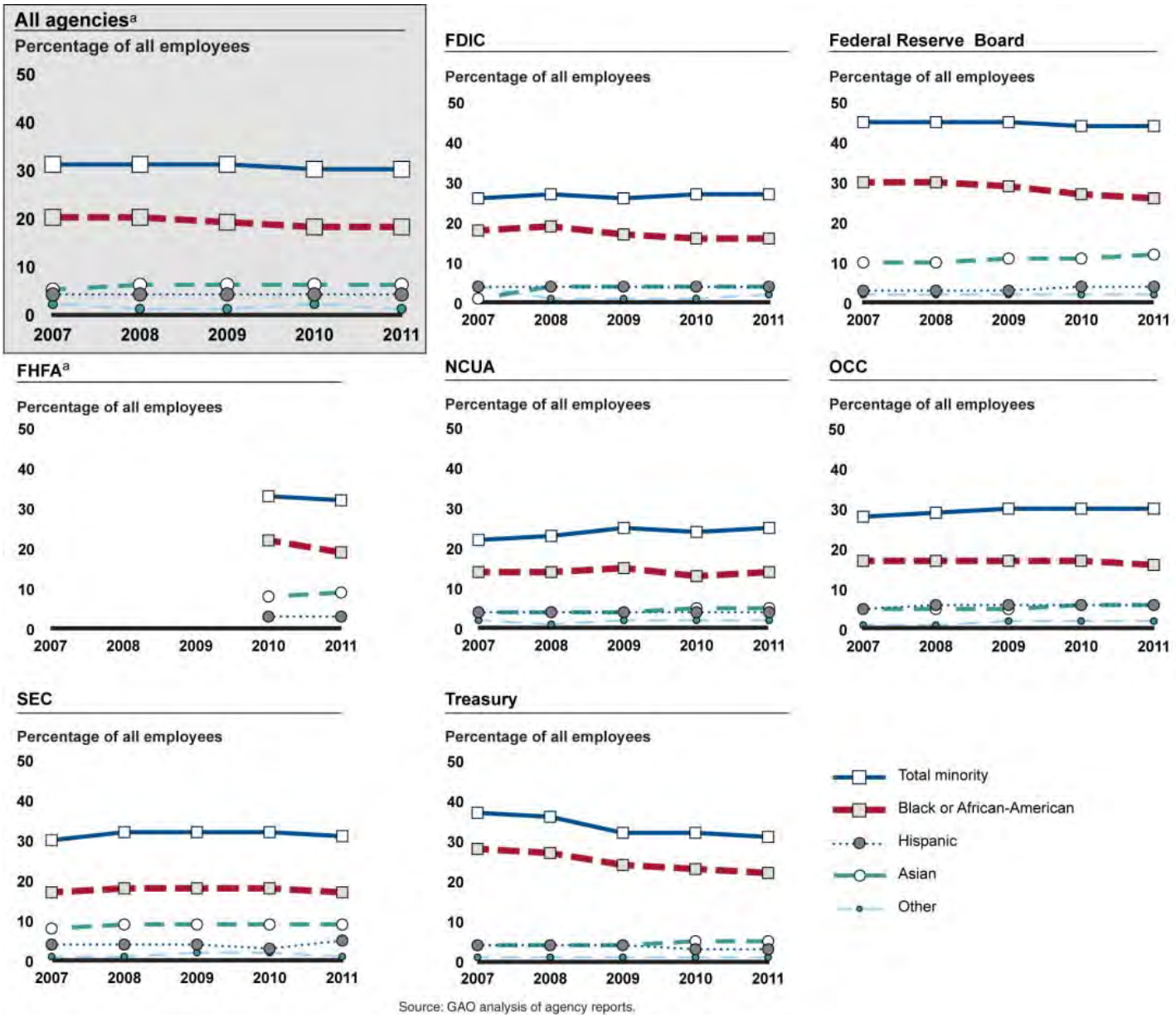
Appendix III: Additional Analysis of Overall Workforce Diversity at Agencies and Reserve Banks

This appendix provides information accompanying our review of changes in overall workforce diversity at federal financial agencies and the 12 Reserve Banks from 2007 through 2011.[1] Tables 11 through 14 in appendix IV provide data supporting the figures in this appendix.

According to MD-715 data, the representation of minorities in the overall workforce of the agencies, in aggregate, changed little from 2007 through 2011. Percentage point changes in the representation of minorities at FDIC, the Federal Reserve Board, NCUA, OCC, SEC, and Treasury varied from a 5 percentage point decrease at Treasury to a 3 percentage point increase at NCUA. In 2011, the representation of minorities in the overall workforce of the agencies and FHFA ranged from 25 percent at NCUA to 44 percent at the Federal Reserve Board.

[1]The agencies included FDIC, the Federal Reserve Board, NCUA, OCC, SEC, and Treasury. FHFA was established in 2008 and started reporting workforce data for 2010, and is excluded from our trend analysis. Additionally, CFPB was established in July 2011 and trend data were not available.

Figure 18: Percentage of Minorities among All Employees at Seven Federal Financial Agencies, 2007-2011



Source: GAO analysis of agency reports.

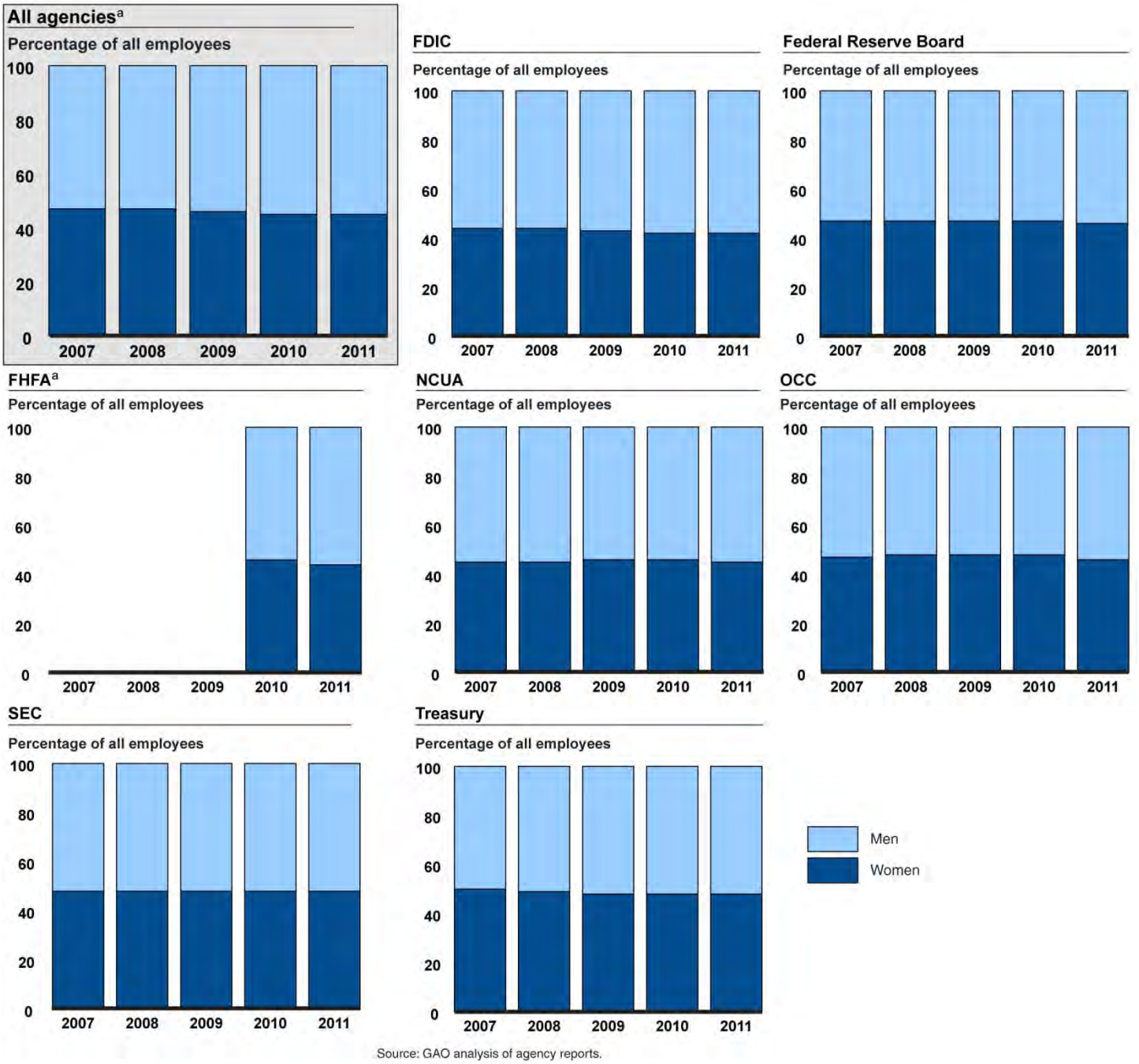
Note: Figures are rounded to the nearest percent.

For our analysis, we reviewed the numbers of employees the agencies reported according to race/ethnicity and gender in table A3 of their MD-715 reports from 2007 through 2011. These data are based on information self-reported by employees to each agency and there were some differences in reporting across the agencies. In some years, some agencies reported all employees—permanent and temporary—in their A3 tables while others reported permanent employees only.

[a]Our trend analysis for "all agencies" excludes CFPB and FHFA. CFPB assumed responsibility for certain consumer financial protection functions in July 2011 and has not yet reported workforce information to EEOC. FHFA was established in 2008 and started reporting workforce data for 2010.

Similarly, we found that the representation of women in the overall workforce of the agencies did not change significantly from 2007 through 2011. Percentage point changes in the representation of women at the agencies from 2007 through 2011 varied from a 2 percentage point decrease at FDIC, the Federal Reserve Board, and Treasury to no percentage point change at NCUA and SEC. In 2011, the representation of minorities in the overall workforce of the agencies and FHFA ranged from 42 percent at FDIC to 48 percent at SEC and Treasury.

Figure 19: Percentage of Women among All Employees at Seven Federal Financial Agencies, 2007-2011



Source: GAO analysis of agency reports.

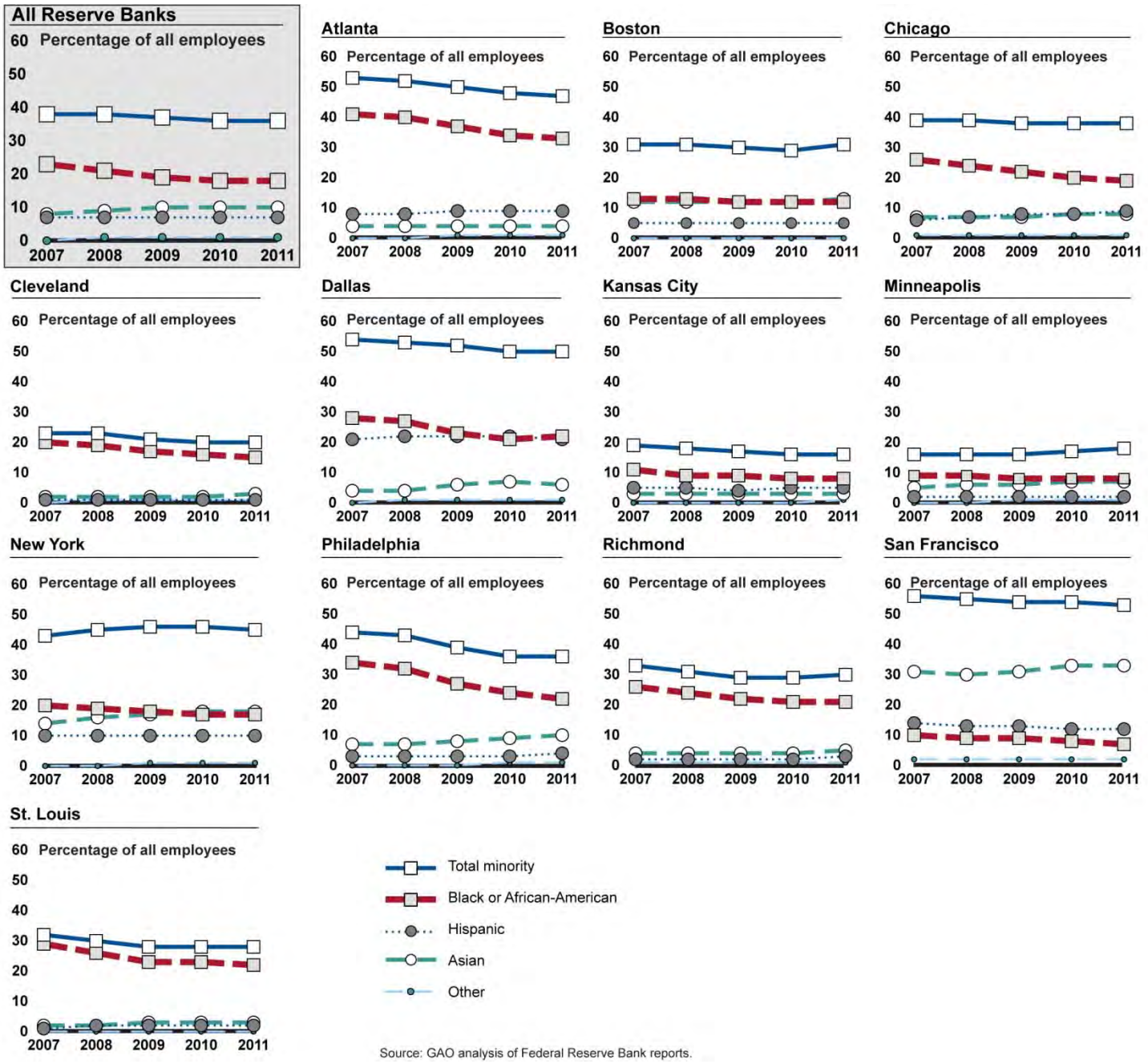
Note: Figures are rounded to the nearest percent.

For our analysis, we reviewed the numbers of employees the agencies reported according to race/ethnicity and gender in table A3 of their MD-715 reports from 2007 through 2011. These data are based on information self-reported by employees to each agency and there were some differences in reporting across the agencies. In some years, some agencies reported all employees—permanent and temporary—in their A3 tables while others reported permanent employees only.

[a]Our trend analysis for "all agencies" excludes CFPB and FHFA. CFPB assumed responsibility for certain consumer financial protection functions in July 2011 and has not yet reported workforce information to EEOC. FHFA was established in 2008 and started reporting workforce data for 2010.

According to EEO-1 data provided by the Reserve Banks, the representation of minorities in the overall workforce of the Reserve Banks decreased somewhat from 2007 through 2011. The banks showed changes in the representation of minorities from 2007 through 2011, from an 8 percentage point decrease at the Reserve Bank of Philadelphia, to a 2 percentage point increase at the Reserve Banks of Minneapolis and New York. The Reserve Bank of Boston showed no percentage point change from 2007 through 2011. In 2011, the representation of minorities in the overall workforce of the Reserve Banks ranged from 16 percent at the Reserve Bank of Kansas City to 53 percent at the Reserve Bank of San Francisco.

Figure 20: Percentage of Minorities among All Employees at the 12 Reserve Banks, 2007-2011

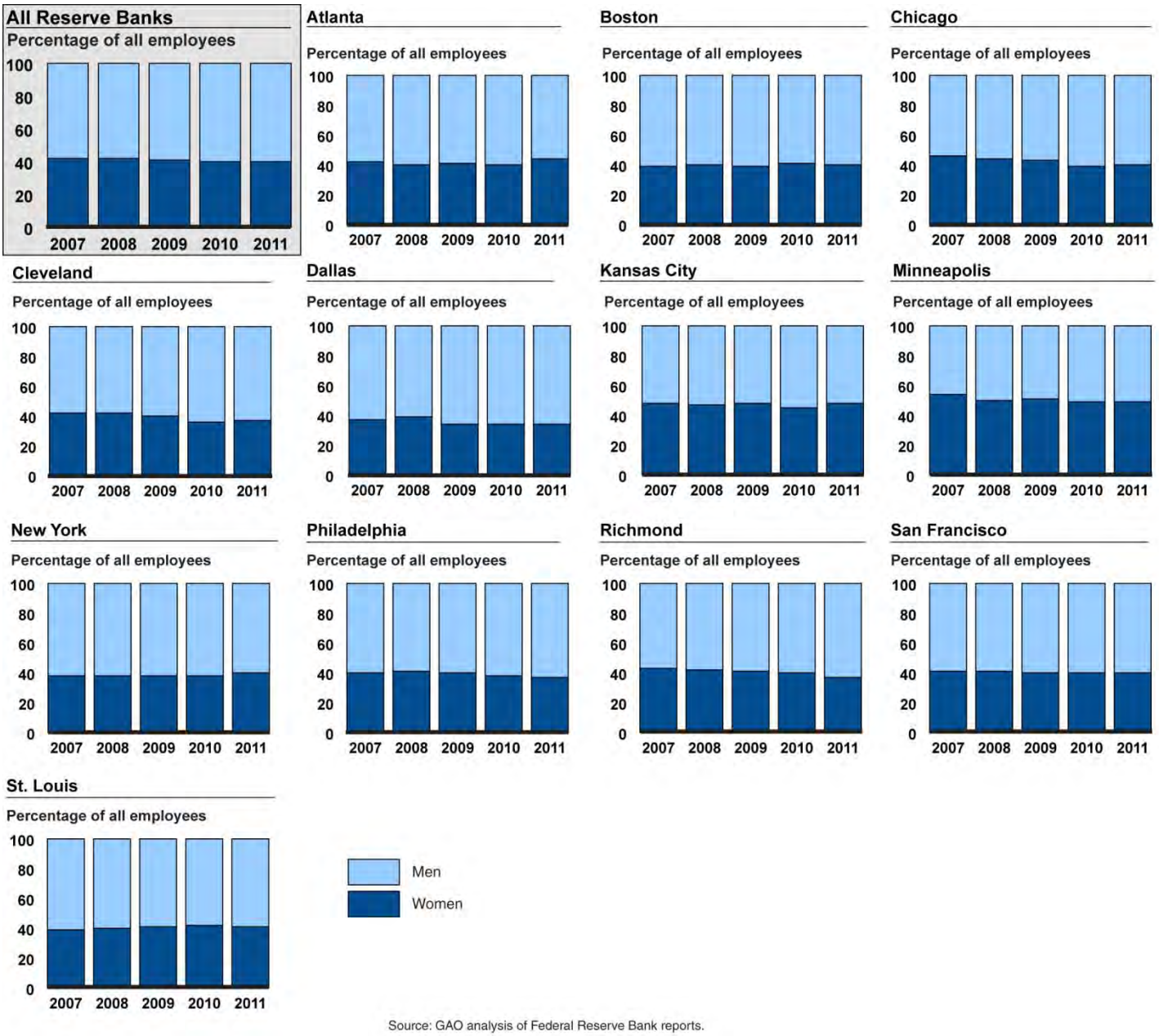


Source: GAO analysis of Federal Reserve Bank reports.

Note: Figures are rounded to the nearest percent.

In addition, we found that from 2007 through 2011, the representation of women in the overall workforce of the Reserve Banks also declined slightly according to EEO-1 data provided by the Reserve Banks. The Reserve Banks showed decreases in the representation of women in the overall workforce from 1 percentage point at the Reserve Bank of New York to 7 percentage points at the Reserve Bank of Cleveland. The representation of women in the overall workforce in 2011 ranged from 40 percent at the Reserve Banks of Philadelphia and Richmond to 53 percent at the Reserve Bank of Minneapolis.

Figure 21: Percentage of Women among All Employees at the 12 Reserve Banks, 2007-2011



Source: GAO analysis of Federal Reserve Bank reports.

Note: Figures are rounded to the nearest percent.

Appendix IV: Representation of Minorities and Women at Federal Financial Agencies and Reserve Banks

We reviewed agency and Reserve Bank reports and found that since the financial crisis, senior management-level minority and gender diversity at the agencies and Reserve Banks has varied across individual entities. We also found the representation of minorities and women in the overall workforce of the agencies changed little from 2007 through 2011, while the representation of minorities and women in the overall workforce of the Reserve Banks declined slightly. The following tables provide data supporting the senior management-level and total workforce figures in this report.

Table 7: Percentage of Minorities among Senior Management-Level Employees at Seven Federal Financial Agencies, 2007-2011

		Senior management-level federal financial agency employees (number and percent)													
Race/ethnicity	**Year**	**FDIC**		**Federal Reserve**		**FHFA[a]**		**NCUA**		**OCC**		**SEC[b]**		**Treasury**	
All	2011	301	100%	343	100%	51	100%	134	100%	251	100%	125	100%	312	100%
	2010	284	100	307	100	29	100	109	100	204	100	-	-	279	100
	2009	258	100	301	100	-	-	101	100	201	100	-	-	276	100
	2008	234	100	289	100	-	-	123	100	252	100	-	-	219	100
	2007	203	100	253	100	-	-	118	100	229	100	-	-	175	100
White	2011	250	83	277	81	39	76	118	88	207	82	111	89	259	83
	2010	237	83	246	80	21	72	95	87	164	80	-	-	238	85
	2009	218	84	247	82	-	-	90	89	164	82	-	-	236	86
	2008	199	85	237	82	-	-	108	88	207	82	-	-	188	86
	2007	171	84	207	82	-	-	104	88	190	83	-	-	150	86
Total minority	2011	51	17	66	19	12	24	16	12	44	18	14	11	53	17
	2010	47	17	61	20	8	28	14	13	40	20	-	-	41	15
	2009	40	16	54	18	-	-	11	11	37	18	-	-	40	14
	2008	35	15	52	18	-	-	15	12	45	18	-	-	31	14
	2007	32	16	46	18	-	-	14	12	39	17	-	-	25	14
Black or African American	2011	31	10	35	10	8	16	5	4	23	9	3	2	29	9
	2010	27	10	33	11	7	24	5	5	23	11	-	-	21	8
	2009	24	9	31	10	-	-	4	4	23	11	-	-	22	8
	2008	24	10	29	10	-	-	7	6	29	12	-	-	19	9
	2007	23	11	27	11	-	-	7	6	29	13	-	-	17	10
Hispanic	2011	9	3	7	2	4	8	6	4	12	5	6	5	12	4
	2010	9	3	7	2	1	3	5	5	10	5	-	-	11	4

		Senior management-level federal financial agency employees (number and percent)													
Race/ethnicity	Year	FDIC		Federal Reserve		FHFA[a]		NCUA		OCC		SEC[b]		Treasury	
	2009	7	3	5	2	-	-	5	5	6	3	-	-	12	4
	2008	5	2	4	1	-	-	5	4	9	4	-	-	8	4
	2007	4	2	3	1	-	-	4	3	6	3	-	-	5	3
Asian	2011	9	3	20	6	0	0	3	2	9	4	3	2	10	3
	2010	9	3	17	6	0	0	2	2	6	3	-	-	8	3
	2009	7	3	13	4	-	-	1	1	7	3	-	-	6	2
	2008	5	2	14	5	-	-	2	2	5	2	-	-	4	2
	2007	1	0	11	4	-	-	2	2	2	1	-	-	3	2
Other	2011	2	1	4	1	0	0	2	1	0	0	2	2	2	1
	2010	2	1	4	1	0	0	2	2	1	0	-	-	1	0
	2009	2	1	5	2	-	-	1	1	1	0	-	-	0	0
	2008	1	0	5	2	-	-	1	1	2	1	-	-	0	0
	2007	4	2	5	2	-	-	1	1	2	1	-	-	0	0

Source: GAO analysis of agency reports.

Notes: Percentages are rounded to the nearest percent.

For our analysis, we reviewed the numbers of employees the agencies reported according to race/ethnicity and gender in table A3 of their MD-715 reports from 2007 through 2011. These data are based on information self-reported by employees to each agency and there were some differences in reporting across the agencies. In some years, some agencies reported all employees—permanent and temporary—in their A3 tables while others reported permanent employees only. We considered employees reported by agencies in the category "Executive/Senior Level" as senior management-level employees. Though the MD-715 report guidelines instruct agencies to identify employees Grades 15 and above who have supervisory responsibility in this category, agencies have discretion to include employees who have significant policymaking responsibilities but do not supervise employees. As a result, the composition of the "Executive/Senior Level" category may vary among the different agencies and does not necessarily involve the same set of managers at each agency.

[a]FHFA was established in 2008 and started reporting workforce data for 2010.

[b]SEC revised how it reported officials and managers between 2007 and 2011. While our analysis includes 2011 management-level data for SEC, we excluded previous years from our trend analysis.

Table 8: Percentage of Minorities among Senior Management-Level Employees at the 12 Reserve Banks, 2007-2011

		Senior management-level Reserve Bank employees (number and percent)																							
Race/ ethnicity	Year	Atlanta		Boston		Chicago		Cleveland		Dallas		Kansas City		Minneapolis		New York		Philadelphia		Richmond		San Francisco		St. Louis	
All	2011	13	100%	13	100%	9	100%	13	100%	9	100%	12	100%	9	100%	59	100%	11	100%	22	100%	13	100%	11	100%
	2010	86	100	11	100	9	100	12	100	10	100	14	100	8	100	74	100	10	100	23	100	23	100	9	100
	2009	82	100	12	100	11	100	12	100	10	100	12	100	8	100	71	100	13	100	20	100	26	100	37	100
	2008	80	100	12	100	11	100	13	100	10	100	11	100	9	100	65	100	12	100	19	100	26	100	34	100
	2007	75	100	12	100	11	100	12	100	10	100	12	100	7	100	55	100	11	100	19	100	26	100	30	100
White	2011	10	77	11	85	8	89	13	100	8	89	11	92	5	56	52	88	10	91	19	86	10	77	10	91
	2010	72	84	11	100	8	89	12	100	9	90	13	93	5	63	66	89	9	90	20	87	20	87	9	100
	2009	68	83	12	100	10	91	12	100	9	90	12	100	7	88	62	87	11	85	19	95	23	88	33	89
	2008	66	83	12	100	10	91	13	100	9	90	11	100	8	89	55	85	10	83	17	89	23	88	31	91
	2007	62	83	12	100	10	91	12	100	9	90	12	100	6	86	46	84	10	91	18	95	24	92	29	97
Total minority	2011	3	23	2	15	1	11	0	0	1	11	1	8	4	44	7	12	1	9	3	14	3	23	1	9
	2010	14	16	0	0	1	11	0	0	1	10	1	7	3	38	8	11	1	10	3	13	3	13	0	0
	2009	14	17	0	0	1	9	0	0	1	10	0	0	1	13	9	13	2	15	1	5	3	12	4	11
	2008	14	18	0	0	1	9	0	0	1	10	0	0	1	11	10	15	2	17	2	11	3	12	3	9
	2007	13	17	0	0	1	9	0	0	1	10	0	0	1	14	9	16	1	9	1	5	2	8	1	3
Black or African American	2011	2	15	2	15	1	11	0	0	1	11	0	0	2	22	4	7	0	0	1	5	1	8	1	9
	2010	11	13	0	0	1	11	0	0	1	10	0	0	1	13	3	4	1	10	1	4	2	9	0	0
	2009	11	13	0	0	1	9	0	0	1	10	0	0	1	13	4	6	1	8	0	0	2	8	2	5
	2008	10	13	0	0	1	9	0	0	1	10	0	0	1	11	4	6	1	8	1	5	2	8	2	6
	2007	9	12	0	0	1	9	0	0	1	10	0	0	1	14	4	7	1	9	1	5	2	8	1	3
Hispanic	2011	0	0	0	0	0	0	0	0	0	0	1	8	0	0	1	2	0	0	2	9	1	8	0	0

		Senior management-level Reserve Bank employees (number and percent)																							
Race/ ethnicity	Year	Atlanta		Boston		Chicago		Cleveland		Dallas		Kansas City		Minneapolis		New York		Philadelphia		Richmond		San Francisco		St. Louis	
	2010	3	3	0	0	0	0	0	0	0	0	1	7	0	0	2	3	0	0	2	9	0	0	0	0
	2009	3	4	0	0	0	0	0	0	0	0	0	0	0	0	2	3	0	0	1	5	0	0	1	3
	2008	4	5	0	0	0	0	0	0	0	0	0	0	0	0	3	5	0	0	1	5	0	0	1	3
	2007	4	5	0	0	0	0	0	0	0	0	0	0	0	0	3	5	0	0	0	0	0	0	0	0
Asian	2011	0	0	0	0	0	0	0	0	0	0	0	0	1	11	2	3	1	9	0	0	1	8	0	0
	2010	0	0	0	0	0	0	0	0	0	0	0	0	1	13	3	4	0	0	0	0	1	4	0	0
	2009	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	4	1	8	0	0	1	4	1	3
	2008	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	5	1	8	0	0	1	4	0	0
	2007	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	4	0	0	0	0	0	0	0	0
Other	2011	1	8	0	0	0	0	0	0	0	0	0	0	1	11	0	0	0	0	0	0	0	0	0	0
	2010	0	0	0	0	0	0	0	0	0	0	0	0	1	13	0	0	0	0	0	0	0	0	0	0
	2009	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	2008	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	2007	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Source: GAO analysis of EEO-1 reports provided by Reserve Banks.

Notes: Percentages are rounded to the nearest percent.

For our analysis of the representation of minorities and women at the senior management level for Reserve Banks, we reviewed the numbers of employees the banks reported as “Executive/Senior Level Officials and Managers” from 2007 through 2011. While EEOC provides instructions on reporting job categories based on the skill levels, knowledge, and responsibilities involved in occupations identified within each job category, employers have discretion to decide which positions they report as Executive/Senior Level Officials and Managers versus those at lower levels of management. Therefore, comparisons of a given management level between the Reserve Banks do not necessarily involve the same set of managers at each bank. For example, the Reserve Bank of Atlanta revised how it reported officials and managers for 2011. From 2007 through 2010, the bank reported all officers as Executive/Senior Level Officials and Managers, and for 2011, the bank reported as Executive/Senior Level Officials and Managers those employees that have strategic roles and/or report to the Reserve Bank’s President. According to Reserve Bank officials, recent efforts have been made to align reporting of officials and managers across the Federal Reserve System.

Table 9: Percentage of Women among Senior Management-Level Employees at Seven Federal Financial Agencies, 2007-2011

		Senior management-level federal financial agency employees (number and percent)													
Gender	Year	FDIC		Federal Reserve		FHFA[a]		NCUA		OCC		SEC[b]		Treasury	
All	2011	301	100%	343	100%	51	100%	134	100%	251	100%	125	100%	312	100%
	2010	284	100	307	100	29	100	109	100	204	100	-	-	279	100
	2009	257	100	301	100	-	-	101	100	201	100	-	-	176	100
	2008	234	100	289	100	-	-	123	100	252	100	-	-	219	100
	2007	203	100	253	100	-	-	118	100	229	100	-	-	175	100
Men	2011	209	69	201	59	27	53	87	65	171	68	85	68	192	62
	2010	197	69	185	60	14	48	77	71	137	67	-	-	178	64
	2009	187	72	184	61	-	-	72	71	130	65	-	-	176	64
	2008	165	71	180	62	-	-	84	68	161	64	-	-	143	65
	2007	147	72	155	61	-	-	82	69	145	63	-	-	115	66
Women	2011	92	31	142	41	24	47	47	35	80	32	40	32	120	38
	2010	87	31	122	40	15	52	32	29	67	33	-	-	101	36
	2009	71	28	117	39	-	-	29	29	71	35	-	-	100	36
	2008	69	29	109	38	-	-	39	32	91	36	-	-	76	35
	2007	56	28	98	39	-	-	36	31	84	37	-	-	60	34

Source: GAO analysis of agency reports.

Notes: Percentages are rounded to the nearest percent.

For our analysis, we reviewed the numbers of employees the agencies reported according to race/ethnicity and gender in table A3 of their MD-715 reports from 2007 through 2011. These data are based on information self-reported by employees to each agency and there were some differences in reporting across the agencies. In some years, some agencies reported all employees—permanent and temporary—in their A3 tables while others reported permanent employees only. We considered employees reported by agencies in the category "Executive/Senior Level" as senior management-level employees. Though the MD-715 report guidelines instruct agencies to identify employees Grades 15 and above who have supervisory responsibility in this category, agencies have discretion to include employees who have significant policymaking responsibilities but do not supervise employees. As a result, the composition of the "Executive/Senior Level" category may vary among the different agencies and does not necessarily involve the same set of managers at each agency.

[a]FHFA was established in 2008 and started reporting workforce data for 2010.

[b]SEC revised how it reported officials and managers between 2007 and 2011. While our analysis includes 2011 management-level data for SEC, we excluded previous years from our trend analysis.

Table 10: Percentage of Women among Senior Management-Level Employees at the 12 Reserve Banks, 2007-2011

		Senior management-level federal financial agency employees (number and percent)																							
Race/ ethnicity	Year	Atlanta		Boston		Chicago		Cleveland		Dallas		Kansas City		Minneapolis		New York		Philadelphia		Richmond		San Francisco		St. Louis	
All	2011	13	100%	13	100%	9	100%	13	100%	9	100%	12	100%	9	100%	59	100%	11	100%	22	100%	13	100%	11	100%
	2010	86	100	11	100	9	100	12	100	10	100	14	100	8	100	74	100	10	100	23	100	23	100	9	100
	2009	82	100	12	100	11	100	12	100	10	100	12	100	8	100	71	100	13	100	20	100	26	100	37	100
	2008	80	100	12	100	11	100	13	100	10	100	11	100	9	100	65	100	12	100	19	100	26	100	34	100
	2007	75	100	12	100	11	100	12	100	10	100	12	100	7	100	55	100	11	100	19	100	26	100	30	100
Men	2011	7	54	11	85	5	56	9	69	6	67	5	42	6	67	34	58	6	55	15	68	9	69	7	64
	2010	53	62	9	82	5	56	9	75	7	70	9	64	6	75	48	65	5	50	16	70	16	70	6	67
	2009	49	60	9	75	6	55	8	67	7	70	8	67	6	75	46	65	9	69	13	65	17	65	26	70
	2008	49	61	9	75	6	55	9	69	7	70	8	73	7	78	43	66	8	67	14	74	17	65	22	65
	2007	48	64	9	75	6	55	8	67	7	70	8	67	6	86	39	71	7	64	15	79	17	65	20	67
Women	2011	6	46	2	15	4	44	4	31	3	33	7	58	3	33	25	42	5	45	7	32	4	31	4	36
	2010	33	38	2	18	4	44	3	25	3	30	5	36	2	25	26	35	5	50	7	30	7	30	3	33
	2009	33	40	3	25	5	45	4	33	3	30	4	33	2	25	25	35	4	31	7	35	9	35	11	30
	2008	31	39	3	25	5	45	4	31	3	30	3	27	2	22	22	34	4	33	5	26	9	35	12	35
	2007	27	36	3	25	5	45	4	33	3	30	4	33	1	14	16	29	4	36	4	21	9	35	10	33

Source: GAO analysis of EEO-1 reports provided by Reserve Banks.

Notes: Percentages are rounded to the nearest percent.

For our analysis of the representation of minorities and women at the senior management level for Reserve Banks, we reviewed the numbers of employees the banks reported as “Executive/Senior Level Officials and Managers” from 2007 through 2011. While EEOC provides instructions on reporting job categories based on the skill levels, knowledge, and responsibilities involved in occupations identified within each job category, employers have discretion to decide which positions they report as Executive/Senior Level Officials and Managers versus those at lower levels of management. Therefore, comparisons of a given management level between the Reserve Banks do not necessarily involve the same set of managers at each bank. For example, the Reserve Bank of Atlanta revised how it reported officials and managers for 2011. From 2007 through 2010, the bank reported all officers as Executive/Senior Level Officials and Managers, and for 2011,

the bank reported as Executive/Senior Level Officials and Managers those employees that have strategic roles and/or report to the Reserve Bank's President. According to Reserve Bank officials, recent efforts have been made to align reporting of officials and managers across the Federal Reserve System.

Table 11: Percentage of Minorities among All Employees at Seven Federal Financial Agencies, 2007-2011

		Federal financial agency employees (number and percent)													
Race/ethnicity	**Year**	**FDIC**		**Federal Reserve**		**FHFA[a]**		**NCUA**		**OCC**		**SEC**		**Treasury**	
All	2011	8,398	100%	2,274	100%	494	100%	1,159	100%	3,560	100%	3,812	100%	1,586	100%
	2010	8,316	100	2,137	100	406	100	1,095	100	3,054	100	3,897	100	1,599	100
	2009	6,530	100	2,143	100	-	-	1,024	100	3,117	100	3,720	100	1,529	100
	2008	5,028	100	2,028	100	-	-	934	100	3,039	100	3,653	100	1,295	100
	2007	4,428	100	1,945	100	-	-	929	100	3,000	100	3,154	100	1,223	100
White	2011	6,152	73	1,276	56	335	38	871	75	2,503	70	2,616	69	1,087	69
	2010	6,107	73	1,196	56	270	67	833	76	2,145	70	2,664	68	1,080	68
	2009	4,800	74	1,187	55	-	-	769	75	2,185	70	2,516	68	1,041	68
	2008	3,655	73	1,115	55	-	-	722	78	2,161	72	2,204	70	772	63
	2007	3,261	74	1,066	55	-	-	722	78	2,161	72	2,204	7	772	63
Total minority	2011	2,246	27	998	44	159	32	288	25	1,057	30	1,196	31	499	31
	2010	2,209	27	941	44	136	33	262	24	909	30	1,233	32	519	32
	2009	1,730	26	956	45	-	-	255	25	932	30	1,204	32	488	32
	2008	1,373	27	913	45	-	-	216	23	887	29	1,168	32	464	36
	2007	1,167	26	879	45	-	-	207	22	839	28	950	30	451	37
Black or African American	2011	1,385	16	591	26	95	19	157	14	577	16	632	17	356	22
	2010	1,353	16	582	27	90	22	141	13	508	17	682	18	372	23
	2009	1,109	17	612	29	-	-	153	15	534	17	679	18	362	24
	2008	944	19	604	30	-	-	133	14	517	17	668	18	352	27
	2007	799	18	589	30	-	-	126	14	501	17	523	17	344	28
Hispanic	2011	359	4	94	4	17	3	48	4	201	6	182	5	46	3
	2010	364	4	81	4	12	3	47	4	181	6	133	3	49	3

		Federal financial agency employees (number and percent)													
Race/ethnicity	Year	FDIC		Federal Reserve		FHFA[a]		NCUA		OCC		SEC		Treasury	
	2009	261	4	75	3	-	-	43	4	181	6	144	4	54	4
	2008	198	4	70	3	-	-	35	4	168	6	137	4	47	4
	2007	181	4	68	3	-	-	34	4	157	5	129	4	50	4
Asian	2011	374	4	271	12	46	9	56	5	212	6	354	9	80	5
	2010	372	4	238	11	33	8	52	5	169	6	352	9	79	5
	2009	283	4	231	11	-	-	37	4	163	5	319	9	60	4
	2008	199	4	204	10	-	-	36	4	158	5	312	9	53	4
	2007	25	1	187	10	-	-	33	4	145	5	266	8	49	4
Other	2011	128	2	42	2	1	0	27	2	67	2	28	1	17	1
	2010	120	1	40	2	1	0	22	2	51	2	66	2	19	1
	2009	77	1	38	2	-	-	22	2	54	2	62	2	12	1
	2008	32	1	35	2	-	-	12	1	44	1	51	1	12	1
	2007	162	4	35	2	-	-	14	2	36	1	32	1	8	1

Source: GAO analysis of agency reports.

Notes: Percentages are rounded to the nearest percent.

For our analysis, we reviewed the numbers of employees the agencies reported according to race/ethnicity and gender in table A3 of their MD-715 reports from 2007 through 2011. These data are based on information self-reported by employees to each agency and there were some differences in reporting across the agencies. In some years, some agencies reported all employees—permanent and temporary—in their A3 tables while others reported permanent employees only.

[a]FHFA was established in 2008 and started reporting workforce data for 2010.

Table 12: Percentage of Minorities among All Employees at the 12 Reserve Banks, 2007-2011

		Reserve Bank employees (number and percent)																							
Race/ ethnicity	Year	Atlanta		Boston		Chicago		Cleveland		Dallas		Kansas City		Minneapolis		New York		Philadelphia		Richmond		San Francisco		St. Louis	
All	2011	1,594	100%	875	100%	1,431	100%	1,094	100%	1,098	100%	1,225	100%	1,011	100%	2,955	100%	839	100%	2,444	100%	1,495	100%	955	100%
	2010	1,623	100	858	100	1,353	100	1,276	100	1,110	100	1,292	100	1,004	100	2,999	100	840	100	2,356	100	1,514	100	944	100
	2009	1,728	100	868	100	1,379	100	1,340	100	1,168	100	1,220	100	1,051	100	2,940	100	914	100	2,421	100	1,632	100	932	100
	2008	1,886	100	884	100	1,415	100	1,511	100	1,225	100	1,277	100	1,172	100	2,791	100	1,016	100	2,534	100	1,700	100	987	100
	2007	2,017	100	978	100	1,532	100	1,568	100	1,269	100	1,357	100	1,278	100	2,860	100	1,092	100	2,733	100	1,779	100	1,089	100
White	2011	839	53	607	69	889	62	878	80	551	50	1,026	84	830	82	1,617	55	539	64	1,721	70	701	47	691	72
	2010	839	52	607	71	845	62	1,017	80	555	50	1,082	84	830	83	1,626	54	534	64	1,672	71	703	46	679	72
	2009	864	50	611	70	850	62	1,063	79	561	48	1,018	83	879	84	1,596	54	562	61	1,719	71	758	46	674	72
	2008	899	48	614	69	866	61	1,168	77	572	47	1,050	82	980	84	1,522	55	581	57	1,753	69	768	45	694	70
	2007	949	47	676	69	933	61	1,213	77	590	46	1,096	81	1,071	84	1,630	57	613	56	1,823	67	774	44	740	68
Total minority	2011	755	47	268	31	542	38	216	20	547	50	199	16	181	18	1,338	45	300	36	723	30	794	53	264	28
	2010	784	48	251	29	508	38	259	20	555	50	210	16	174	17	1,373	46	306	36	684	29	811	54	265	28
	2009	864	50	257	30	529	38	277	21	607	52	202	17	172	16	1,344	46	352	39	702	29	874	54	258	28
	2008	987	52	270	31	549	39	343	23	653	53	227	18	192	16	1,269	45	435	43	781	31	932	55	293	30
	2007	1068	53	302	31	599	39	355	23	679	54	261	19	207	16	1,230	43	479	44	910	33	1,005	56	349	32
Black or African American	2011	525	33	108	12	279	19	167	15	238	22	93	8	79	8	494	17	184	22	509	21	101	7	209	22
	2010	557	34	106	12	275	20	208	16	229	21	107	8	81	8	523	17	198	24	503	21	116	8	215	23
	2009	634	37	107	12	310	22	228	17	269	23	109	9	82	8	530	18	248	27	533	22	140	9	216	23
	2008	758	40	117	13	334	24	290	19	326	27	120	9	102	9	539	19	330	32	603	24	160	9	254	26
	2007	830	41	132	13	391	26	308	20	354	28	146	11	118	9	560	20	372	34	713	26	178	10	315	29
Hispanic	2011	147	9	45	5	132	9	12	1	235	21	57	5	24	2	301	10	31	4	65	3	179	12	19	2

		Reserve Bank employees (number and percent)																							
Race/ ethnicity	Year	Atlanta		Boston		Chicago		Cleveland		Dallas		Kansas City		Minneapolis		New York		Philadelphia		Richmond		San Francisco		St. Louis	
	2010	148	9	41	5	114	8	13	1	247	22	59	5	21	2	301	10	28	3	58	2	177	12	19	2
	2009	152	9	44	5	112	8	13	1	260	22	51	4	20	2	290	10	28	3	56	2	205	13	15	2
	2008	148	8	47	5	102	7	16	1	265	22	62	5	20	2	278	10	28	3	59	2	224	13	15	2
	2007	153	8	52	5	96	6	14	1	266	21	67	5	20	2	280	10	29	3	63	2	251	14	9	1
Asian	2011	69	4	112	13	119	8	29	3	67	6	41	3	71	7	523	18	80	10	129	5	490	33	33	3
	2010	68	4	104	12	109	8	31	2	73	7	40	3	66	7	532	18	75	9	103	4	493	33	29	3
	2009	68	4	105	12	95	7	29	2	70	6	38	3	64	6	508	17	73	8	96	4	502	31	25	3
	2008	72	4	106	12	101	7	28	2	54	4	41	3	65	6	439	16	75	7	103	4	516	30	22	2
	2007	78	4	117	12	104	7	26	2	53	4	43	3	64	5	389	14	75	7	113	4	547	31	23	2
Other	2011	14	1	3	0	12	1	8	1	7	1	8	1	7	1	20	1	5	1	20	1	24	2	3	0
	2010	11	1	0	0	10	1	7	1	6	1	4	0	6	1	17	1	5	1	20	1	25	2	2	0
	2009	10	1	1	0	12	1	7	1	8	1	4	0	6	1	16	1	3	0	17	1	27	2	2	0
	2008	9	0	0	0	12	1	9	1	8	1	4	0	5	0	13	0	2	0	16	1	32	2	2	0
	2007	7	0	1	0	8	1	7	0	6	0	5	0	5	0	1	0	3	0	21	1	29	2	2	0

Source: GAO analysis of EEO-1 reports provided by Reserve Banks.

Note: Percentages are rounded to the nearest percent.

Table 13: Percentage of Women among All Employees at Seven Federal Financial Agencies, 2007-2011

		Federal financial agency employees (number and percent)													
Gender	Year	FDIC		Federal Reserve		FHFA[a]		NCUA		OCC		SEC		Treasury	
All	2011	8,398	100%	2,274	100%	494	100%	1,159	100%	3,560	100%	3,812	100%	1,586	100%
	2010	8,316	100	2,137	100	406	100	1,095	100	3,054	100	3,897	100	1,599	100
	2009	6,530	100	2,143	100	-	-	1,024	100	3,117	100	3,720	100	1,529	100
	2008	5,028	100	2,028	100	-	-	934	100	3,039	100	3,653	100	1,295	100
	2007	4,428	100	1,945	100	-	-	929	100	3,000	100	3,154	100	1,223	100
Men	2011	4,846	58	1,238	54	277	56	640	55	1,917	54	1,984	52	822	52
	2010	4,852	58	1,138	53	219	54	589	54	1,587	52	2,024	52	827	52
	2009	3,735	57	1,140	53	-	-	555	54	1,617	52	1,924	52	798	52
	2008	2,809	56	1,080	53	-	-	515	55	1,584	52	1,882	52	657	51
	2007	2,462	56	1,022	53	-	-	509	55	1,583	53	1,655	52	613	50
Women	2011	3,552	42	1,036	46	217	44	519	45	1,643	46	1,828	48	764	48
	2010	3,464	42	999	47	187	46	506	46	1,467	48	1,873	48	772	48
	2009	2,795	43	1,003	47	-	-	469	46	1,500	48	1,796	48	731	48
	2008	2,219	44	948	47	-	-	419	45	1,455	48	1,771	48	638	49
	2007	1,966	44	923	47	-	-	420	45	1,417	47	1,499	48	610	50

Source: GAO analysis of agency reports.

Note: Percentages are rounded to the nearest percent.

For our analysis, we reviewed the numbers of employees the agencies reported according to race/ethnicity and gender in table A3 of their MD-715 reports from 2007 through 2011. These data are based on information self-reported by employees to each agency and there were some differences in reporting across the agencies. In some years, some agencies reported all employees—permanent and temporary—in their A3 tables while others reported permanent employees only.

[a]FHFA was established in 2008 and started reporting workforce data for 2010.

Table 14: Percentage of Women among All Employees at the 12 Reserve Banks, 2007-2011

Race/ Ethnicity	Year	Reserve Bank employees (number and percent)																							
		Atlanta		Boston		Chicago		Cleveland		Dallas		Kansas City		Minneapolis		New York		Philadelphia		Richmond		San Francisco		St. Louis	
All	2011	1,594	100%	875	100%	1,431	100%	1,094	100%	1,098	100%	1,225	100%	1,011	100%	2,955	100%	869	100%	2,444	100%	1,495	100%	955	100%
	2010	1,623	100	858	100	1,353	100	1,276	100	1,110	100	1,292	100	1,004	100	2,999	100	840	100	2,356	100	1,514	100	944	100
	2009	1,728	100	868	100	1,379	100	1,340	100	1,168	100	1,220	100	1,051	100	2,940	100	914	100	2,421	100	1,632	100	932	100
	2008	1,886	100	884	100	1,415	100	1,511	100	1,225	100	1,277	100	1,172	100	2,791	100	1016	100	2,534	100	1,700	100	987	100
	2007	2,017	100	978	100	1,532	100	1,568	100	1,269	100	1,357	100	1,278	100	2,860	100	1092	100	2,733	100	1,779	100	1,089	100
Men	2011	853	54	475	54	775	54	594	54	631	57	650	53	473	47	1,587	54	503	60	1,460	60	889	59	517	54
	2010	856	53	469	55	728	54	648	51	640	58	677	52	468	47	1,621	54	498	59	1,396	59	905	60	510	54
	2009	913	53	471	54	729	53	678	51	669	57	617	51	474	45	1,600	54	432	58	1,410	58	950	58	499	54
	2008	964	51	477	54	707	50	727	48	685	56	626	49	497	42	1,506	54	567	56	1,420	56	959	56	526	53
	2007	1,008	50	491	50	745	49	741	47	689	54	647	48	521	41	1,512	53	603	55	1,505	55	992	56	556	51
Women	2011	741	46	400	46	656	46	500	46	467	43	575	47	538	53	1,368	46	336	40	984	40	606	41	438	46
	2010	767	47	389	45	625	46	628	49	470	42	615	48	536	53	1,378	46	342	41	960	41	609	40	434	46
	2009	815	47	397	46	650	47	662	49	499	43	603	49	577	55	1,340	46	382	42	1,011	42	682	42	433	46
	2008	922	49	407	46	708	50	784	52	540	44	651	51	675	58	1,285	46	449	44	1,114	44	741	44	461	47
	2007	1,009	50	487	50	787	51	827	53	580	46	710	52	757	59	1,348	47	489	45	1,228	45	787	44	533	49

Source: GAO analysis of EEO-1 reports provided by Reserve Banks.

Note: Percentages are rounded to the nearest percent.

Appendix V: Comments from the Consumer Financial Protection Bureau

cfpb Consumer Financial Protection Bureau

1700 G Street NW, Washington, DC 20552

March 25, 2013

Mr. Daniel Garcia-Diaz
Director
Financial Markets and Community Investment
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Garcia-Diaz:

Thank you for the opportunity to comment on the Government Accountability Office's (GAO) draft report, *Diversity Management, Trends and Practices in the Financial Services Industry and Agencies After the Recent Financial Crisis*, GAO-13-238.

This report examines workforce diversity in the financial services industry and in the financial regulatory agencies from 2007 through 2011 and also efforts by the financial regulatory agencies to implement workforce and contractor diversity practices under the Dodd-Frank Act. The Consumer Financial Protection Bureau (CFPB or Bureau) opened its doors for business in July 2011, and its Office of Minority and Women Inclusion (OMWI) was established in January 2012. As the report notes, the Director of OMWI assumed his duties on April 30, 2012.

The report contains one recommendation:

> To enhance the availability of information on the progress and impact of agency and reserve bank diversity practices, we are recommending to CFPB…that each OMWI report on efforts to measure the progress of its employment diversity and inclusion practices, including measurement outcomes as appropriate, to indicate areas for improvement as part of its annual report to Congress.

CFPB concurs with the recommendation.

As we discussed during our meetings, the OMWI at CFPB is the newest OMWI to open following the creation of the Bureau in the Dodd-Frank Act. Because the Bureau was formed after the period 2007-11, the report does not contain workforce information from that period. The CFPB did provide demographic information about its workforce as of May 2012.

Since I began my tenure as the OMWI Director on April 30, 2012, the office has been building capacity to address the three primary responsibilities of the office: promoting

diversity and inclusion in the Bureau's workforce, in the Bureau's procurement, and working with our fellow financial regulators and their OMWI offices to create standards for diversity and inclusion at regulated entities. The office has made good progress during these opening months in addressing these disparate challenges, and has set a solid foundation for the work that lies ahead.

We agree that reporting on appropriate measures to improve diversity and inclusion in employment would be a valuable addition to the annual report to Congress. Much of our work in this first year is obtaining and understanding the baselines for measurements. We expect in future reports to build out this reporting, as appropriate, and to address areas for improvement.

Thank you for the opportunity to comment on the report.

Sincerely,

Stuart J. Ishimaru
Director
Office of Minority and Women Inclusion

consumerfinance.gov

Appendix VI: Comments from the Federal Reserve Banks

FEDERAL RESERVE BANKS

of

Boston • New York • Philadelphia • Cleveland • Richmond • Atlanta
Chicago • St. Louis • Minneapolis • Kansas City • Dallas • San Francisco

March 25, 2013

Mr. Daniel Garcia-Diaz
Director
Financial Markets and Community Investment
Government Accountability Office
441 G Street, NW
Washington, D.C. 20548

Dear Mr. Garcia-Diaz:

Thank you for the opportunity to respond to the GAO's draft report on "Diversity Management: Trends and Practices in the Financial Services Industry and Agencies after the Recent Financial Crisis" (GAO-13-238). This letter represents a consolidated response from all twelve Directors of the Office of Minority and Women Inclusion (OMWI) at the Reserve Banks.

The Reserve Banks are committed to promoting workforce diversity and increasing contracting opportunities for minority-owned and women-owned businesses. As the GAO report recognizes, significant efforts have been undertaken to satisfy the requirements of Section 342 of the Dodd-Frank Wall Street Reform and Consumer Protection Act. The report contains one recommendation to the agencies and Reserve Banks: that each OMWI report on its efforts to measure the progress of diversity and inclusion practices in its annual report to Congress. The Reserve Banks currently include some measurements in the annual reports. We will evaluate these current efforts and consider additional ways to measure and report on the progress of our diversity practices.

We appreciate the attention of the GAO to this important topic and wish to thank the GAO staff for the courtesy and professionalism demonstrated during the review.

FEDERAL RESERVE BANKS

of

Boston • New York • Philadelphia • Cleveland • Richmond • Atlanta
Chicago • St. Louis • Minneapolis • Kansas City • Dallas • San Francisco

Marques Benton
Federal Reserve Bank of Boston

Diane Ashley
Federal Reserve Bank of New York

Mary Ann Hood
Federal Reserve Bank of Philadelphia

David W. Hollis
Federal Reserve Bank of Cleveland

Tammy H. Cummings
Federal Reserve Bank of Richmond

Joan H. Buchanan
Federal Reserve Bank of Atlanta

Valerie Van Meter
Federal Reserve Bank of Chicago

James Price
Federal Reserve Bank of St. Louis

Duane Carter
Federal Reserve Bank of Minneapolis

Donna J. Ward
Federal Reserve Bank of Kansas City

Tyrone Gholson
Federal Reserve Bank of Dallas

Susan A. Sutherland
Federal Reserve Bank of San Francisco

Appendix VII: Comments from the Federal Reserve Board

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
WASHINGTON, DC 20551

March 26, 2013

Mr. Daniel Garcia-Diaz
Director, Financial Markets
and Community Investment
Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Garcia-Diaz:

Thank you for the opportunity to comment on your draft report entitled "Diversity Management: Trends and Practices in the Financial Services Industry and Agencies After the Recent Financial Crisis". The Federal Reserve Board takes seriously its efforts to encourage and promote diversity in its workforce and contracting decisions. As the draft report shows, the Federal Reserve Board's representation of both minorities and women at the senior management-level increased from 2007 through 2011. In addition, the report determined that the representation of both minorities and women among mid-level officials and managers at the Federal Reserve Board in 2011 was highest among the agencies the GAO reviewed.

The report includes one recommendation to the agencies and reserve banks, which is:
To enhance the availability of information on the progress and impact of agency and Reserve Bank diversity practices, we are recommending to CFPB, FDIC, the Federal Reserve Board, FHFA, NCUA, OCC, SEC, Treasury, and the Reserve Banks that each OMWI report on efforts to measure the progress of its employment diversity and inclusion practices, including measurement outcomes as appropriate, to indicate areas for improvement as part of its annual report to Congress.

www.federalreserve.gov

As we have discussed with the GAO, this recommendation is consistent with our ongoing practices. We will look for additional ways to measure and report on the progress of our diversity practices.

We appreciate the thorough and comprehensive analysis the GAO has provided.

Sheila Clark
Director
Office of Minority and Women and Inclusion

Appendix VIII: Comments from the Federal Deposit Insurance Corporation

FDIC
Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226-3500
Office of Minority and Women Inclusion

March 29, 2013

Mr. Daniel Garcia-Diaz
Director, Financial Markets and Community Investment
United States Government Accountability Office
Washington, DC 20548

Dear Mr. Garcia-Diaz:

The Federal Deposit Insurance Corporation (FDIC) reviewed the GAO report *Diversity Management: Trends and Practices in the Financial Services Industry and Agencies After the Recent Financial Crisis* (Report) (GAO-13-238). The Report stated each agency should include in its annual OMWI report to Congress efforts to measure the progress of its diversity practices. The FDIC agrees with the Report's recommendation and will include efforts to measure the progress of our diversity practices in annual OMWI report to Congress. We believe this recommendation is important to not only meeting the requirements of Section 342 of the Dodd-Frank Act, but to the success of the FDIC in carrying out its mission responsibilities.

The FDIC is committed to providing all employees with a work environment that embodies excellence, and acknowledges and honors the diversity of its employees. In 2012, the FDIC Acting Chairman established a number of Performance Goals designed to enhance the FDIC's commitment to diversity, inclusion, and equal employment opportunity, including asking the Corporation's senior leaders to update the FDIC's Diversity Strategic Plan and directing each division and major office to develop its own strategic plans to identify steps to increase diversity through the FDIC's recruiting and hiring.

The FDIC's updated 2013 Diversity and Inclusion Strategic Plan addresses the goals of Executive Order 13583, dated August 18, 2011, which calls for federal agencies to develop and implement a more comprehensive, integrated, and strategic focus on diversity and inclusion. The plan lays out a course for achieving workforce diversity by recruiting from a diverse, qualified group of potential applicants; cultivating workplace inclusion through collaboration, flexibility, and fairness; and ensuring sustainability of diversity and inclusion achievements by equipping leaders with the ability to manage diversity, measure results, and refine approaches based on available data. The updated plan issued on March 1, 2013, follows the guidance issued by the U.S. Office of Personnel Management (OPM) in November 2011, and identifies a number of strategies and action plans to address workforce diversity, workplace inclusion, and sustainability.

Specifically, under sustainability, the FDIC will develop structures and strategies to equip leaders with the ability to manage diversity, be accountable, measure results, refine approaches on the basis of such data, and institutionalize a culture of inclusion. This objective will improve

diversity and inclusion analytics and reporting by using a strategy to make diversity and inclusion reporting more actionable through improvements in data collection, presentation, and reporting frequency.

Further, in 2012, the FDIC contracted for a third party review of diversity and inclusion programs and activities to help us identify additional initiatives to strengthen our diversity practices.

Thank you for the opportunity to review the Report.

Sincerely,

D. Michael Collins
Director

Appendix IX: Comments from the Federal Housing Finance Agency

Federal Housing Finance Agency
Constitution Center
400 7th Street, S.W.
Washington, D.C. 20024
Telephone: (202) 649-3800
Facsimile: (202) 649-1071
www.fhfa.gov

March 25, 2013

Mr. Daniel Garcia-Diaz
Director
Financial Markets and Community Investment
Government Accountability Office (GAO)
441 G Street, NW
Washington, DC 20548

Dear Mr. Garcia-Diaz:

Thank you for the opportunity to review and comment on the Government Accountability Office (GAO) Report, *Diversity Management; Trends and Practices in the Financial Services Industry and Agencies After the Recent Financial Crisis*.

During the review GAO examined diversity in the financial services industry, the federal financial agencies, and the Federal Reserve Banks (Reserve Banks) and efforts of the agencies and Reserve Banks to implement diversity practices under the Dodd-Frank Act. The GAO has recommended that the agencies and Reserve Banks, including the Federal Housing Finance Agency (FHFA), should include in its annual Office of Minority and Women Inclusion (OMWI) report to Congress efforts to measure the progress of its diversity practices, including measurement outcomes as appropriate, to indicate areas for improvement as part of their annual reports to Congress.

FHFA agrees with the recommendation to include in our annual OMWI report to Congress our efforts to measure the progress of our diversity efforts, and will include this information in FHFA's 2013 OMWI Annual Report to Congress.

If you have any questions, please do not hesitate to contact me.

Sincerely,

Nancy

Nancy P. Burnett
Acting Associate Director
Office of Minority and Women Inclusion
Federal Housing Finance Agency

Appendix X: Comments from the National Credit Union Administration

National Credit Union Administration

March 26, 2013

Ms. Kay D. Kuhlman
Assistant Director
Financial Markets and Community Investment
U. S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Kuhlman:

Thank you for the opportunity to review and comment on the draft GAO report for the Committee on Financial Services of the U.S. House of Representatives. The report, titled "Diversity Management: Trends and Practice in the Financial Services Industry and Agencies After the Recent Financial Crisis" is comprehensive and appropriately outlines the changes in the agencies' workforce and in the industry from 2007 to 2011.

Overall, your report indicates the financial services agencies made some progress in diversity although additional progress needs to be made. In 2012, NCUA continues to make strides and address challenges in achieving its goal of "cultivating a diverse, well trained, and motivated workforce." The establishment of the Office of Minority and Women Inclusion, in 2011, helped NCUA focus its diversity efforts. Our 2012 Annual Report to Congress highlights many of the accomplishments achieved in diversity of the workforce and contracting as well as the challenges.

We agree with your recommendation and will work towards reporting on our efforts to measure the progress of the workforce diversity and inclusion practices, including measurement outcomes as appropriate, as part of the annual reports to Congress.

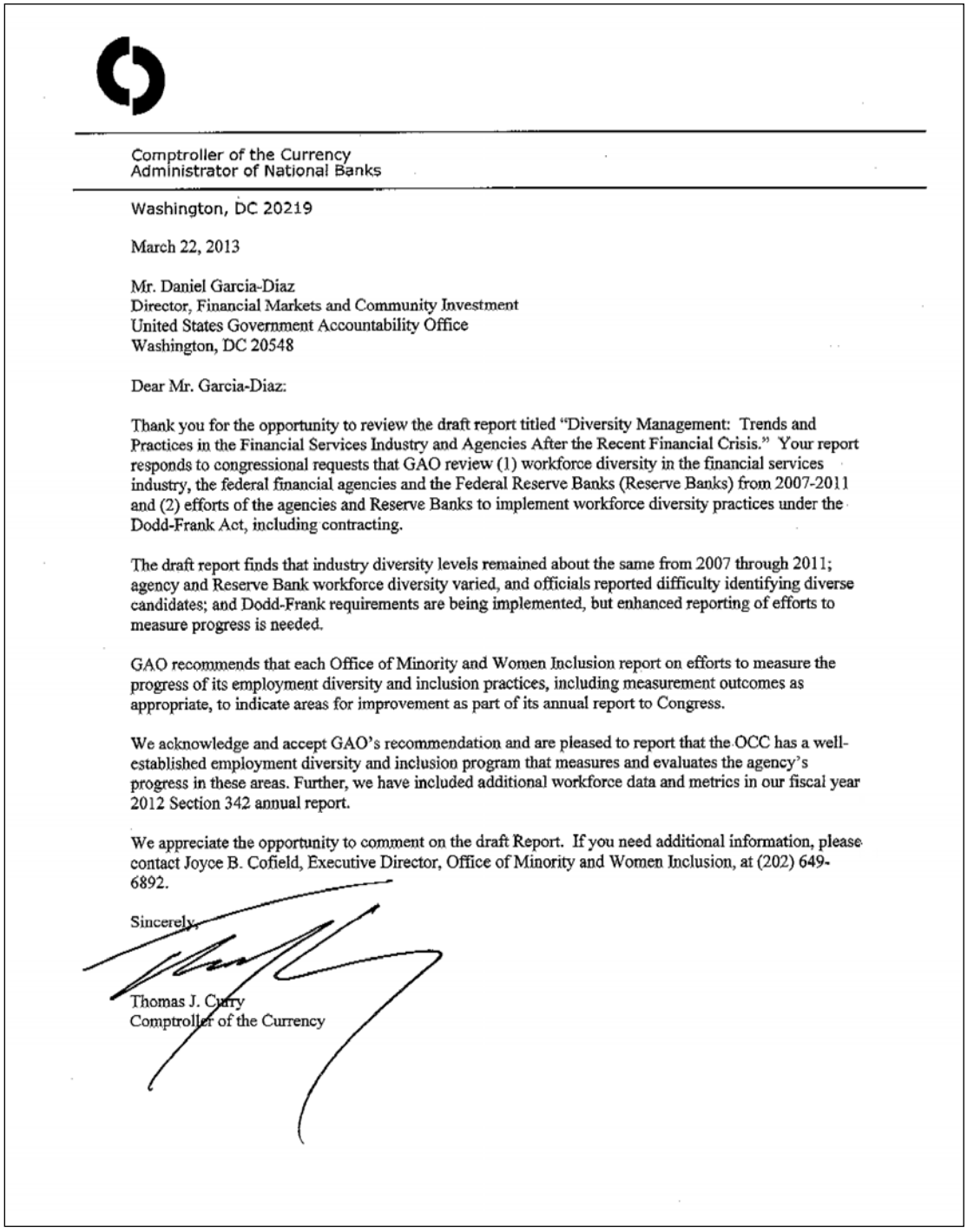
Sincerely,

Mark A. Treichel

Mark A. Treichel
Executive Director

1775 Duke Street - Alexandria, VA 22314-3428 - 703-518-6300

Appendix XI: Comments from the Comptroller of the Currency



Comptroller of the Currency
Administrator of National Banks

Washington, DC 20219

March 22, 2013

Mr. Daniel Garcia-Diaz
Director, Financial Markets and Community Investment
United States Government Accountability Office
Washington, DC 20548

Dear Mr. Garcia-Diaz:

Thank you for the opportunity to review the draft report titled "Diversity Management: Trends and Practices in the Financial Services Industry and Agencies After the Recent Financial Crisis." Your report responds to congressional requests that GAO review (1) workforce diversity in the financial services industry, the federal financial agencies and the Federal Reserve Banks (Reserve Banks) from 2007-2011 and (2) efforts of the agencies and Reserve Banks to implement workforce diversity practices under the Dodd-Frank Act, including contracting.

The draft report finds that industry diversity levels remained about the same from 2007 through 2011; agency and Reserve Bank workforce diversity varied, and officials reported difficulty identifying diverse candidates; and Dodd-Frank requirements are being implemented, but enhanced reporting of efforts to measure progress is needed.

GAO recommends that each Office of Minority and Women Inclusion report on efforts to measure the progress of its employment diversity and inclusion practices, including measurement outcomes as appropriate, to indicate areas for improvement as part of its annual report to Congress.

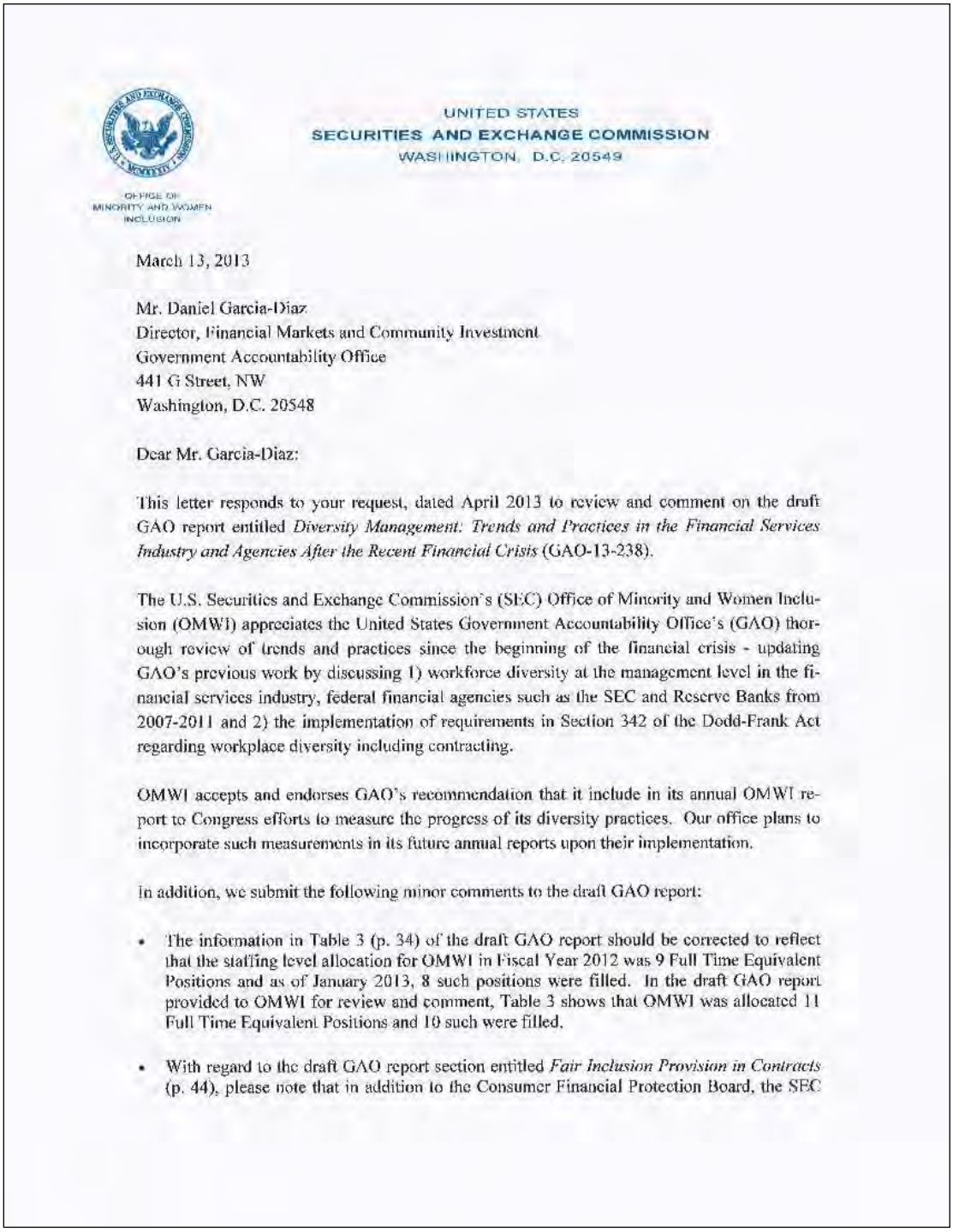
We acknowledge and accept GAO's recommendation and are pleased to report that the OCC has a well-established employment diversity and inclusion program that measures and evaluates the agency's progress in these areas. Further, we have included additional workforce data and metrics in our fiscal year 2012 Section 342 annual report.

We appreciate the opportunity to comment on the draft Report. If you need additional information, please contact Joyce B. Cofield, Executive Director, Office of Minority and Women Inclusion, at (202) 649-6892.

Sincerely,

Thomas J. Curry
Comptroller of the Currency

Appendix XII: Comments from the Securities and Exchange Commission



UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

OFFICE OF
MINORITY AND WOMEN
INCLUSION

March 13, 2013

Mr. Daniel Garcia-Diaz
Director, Financial Markets and Community Investment
Government Accountability Office
441 G Street, NW
Washington, D.C. 20548

Dear Mr. Garcia-Diaz:

This letter responds to your request, dated April 2013 to review and comment on the draft GAO report entitled *Diversity Management: Trends and Practices in the Financial Services Industry and Agencies After the Recent Financial Crisis* (GAO-13-238).

The U.S. Securities and Exchange Commission's (SEC) Office of Minority and Women Inclusion (OMWI) appreciates the United States Government Accountability Office's (GAO) thorough review of trends and practices since the beginning of the financial crisis - updating GAO's previous work by discussing 1) workforce diversity at the management level in the financial services industry, federal financial agencies such as the SEC and Reserve Banks from 2007-2011 and 2) the implementation of requirements in Section 342 of the Dodd-Frank Act regarding workplace diversity including contracting.

OMWI accepts and endorses GAO's recommendation that it include in its annual OMWI report to Congress efforts to measure the progress of its diversity practices. Our office plans to incorporate such measurements in its future annual reports upon their implementation.

In addition, we submit the following minor comments to the draft GAO report:

- The information in Table 3 (p. 34) of the draft GAO report should be corrected to reflect that the staffing level allocation for OMWI in Fiscal Year 2012 was 9 Full Time Equivalent Positions and as of January 2013, 8 such positions were filled. In the draft GAO report provided to OMWI for review and comment, Table 3 shows that OMWI was allocated 11 Full Time Equivalent Positions and 10 such were filled.

- With regard to the draft GAO report section entitled *Fair Inclusion Provision in Contracts* (p. 44), please note that in addition to the Consumer Financial Protection Board, the SEC

has also been using the equal employment opportunity statement contained in the Federal Acquisition Regulation in executed contracts while the SEC develops an inclusion statement pursuant to Section 342(c)(2).

- Under the same section entitled *Fair Inclusion Provision in Contracts* and in relation to Section 342 (c)(1) and (2), OMWI suggests restating the second sentence to provide as follows: "Section 342 of the Dodd-Frank Act requires agencies and Reserve Banks to develop procedures for review and evaluation of contract proposals and for hiring service providers that include a written statement that a contractor shall ensure, to the maximum extent possible, the fair inclusion of women and minorities in the workforce of the contractor and, as applicable, subcontractors."

Thank you for the consideration that you and your staff have shown our staff and for the opportunity to comment on this draft report. If you have any questions or would like to further discuss this letter, please feel free to contact me at (202) 551-6503.

Sincerely,

Pamela A. Gibbs
Director

Appendix XIII: Comments from the Treasury Department

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

March 29, 2013

Daniel Garcia-Diaz
Director, Financial Markets and Community Investment
Government Accountability Office
441 G Street NW
Washington, DC 20548

Sent via email to trinderj@gao.gov

Dear Mr. Garcia-Diaz,

Thank you for providing the Department of the Treasury an opportunity to review your draft report entitled *Diversity Management: Trends and Practices in the Financial Services Industry and Agencies After the Recent Financial Crisis*. Covering 2007 to 2011, the report provides important workforce trends leading up to the FY 2011 baseline year for the Treasury's Departmental Offices, Office of Minority and Women Inclusion (OMWI). While the workforce of Treasury's Departmental Offices is comprised of a different range of critical occupations than those of the financial services industry, the federal reserve banks and the other federal financial agencies, the data in the draft report are relevant to our analysis of that segment of common occupations in our workforce.

We welcome the GAO recommendation to incorporate one of the nine leading diversity practices as part of the analysis in future OMWI annual reports to Congress. This recommendation is consistent with the efforts of Treasury's Departmental Offices to move beyond using only demographic representation to gauge the status and progress of diversity and inclusion within the Departmental Offices.

While there is still much more work to be done, we value the important strides that have been made in workforce and business diversity within Treasury's Departmental Offices.

Sincerely,

Lorraine Cole

Lorraine Cole, Ph.D.
Director, Office of Minority and Women Inclusion

Appendix XIV: GAO Contact and Staff Acknowledgments

GAO Contact

Daniel Garcia-Diaz, (202) 512-8678 or garciadiazd@GAO.gov

Staff Acknowledgments

In addition to the individual named above, Kay Kuhlman, Assistant Director; Heather Chartier; Brendan Kretzschmar; Alma Laris; Ruben Montes de Oca; Cheryl Peterson; Jennifer Schwartz; Jena Sinkfield; Andrew Stavisky; and Julie Trinder made major contributions to this report.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

DISCIPLINARY BEST PRACTICES AND ADVISORY GUIDELINES UNDER THE NO FEAR ACT

September 2008

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Working for America

A MESSAGE FROM THE ACTING DIRECTOR OF THE OFFICE OF PERSONNEL MANAGEMENT

I am pleased to release the report *Disciplinary Best Practices and Advisory Guidelines Under the No FEAR Act*. This report discusses the results of a study by OPM of agency best practices for taking disciplinary action for conduct inconsistent with "Antidiscrimination Laws" and "Whistleblower Protection Laws" as those terms are defined in 5 CFR 724.102. The report also provides advisory guidelines agencies may follow in taking such disciplinary actions. The study and the advisory guidelines were required by the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (No FEAR Act).

The No FEAR Act and OPM's regulations at 5 CFR 724.404 require each agency to provide a written statement to the Speaker of the U.S. House of Representatives; the President Pro Tempore of the U.S. Senate; the Chair, Equal Employment Opportunity Commission (EEOC); the Attorney General; and the Director, OPM describing in detail the extent to which the agency will follow the advisory guidelines. The specific content of the written statements is prescribed in the regulations. The statements must be submitted within 30 working days of the date of this report.

I strongly encourage agencies to draw on the best practices discussed in the report and follow the advisory guidelines to strengthen compliance with the Antidiscrimination Laws and the Whistleblower Protection Laws. As Congress noted in enacting the No FEAR Act: "Federal agencies cannot be run effectively if those agencies practice or tolerate discrimination."

The report also is available on the OPM Web site at www.opm.gov.

Michael W. Hager
Acting Director

DISCIPLINARY BEST PRACTICES AND ADVISORY GUIDELINES UNDER THE NO FEAR ACT

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report provides the results of a study of agency best practices for taking disciplinary action for employee conduct inconsistent with "Antidiscrimination Laws" and "Whistleblower Protection Laws" as those terms are defined in 5 CFR 724.102. The report also provides advisory guidelines agencies may follow when taking appropriate disciplinary action for such conduct. The study and the advisory guidelines are required by the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (No FEAR Act).

Methodology

The U.S. Office of Personnel Management (OPM) conducted the study. As part of the study, OPM reviewed and analyzed annual reports required by the No FEAR Act and provided by 48 agencies. In addition, OPM conducted interviews with officials from 11 agencies and five major agency components concerning their practices in taking disciplinary actions. In selecting the agencies to interview, OPM took into account which agencies reported taking disciplinary actions in their No FEAR reports, which did not, and how agencies scored under the 2006 Federal Human Capital Survey (FHCS) concerning their employees' views on their leadership.

Best Practices

The best practices for taking appropriate disciplinary actions address a number of key components of an effective disciplinary process. Among the topics discussed are the development of disciplinary policies; the roles of supervisors, managers, and others; and the communication of information required to recognize and correct inappropriate conduct. Also discussed are preventive measures such as training that agencies have used to help create workplace environments conducive to reducing or preventing improper conduct.

Advisory Guidelines

There are six advisory guidelines agencies may follow to ensure appropriate disciplinary actions are taken for conduct inconsistent with Antidiscrimination Laws and Whistleblower Protection Laws. These guidelines address the development and communication of disciplinary policies, procedures for ensuring improper conduct is addressed, the necessary ingredients for taking appropriate discipline, the importance of agency officials working together to take action, the importance of good communications in dealing with inappropriate conduct, and the need to prepare staff to provide good advice to supervisors and managers. Agencies are required under the No FEAR Act and OPM's regulations to report to Congress and others within 30 working days of this report on the extent to which they will follow the advisory guidelines.

BACKGROUND

The United States and its citizens are best served when the Federal workplace is free of discrimination and retaliation. In order to maintain a productive workforce that is fully engaged in the many important missions of the Government, the rights of employees, former employees and applicants for Federal employment must be steadfastly protected and those who violate these rights must be held accountable. Agencies and departments ("agencies") should take appropriate and timely steps, including discipline, if appropriate, to address conduct inconsistent with "Antidiscrimination Laws" and "Whistleblower Protection Laws" (hereinafter "Antidiscrimination and Whistleblower Protection Laws" or "applicable laws") as defined in 5 CFR 724.102.

Title II of the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (No FEAR Act) requires a comprehensive study of best practices in the Executive branch for taking disciplinary action for conduct inconsistent with Antidiscrimination and Whistleblower Protection Laws. The Act also requires the issuance of advisory guidelines agencies may follow when taking disciplinary action for such conduct. OPM has completed the required study and is issuing this report on best practices and advisory guidelines.

Methodology

To identify agency best practices for addressing conduct inconsistent with Antidiscrimination and Whistleblower Protection Laws, OPM began its study by analyzing agencies' Fiscal Year (FY) 2006 No FEAR reports to identify which agencies took disciplinary action (as well as the conduct on which the action was based), reviewing their disciplinary policies where publicly available, and reviewing the results of the 2006 Federal Human Capital Survey (FHCS) to identify agencies having the most favorable employee perceptions about how effectively they manage their workforce.

From that review and analysis, OPM selected 11 agencies and five components for in-depth interviews to find out more about their practices for addressing inappropriate conduct. Specifically, OPM interviewed five of the six agencies which reported taking disciplinary action in FY 2006, as well as five agency components that had taken disciplinary action. In addition, OPM interviewed six agencies which reported no disciplinary action taken in their FY 2006 No FEAR reports and were among the 2006 FHCS Top-10 agencies where employees hold their leadership in high regard, both overall and on specific facets of leadership.

When possible, OPM interviewed both the Equal Employment Opportunity (EEO) and Employee Relations (ER) Directors to discuss the agency's disciplinary process and practices concerning antidiscrimination and whistleblower protection. In one

instance, OPM interviewed Office of General Counsel staff. OPM reviewed additional materials provided by agencies interviewed, including training and resource materials provided on agency Intranet sites, brochures, and CD-ROMs.

No FEAR Reports from Agencies

The FY 2006 No FEAR reports from agencies showed that six agencies took disciplinary action. Some of the agency reports provided detailed discussions of trends, causal analysis, and practical knowledge gained through experience with taking discipline. These discussions contributed to the identification of best practices for taking disciplinary action and preventive measures.

Federal Human Capital Survey Results

OPM reviewed the 2006 FHCS results for the agencies that took discipline and other agencies that were highly rated by their employees on leadership (i.e., the extent employees hold their leadership in high regard, both overall and on certain aspects of leadership). The leadership category of the FHCS includes the questions most relevant to successful antidiscrimination and whistleblower protection practices. These questions cover the employee's trust and confidence in his or her supervisor, the employee's level of respect for the organization's senior leaders, and whether leaders in an organization generate high levels of motivation and commitment in the workforce. For example, employees were asked to rate this statement: "I can disclose a suspected violation of any law, rule or regulation without fear of reprisal." The agencies which reported taking disciplinary action in FY 2006 ranked at the higher end of agencies scoring well for this question. Another FHCS item is: "Prohibited Personnel Practices (for example, illegally discriminating for or against any employee/applicant, obstructing a person's right to compete for employment, knowingly violating veterans' preference requirements) are not tolerated." All except one of the agencies taking disciplinary action were above the government-wide average for this FHCS item.

Agency Interviews

As noted above, five agencies and five agency components OPM interviewed took disciplinary actions for conduct inconsistent with Antidiscrimination Laws during FY 2006. Overall, the types of conduct on which discipline was based included creating a hostile work environment, harassment, sexual harassment, making ethnic slurs toward another employee, and other inappropriate conduct based upon race, gender, or some other protected category. The level of discipline agencies took included removal, demotion, and suspension. In some instances, employees resigned or retired to avoid discipline.

Agencies also used alternative means for correcting behavior. For example, some employees who could have been disciplined were reassigned or transferred. In addition, lesser penalties of written and oral counseling were used by one agency for misconduct by employees in certain circumstances. In another agency, alternative discipline was used where the collective bargaining agreement provided it could be initiated by the employee being disciplined. While alternative dispute resolution processes were available in some agencies, those agencies generally did not use them. No agencies reported taking discipline for conduct inconsistent with Whistleblower Protection Laws in FY 2006.

DISCIPLINARY BEST PRACTICES

In accordance with existing law (typically chapter 75 of title 5, United States Code), Federal employees may be disciplined for conduct inconsistent with applicable laws, up to and including removal from the Federal service. This study identified the following best practices to follow in considering such disciplinary actions.

Develop or modify disciplinary policy through joint effort of relevant agency program offices and senior staff

Agency disciplinary policies are likely to be effective if they are developed or modified collaboratively by the various offices involved in taking disciplinary actions and subsequently defending them before third parties when they are challenged. In this manner, technical and legal requirements could be reflected in the disciplinary policy. OPM found at least one agency that generally used a collaborative approach to craft policy and this agency created a No FEAR task force to propose revisions to the agency's disciplinary policy. The task force consisted of senior officials from the agency's offices of Human Resources (HR), EEO, Inspector General, legal counsel, and information and technology. The task force submitted its proposals to the agency's leadership for its joint review and approval. The revisions were fully implemented in FY 2007. Using this approach, the agency was able to generate commitment and buy-in from program offices and agency leadership before the policy was effected.

Provide written guidance to supervisors and managers on their responsibility to take appropriate steps to address conduct inconsistent with Antidiscrimination and Whistleblower Protection Laws, and on selecting the appropriate penalty

Supervisors and managers are responsible for observing and enforcing applicable laws. A disciplinary policy and any other written disciplinary guidance communicates

the agency's expectations with respect to correcting misconduct, including conduct inconsistent with antidiscrimination and whistleblower protection, and taking disciplinary action, when appropriate. Providing instruction on selecting an appropriate penalty is a critical part of any disciplinary policy or guidance because the application of appropriate penalties discourages behavior that undermines the efficiency of the civil service, while ensuring consistency of penalty selection. For that reason, it also helps ensure the action taken is legally defensible. Ideally, the policy and guidance should be drafted to be unambiguous to any reader regardless of his or her level of experience in dealing with misconduct and should set forth the steps supervisors and managers must take, including identifying which agency officials should be notified or consulted, and requiring disciplinary actions be taken promptly.

We found several agencies' disciplinary policies addressed the specific responsibility of supervisors and managers, and most policies clearly stated how supervisors and managers should determine the penalty. Some policies advised supervisors they are to keep employees informed of rules, regulations and standards of conduct and to take disciplinary action when appropriate. Several policies required supervisors to gather and carefully consider all relevant facts and circumstances, to include reviewing prior similar cases within the agency, before proposing or recommending disciplinary action. These instructions help ensure equity and consistency in the agency's imposition of discipline. Employee Relations (ER) staff and legal counsel can advise the supervisor or manager on the right charge to bring based on the conduct at issue, what is required to prove the charge and the penalties the agency has imposed in similar cases, if any, to assist in determining the appropriate penalty in his or her case.

One FHCS top-ranked agency recently modified its disciplinary policy to incorporate specific procedures for taking disciplinary actions against employees for conduct inconsistent with applicable laws. The revised policy now requires its EEO Director to notify a designated agency official in writing when he or she learns an employee may have engaged in this prohibited behavior. That official is then required to advise appropriate senior management who would be responsible for taking disciplinary action if warranted. The policy provides the specific content of the written notification and the steps for determining whether disciplinary action is warranted, including making an inquiry as soon as possible to gather and analyze facts. An unambiguous policy like any of the policies discussed here helps to affirm the agency's commitment to uphold Antidiscrimination and Whistleblower Protection Laws and will aid managers and supervisors in taking appropriate disciplinary action.

In addition to the disciplinary policy, other agency guidance can effectively inform supervisors of their responsibility in this area. For example, one agency issued a memorandum recently from its Deputy Director to senior management on disciplinary and adverse actions. The communication emphasized the responsibility of executive managers to ensure employees receive their due process rights in all disciplinary and

adverse actions. Managers were reminded discipline must promote the efficiency of the service, their decisions must reflect a conscientious application of all relevant factors, and they should use all available resources to properly take disciplinary action.

Another agency guide warned that any personnel action intended to punish an employee for whistleblowing may be investigated by the Office of Inspector General or the Office of Special Counsel as a reprisal, which is a prohibited personnel practice under 5 U.SC. 2302(b)(8)(A) and (B). Further, the guide stated a supervisor (or other employee) who is found to have reprised against an employee is subject to serious sanctions including, but not limited to, reduction in grade or removal from Federal employment. This and the other types of advisories provide support to an agency's disciplinary policy.

Require supervisors and managers to work with ER staff and legal counsel to take appropriate disciplinary action

Sound disciplinary actions are based on advice and guidance the supervisor or manager receives from those with expertise in taking and defending disciplinary actions. OPM found several agencies require supervisors and managers to consult with the ER office before taking disciplinary action, including obtaining their concurrence on all adverse action proposals and decision letters. In one agency, a similar requirement was supplemented by an instruction for the personnel officer to consult with an appropriate staff attorney or the organization involved in litigating appeals or grievances on behalf of the agency. When the supervisor or manager relies on advice from ER staff and legal counsel in taking disciplinary action, agencies can better ensure consistency in their disciplinary practices and the legal sufficiency of their cases.

Provide ER staff with the knowledge and tools necessary to provide managers sound advice and to elevate issues within the management chain if necessary

Agency ER offices are generally responsible for advising managers on how and when to take appropriate disciplinary action. A good working relationship between ER staff and the managers they advise is critical to ensuring the agency takes appropriate and defensible disciplinary action so employees know they will be held accountable for engaging in misconduct. Providing ER staff with adequate training, mentoring, and supervision to ensure they communicate accurate and well-reasoned advice to managers is the first step in establishing a good working relationship with management. Agency ER offices interviewed generally have good working relationships with management, because they have invested the time and resources

to ensure their staff provide managers with high-quality ER advice. In such cases, managers tend to respect and follow the advice provided. When managers are resistant to taking appropriate discipline, particularly in cases involving supervisory misconduct, ER offices indicated they elevate matters within the supervisory chain as needed and seek the assistance of legal counsel. By authorizing ER offices to notify higher-level agency officials if they believe management is not taking appropriate discipline, the agency can take steps to ensure misconduct is properly addressed.

Develop effective working relationships among the agency's ER office, EEO office, and legal counsel through periodic discussions or meetings

Encouraging regular communication between these offices (whether they are at headquarters, field offices or components) facilitates the appropriate exchange of information while establishing good working relationships among agency organizations. Several agencies have informal, periodic updates between two or more of these offices regarding new or ongoing issues within the agency. At one agency, in addition to meeting with colleagues from the other offices, the EEO office has appointed a member of its staff as a liaison with the agency's ER office. An audio-conference is used to bring ER and EEO staffs together at an agency where the discussion includes noticeable trends. The offices which hold these periodic meetings and communications have developed a level of trust which has allowed them to better understand each other's respective roles in addressing conduct inconsistent with applicable laws. These work relations are enhanced over time and, with the continued efforts by all parties, help the agency effectively address these cases of misconduct.

Use alternative discipline when appropriate

Alternative discipline is a tool available to managers and supervisors in correcting improper behavior. Working with ER and legal counsel, supervisors can use their discretion based on all of the information available to assess whether alternative discipline would result in correcting improper behavior. Few agencies use alternative discipline for conduct inconsistent with Antidiscrimination and Whistleblower Protection Laws. However, alternative discipline could be successfully used in some cases by giving an employee a last chance agreement, i.e., holding in abeyance appropriate disciplinary action pending successful completion of some requirement intended to correct inappropriate conduct. In such cases, if the terms of the last chance agreement are not met, the discipline would be imposed immediately, typically without further recourse by the employee disciplined. This alternative means of discipline may be appropriate, for example, when the employee has many years of service free of any previous disciplinary actions or allegations of improper conduct and demonstrates good potential for rehabilitation. Again, a careful analysis of the

facts and circumstances of the case and the employee's work record would be required to successfully utilize alternative discipline as a way to correct improper behavior.

PREVENTIVE MEASURES

Many agencies recognize the necessity for all responsible offices to work with managers and supervisors to address workplace issues before they develop into misconduct requiring disciplinary action. Several agencies, especially the FHCS top-performing organizations, focus on preventing misconduct. A number of approaches were helpful in efforts to deter misconduct. The following is a discussion of preventive measures.

Provide effective training and otherwise raise awareness of supervisors and managers about EEO and ER services and how to handle potential disciplinary issues early

Deliver training specifically for supervisors and managers

As part of an overall training strategy, training targeted toward supervisors and managers allows them to discuss issues, questions and solutions concerning disciplinary issues with their peers. Several agencies have found a variety of vehicles useful in delivering their supervisory training, such as agency leadership institutes or development programs, online training, conferences and classroom training. Through training dedicated to them, supervisors and managers are better able to identify conduct inconsistent with applicable laws and to understand their responsibilities with respect to addressing inappropriate conduct.

Several agencies provided training on taking disciplinary actions as part of a broader HR training program for supervisors and managers. One agency provided training as part of a forum to discuss various human capital issues while another agency's field office required all managers to attend an annual two-day retreat for EEO training. Another agency took advantage of the opportunity presented by a lengthy training program for supervisors and incorporated classroom training on issues such as diversity and anti-harassment.

An advantage of including training in taking disciplinary actions as part of a broader HR curriculum is supervisors are more likely to make time in their busy schedules to attend. Such events lead to increased awareness of antidiscrimination and whistleblower protection issues. In addition, they are opportunities for managers and supervisors to become familiar with who to contact for assistance.

Use a combination of computer-based training and in-person training

While there are pros and cons to using computer-based training versus classroom training, agencies are starting to use more online training. The benefits to using face-to-face training include the potential to increase the participants' understanding of covered materials through classroom questions and answers. The benefits of online computer-based training include ensuring an agency-wide audience receives the same message and its delivery to employees is cost effective.

Several agencies deliver in-person training to small groups to allow more interaction between the trainer and the audience. In addition, attendees learn a great deal through discussion of issues. A few agencies conduct training with a combination of online and at least a simulation of in-person delivery through computer interaction techniques, if not actual face-to-face classes. To give participants a more dynamic learning experience, one agency complemented the online training with audio-visual scenarios to continually engage participants. In another instance, an agency used a combination of online training (on antidiscrimination issues) followed by a panel discussion to receive questions. Such designs can assist agencies to effectively exploit the benefits of both types of training. Moreover, training that is fresh, interesting and diversified in delivery will help keep the audience engaged and attentive.

Include legal counsel as a presenter in training and awareness sessions for supervisors and managers

Agency legal counsel typically is an integral partner in advising management on addressing misconduct and how and when to take disciplinary action. Because it represents the agency before third-party adjudicators when disciplinary actions are challenged, it is important for supervisors and managers to understand when they should seek the advice of agency legal counsel to avoid potential legal liabilities.

Provide training on interpersonal and conflict resolution skills

Supervisors and managers must be able to work and communicate effectively with their employees to ensure workplace issues do not escalate into large problems requiring more formal action. This is a challenging skill to master. Supervisors must learn how to recognize early warning signs and not allow issues to fester and become more serious. To gain these skills, supervisors should be trained in interpersonal communications and related areas. Some agencies offer training opportunities for supervisors and managers on preventive tools and techniques in the areas of team building, emotional intelligence, and conflict resolution in the workplace.

Some agencies characterize on-site conflict resolution training as performing interventions or facilitated discussions. Some agencies have found this type of training to be very productive. At one agency, for example, a one-day session on team building was so helpful to the office, it requested the trainers to provide additional training, and a two-day session on the topic was provided. Follow-up one year later indicated success was sustained beyond the immediate intervention. At another agency, a Conflict-Management Initiative was successfully piloted and will be implemented as ongoing training. It is a one-day session on dealing with interpersonal conflict. Supervisors and managers are trained separately from employees in this program. Sometimes referred to as "soft" skills, interpersonal communication and associated proficiencies are essential components of strong, effective supervision and management.

Use a variety of media to communicate agency policy regarding conduct inconsistent with Antidiscrimination and Whistleblower Protection Laws

To reach the maximum number of employees, it is helpful to use various forms of communication. A multi-media effort, along with other types of outreach to employees, helps promote awareness of agency policies concerning improper conduct. The No FEAR Act requires agencies to ensure employees are trained in the agency's policies concerning antidiscrimination and whistleblower protection. A clearly defined antidiscrimination policy that defines prohibited behaviors was evident at all of the agencies interviewed. Typically, they provided this information on their Intranet or Internet site. Several agencies list the individual names and contact information for EEO counselors on their web sites. Downloadable fact sheets and brochures, EEO training, and agency guidelines were among the online resources agencies made available. Another issues a quarterly EEO newsletter. Yet another agency reaches its employees at remote locations by providing training on a CD-ROM. By communicating the message of equal employment opportunity in multiple ways, agencies are able to better reinforce their policies against conduct inconsistent with applicable laws.

Issue periodic policy statements or endorsements from the agency head

Ideally, the responsibility for setting the tone for agency compliance with anti-discrimination and whistleblower protection laws starts with the agency's top leader. Senior staff, in turn, take their cue from the agency head about the priorities and goals of the organization. While it is important for agencies to post their policies online, it is extremely valuable for the agency head to demonstrate an active involvement in the prevention of conduct inconsistent with Antidiscrimination and

Whistleblower Protection Laws. Over one-half of the agencies' EEO policies were issued and/or signed by the agency head. Many agencies found issuances by the agency head let everyone know, from senior leadership through all employee ranks, discrimination is not tolerated at the agency. When statements or endorsements come from an agency head and are highly visible, they also help signal everyone will be held accountable.

CONCLUSION

The study has identified a wide range of activities and initiatives by agencies to address conduct inconsistent with Antidiscrimination and Whistleblower Protection Laws. Some are unique to individual agencies and some are employed by a number of agencies. Taken together, the best of these activities and initiatives serve as the basis for advisory guidelines intended under the No FEAR Act of 2002 to help all agencies more efficiently and effectively take appropriate disciplinary actions.

ADVISORY GUIDELINES

The No FEAR Act requires the issuance of advisory guidelines incorporating best practices Federal agencies may follow to take appropriate disciplinary actions against employees for conduct inconsistent with Antidiscrimination and Whistleblower Protection Laws. The Act further requires each agency to provide a written statement to the Speaker of the U.S. House of Representatives; the President Pro Tempore of the U.S. Senate; the Chair, Equal Employment Opportunity Commission (EEOC); and the Attorney General stating the extent to which each agency will follow the guidelines. The specific content of the written statements is prescribed in OPM's regulations at 5 CFR 724.404 and must be submitted within 30 working days of date of this report. This government-wide regulation requires the statements also be provided to OPM. The advisory guidelines for taking disciplinary action are:

1. Ensure each agency's disciplinary policy addresses conduct inconsistent with Antidiscrimination and Whistleblower Protection Laws and the agency's human resources office, EEO office, and legal counsel are involved in future modifications to the policy. The policy should clearly set forth the responsibility of managers and supervisors to take appropriate action, should address the sanctions for this type of misconduct, and accurately reflect current developments in law, including case law.

2. Ensure procedures are in place to promptly inform agency management of potential employee conduct inconsistent with Antidiscrimination and Whistleblower Protection Laws which may be the basis for disciplinary action, including an appropriate mechanism by which the EEO office can report potentially inconsistent conduct to an appropriate agency official.

3. Ensure such conduct, if its occurrence is supported by the facts and evidence, is addressed promptly in a manner that is reasonable, based on the circumstances of the case, and, to the extent feasible, consistent, based on any other similar cases (and the degree of similarity).

4. Ensure supervisors and managers, when taking disciplinary actions, work with the employee relations (ER) office as appropriate, as well as the agency's legal counsel or whatever office is responsible for representing the agency in third-party appeals.

5. Ensure ongoing communications among appropriate agency offices such as ER, EEO, and legal counsel concerning new developments in employee misconduct cases and any systemic problems.

6. Ensure ER staff receives adequate training, mentoring, and supervision in order to communicate accurate and well-reasoned advice to supervisors and managers on taking disciplinary action.

Issued September 30, 2008
U.S. Office of Personnel Management

UNITED STATES
OFFICE OF PERSONNEL MANAGEMENT
1900 E Street, NW
Washington, DC 20415

SHRP/CWRAP/EAG-01

United States Government Accountability Office

GAO

By the Comptroller General of the United States

December 2011

Government Auditing Standards

2011 Revision

GAO-12-331G

United States Government Accountability Office

GAO

By the Comptroller General of the United States

December 2011

Government Auditing Standards

2011 Revision

The 2011 revision of Government Auditing Standards supersedes the 2007 revision. The 2011 revision should be used by government auditors until further updates and revisions are made. An electronic version of this document can be accessed on GAO's Yellow Book Web page at http://www.gao.gov/yellowbook.

The 2011 revision of Government Auditing Standards is effective for financial audits and attestation engagements for periods ending on or after December 15, 2012, and for performance audits beginning on or after December 15, 2011. Early implementation is not permitted.

Revised on January 20, 2012, to correct a typo in paragraph 7.19.

GAO-12-331G

Contents

Abbreviations

AICPA	American Institute of Certified Public Accountants
AU-C	AICPA *Codification of Statements on Auditing Standards for Auditing*
AT	AICPA *Codification of Statements on Standards for Attestation Engagements*
CPA	certified public accountants
CPE	continuing professional education
COSO	Committee of Sponsoring Organizations of the Treadway Commission
ERISA	Employee Retirement Income Security Act
FISCAM	*Federal Information System Controls Audit Manual*
GAAP	generally accepted accounting principles
GAGAS	generally accepted government auditing standards
GAO	Government Accountability Office
IT	information technology
IAASB	International Auditing and Assurance Standards Board
IIA	Institute of Internal Auditors
ISAE	International Standards on Assurance Engagements
ISA	International Standards on Auditing
MD&A	management's discussion and analysis
OMB	Office of Management and Budget
PCAOB	Public Company Accounting Oversight Board
SAS	Statements on Auditing Standards
SSAE	Statements on Standards for Attestation Engagements

Audits provide essential accountability and transparency over government programs. Given the current challenges facing governments and their programs, the oversight provided through auditing is more critical than ever. Government auditing provides objective analysis and information needed to make the decisions necessary to help create a better future. The professional standards presented in this 2011 revision of Government Auditing Standards provide a framework for performing high-quality audit work with competence, integrity, objectivity, and independence to provide accountability and to help improve government operations and services. These standards provide the foundation for government auditors to lead by example in the areas of independence, transparency, accountability, and quality through the audit process.

The 2011 revision of Government Auditing Standards represents a modernized version of the standards, taking into account recent changes in other auditing standards, including international standards. This revision supersedes the 2007 revision. It contains the following major changes from the 2007 revision that reinforce the principles of transparency and accountability and provide the framework for high-quality government audits that add value.

- A conceptual framework for independence was added to provide a means for auditors to assess their independence for activities that are not expressly prohibited in the standards. This more principles-based approach to analyzing independence provides the framework for auditors to assess the unique facts and circumstances that arise during their work.

- This revision drops discussion surrounding certain AICPA Statements on Auditing Standards (SAS) and

Statements on Standards for Attestation Engagements (SSAE) requirements that were incorporated by reference and included in the 2007 revision, as the standards have converged in those areas.

- The definition of validity as an aspect of the quality of evidence has been clarified for performance audits.

Effective with the implementation dates for the 2011 revision of Government Auditing Standards, GAO is also retiring Government Auditing Standards: Answers to Independence Standard Questions (GAO-02-870G, July 2002).

This revision of the standards has gone through an extensive deliberative process, including public comments and input from the Comptroller General's Advisory Council on Government Auditing Standards. The Advisory Council generally consists of about 25 experts in financial and performance auditing and reporting drawn from federal, state, and local government; the private sector; and academia. The views of all parties were thoroughly considered in finalizing the standards.

The 2011 revision of Government Auditing Standards will be effective for financial audits and attestation engagements for periods ending on or after December 15, 2012, and for performance audits beginning on or after December 15, 2011. Early implementation is not permitted.

An electronic version of this document and any interpretive publications can be accessed at http://www.gao.gov/yellowbook.

I extend special thanks to the members of the Advisory Council for their extensive input and feedback through the entire process of developing and finalizing the standards.

Gene L. Dodaro
Comptroller General
of the United States

December 2011

Government Auditing: Foundation and Ethical Principles

Introduction

1.01 The concept of accountability for use of public resources and government authority is key to our nation's governing processes. Management and officials entrusted with public resources are responsible for carrying out public functions and providing service to the public effectively, efficiently, economically, ethically, and equitably within the context of the statutory boundaries of the specific government program.

1.02 As reflected in applicable laws, regulations, agreements, and standards, management and officials of government programs are responsible for providing reliable, useful, and timely information for transparency and accountability of these programs and their operations.[1] Legislators, oversight bodies, those charged with governance,[2] and the public need to know whether (1) management and officials manage government resources and use their authority properly and in compliance with laws and regulations; (2) government programs are achieving their objectives and desired outcomes; and (3) government services are provided effectively, efficiently, economically, ethically, and equitably.

1.03 Government auditing is essential in providing accountability to legislators, oversight bodies, those charged with governance, and the public. Audits[3] provide an independent, objective, nonpartisan assessment of the stewardship, performance, or cost of government policies, programs, or operations, depending upon the type and scope of the audit.

[1]See paragraph A1.08 for additional information on management's responsibilities.

[2]See paragraphs A1.05 through A1.07 for additional discussion on the role of those charged with governance.

[3]See paragraph 1.07c for discussion of the term "audit" as it is used in chapters 1 through 3 and corresponding sections of the Appendix.

Purpose and Applicability of GAGAS

1.04 The professional standards and guidance contained in this document, commonly referred to as generally accepted government auditing standards (GAGAS), provide a framework for conducting high quality audits with competence, integrity, objectivity, and independence. These standards are for use by auditors of government entities and entities that receive government awards and audit organizations performing GAGAS audits. Overall, GAGAS contains standards for audits, which are comprised of individual requirements that are identified by terminology as discussed in paragraphs 2.14 through 2.18. GAGAS contains requirements and guidance dealing with ethics, independence, auditors' professional judgment and competence, quality control, performance of the audit, and reporting.

1.05 Audits performed in accordance with GAGAS provide information used for oversight, accountability, transparency, and improvements of government programs and operations. GAGAS contains requirements and guidance to assist auditors in objectively acquiring and evaluating sufficient, appropriate evidence and reporting the results. When auditors perform their work in this manner and comply with GAGAS in reporting the results, their work can lead to improved government management, better decision making and oversight, effective and efficient operations, and accountability and transparency for resources and results.

1.06 Provisions of laws, regulations, contracts, grant agreements, or policies frequently require audits be conducted in accordance with GAGAS. In addition, many auditors and audit organizations voluntarily choose to perform their work in accordance with GAGAS. The requirements and guidance in GAGAS apply to audits of government entities, programs, activities, and functions, and of government assistance administered by contractors, nonprofit entities, and other nongovernmental entities when the use of GAGAS is required or is voluntarily followed.[4]

1.07 This paragraph describes the use of the following terms in GAGAS.

a. The term "auditor" as it is used throughout GAGAS describes individuals performing work in accordance with GAGAS (including audits and attestation engagements) regardless of job title. Therefore, individuals who may have the titles auditor, analyst, practitioner, evaluator, inspector, or other similar titles are considered auditors in GAGAS.

b. The term "audit organization" as it is used throughout GAGAS refers to government audit organizations as well as public accounting or other firms that perform audits and attestation engagements using GAGAS.

c. The term "audit" as it is used in chapters 1 through 3 and corresponding sections of the Appendix refers to financial audits, attestation engagements, and performance audits conducted in accordance with GAGAS.

[4]See paragraphs A1.02 through A1.04 for discussion of laws, regulations, and guidelines that require use of GAGAS.

1.08 A government audit organization can be structurally located within or outside the audited entity.[5] Audit organizations that are external to the audited entity and report to third parties are considered to be external audit organizations. Audit organizations that are accountable to senior management and those charged with governance of the audited entity, and do not generally issue their reports to third parties external to the audited entity, are considered internal audit organizations.

1.09 Some government audit organizations represent a unique hybrid of external auditing and internal auditing in their oversight role for the entities they audit. These audit organizations have external reporting requirements consistent with the reporting requirements for external auditors while at the same time being part of their respective agencies. These audit organizations often have a dual reporting responsibility to their legislative body as well as to the agency head and management.

Ethical Principles

1.10 The ethical principles presented in this section provide the foundation, discipline, and structure, as well as the climate that influence the application of GAGAS. This section sets forth fundamental principles rather than establishing specific standards or requirements.

1.11 Because auditing is essential to government accountability to the public, the public expects audit organizations and auditors who conduct their work in accordance with GAGAS to follow ethical principles. Management of the audit organization sets the tone for

[5]See paragraph 1.19 for a discussion of objectivity and paragraphs 3.27 through 3.32 for requirements related to independence considerations for government auditors and audit organization structure.

ethical behavior throughout the organization by maintaining an ethical culture, clearly communicating acceptable behavior and expectations to each employee, and creating an environment that reinforces and encourages ethical behavior throughout all levels of the organization. The ethical tone maintained and demonstrated by management and staff is an essential element of a positive ethical environment for the audit organization.

1.12 Conducting audit work in accordance with ethical principles is a matter of personal and organizational responsibility. Ethical principles apply in preserving auditor independence,[6] taking on only work that the audit organization is competent[7] to perform, performing high-quality work, and following the applicable standards cited in the auditors' report. Integrity and objectivity are maintained when auditors perform their work and make decisions that are consistent with the broader interest of those relying on the auditors' report, including the public.

1.13 Other ethical requirements or codes of professional conduct may also be applicable to auditors who conduct audits in accordance with GAGAS. For example, individual auditors who are members of professional organizations or are licensed or certified professionals may also be subject to ethical requirements of those professional organizations or licensing bodies. Auditors employed by government entities may also be subject to government ethics laws and regulations.

[6]See paragraphs 3.02 through 3.59 for requirements related to independence.

[7]See paragraphs 3.69 through 3.81 for additional information on competence.

1.14 The ethical principles that guide the work of auditors who conduct audits in accordance with GAGAS are

a. the public interest;

b. integrity;

c. objectivity;

d. proper use of government information, resources, and positions; and

e. professional behavior.

The Public Interest

1.15 The public interest is defined as the collective well-being of the community of people and entities the auditors serve. Observing integrity, objectivity, and independence in discharging their professional responsibilities assists auditors in meeting the principle of serving the public interest and honoring the public trust. The principle of the public interest is fundamental to the responsibilities of auditors and critical in the government environment.

1.16 A distinguishing mark of an auditor is acceptance of responsibility to serve the public interest. This responsibility is critical when auditing in the government environment. GAGAS embodies the concept of accountability for public resources, which is fundamental to serving the public interest.

Integrity

1.17 Public confidence in government is maintained and strengthened by auditors performing their professional responsibilities with integrity. Integrity includes auditors conducting their work with an attitude that is objective, fact-based, nonpartisan, and nonideological with regard

to audited entities and users of the auditors' reports. Within the constraints of applicable confidentiality laws, rules, or policies, communications with the audited entity, those charged with governance, and the individuals contracting for or requesting the audit are expected to be honest, candid, and constructive.

1.18 Making decisions consistent with the public interest of the program or activity under audit is an important part of the principle of integrity. In discharging their professional responsibilities, auditors may encounter conflicting pressures from management of the audited entity, various levels of government, and other likely users. Auditors may also encounter pressures to inappropriately achieve personal or organizational gain. In resolving those conflicts and pressures, acting with integrity means that auditors place priority on their responsibilities to the public interest.

Objectivity

1.19 The credibility of auditing in the government sector is based on auditors' objectivity in discharging their professional responsibilities. Objectivity includes independence of mind and appearance when providing audits, maintaining an attitude of impartiality, having intellectual honesty, and being free of conflicts of interest. Maintaining objectivity includes a continuing assessment of relationships with audited entities and other stakeholders in the context of the auditors' responsibility to the public. The concepts of objectivity and independence are closely related. Independence impairments impact objectivity.[8]

[8]See independence standards at paragraphs 3.02 through 3.59.

Proper Use of Government Information, Resources, and Positions

1.20 Government information, resources, and positions are to be used for official purposes and not inappropriately for the auditor's personal gain or in a manner contrary to law or detrimental to the legitimate interests of the audited entity or the audit organization. This concept includes the proper handling of sensitive or classified information or resources.

1.21 In the government environment, the public's right to the transparency of government information has to be balanced with the proper use of that information. In addition, many government programs are subject to laws and regulations dealing with the disclosure of information. To accomplish this balance, exercising discretion in the use of information acquired in the course of auditors' duties is an important part in achieving this goal. Improperly disclosing any such information to third parties is not an acceptable practice.

1.22 Accountability to the public for the proper use and prudent management of government resources is an essential part of auditors' responsibilities. Protecting and conserving government resources and using them appropriately for authorized activities is an important element in the public's expectations for auditors.

1.23 Misusing the position of an auditor for financial gain or other benefits violates an auditor's fundamental responsibilities. An auditor's credibility can be damaged by actions that could be perceived by an objective third party with knowledge of the relevant information as improperly benefiting an auditor's personal financial interests or those of an immediate or close family member; a general partner; an organization for which the auditor serves as an officer, director, trustee, or employee; or an organization with which the auditor is negotiating concerning future employment.

Professional Behavior

1.24 High expectations for the auditing profession include compliance with all relevant legal, regulatory, and professional obligations and avoidance of any conduct that might bring discredit to auditors' work, including actions that would cause an objective third party with knowledge of the relevant information to conclude that the auditors' work was professionally deficient. Professional behavior includes auditors putting forth an honest effort in performance of their duties and professional services in accordance with the relevant technical and professional standards.

Standards for Use and Application of GAGAS

Introduction

2.01 This chapter establishes requirements and provides guidance for audits[9] performed in accordance with generally accepted government auditing standards (GAGAS). This chapter also identifies the types of audits that may be performed in accordance with GAGAS, explains the terminology that GAGAS uses to identify requirements, explains the relationship between GAGAS and other professional standards, and provides requirements for stating compliance with GAGAS in the auditors' report.

Types of GAGAS Audits and Attestation Engagements

2.02 This section describes the types of audits that audit organizations may perform in accordance with GAGAS. This description is not intended to limit or require the types of audits that may be performed in accordance with GAGAS.

2.03 All audits begin with objectives, and those objectives determine the type of audit to be performed and the applicable standards to be followed. The types of audits that are covered by GAGAS, as defined by their objectives, are classified in this document as financial audits, attestation engagements, and performance audits.

2.04 In some audits, the standards applicable to the specific objective will be apparent. For example, if the objective is to express an opinion on financial statements, the standards for financial audits apply. However, some audits may have multiple or overlapping objectives. For example, if the objectives are to determine the reliability of performance measures, this work can be done in accordance with either the standards for attestation engagements or performance

[9]See paragraph 1.07c for discussion of the term "audit" as it is used in chapters 1 through 3 and corresponding sections of the Appendix.

audits. In cases in which there is a choice between applicable standards, auditors should evaluate users' needs and the auditors' knowledge, skills, and experience in deciding which standards to follow.

2.05 GAGAS requirements apply to the types of audits that may be performed in accordance with GAGAS as follows:

a. Financial audits: the requirements and guidance in chapters 1 through 4 apply.

b. Attestation engagements: the requirements and guidance in chapters 1 through 3, and 5 apply.

c. Performance audits: the requirements and guidance in chapters 1 through 3, 6, and 7 apply.

2.06 Appendix I includes supplemental guidance for auditors and audited entities to assist in the implementation of GAGAS. Appendix I does not establish auditor requirements but instead is intended to facilitate implementation of the standards contained in chapters 2 through 7. Appendix II includes a flowchart which may assist in the application of the conceptual framework for independence.[10]

Financial Audits

2.07 Financial audits provide an independent assessment of whether an entity's reported financial information (e.g., financial condition, results, and use of resources) are presented fairly in accordance with recognized criteria. Financial audits performed in accordance with GAGAS include financial statement audits and other related financial audits:

[10]See paragraphs 3.07 through 3.32 for discussion of the conceptual framework.

a. Financial statement audits: The primary purpose of a financial statement audit is to provide an opinion about whether an entity's financial statements are presented fairly in all material respects in conformity with an applicable financial reporting framework. Reporting on financial statement audits performed in accordance with GAGAS also includes reports on internal control over financial reporting and on compliance with provisions of laws, regulations, contracts, and grant agreements that have a material effect on the financial statements.

b. Other types of financial audits: Other types of financial audits conducted in accordance with GAGAS entail various scopes of work, including: (1) obtaining sufficient, appropriate evidence to form an opinion on single financial statements, specified elements, accounts, or items of a financial statement;[11] (2) issuing letters for underwriters and certain other requesting parties;[12] and (3) auditing compliance with applicable compliance requirements relating to one or more government programs.[13]

2.08 GAGAS incorporates by reference the American Institute of Certified Public Accountants (AICPA)

[11]See American Institute of Certified Public Accountants (AICPA) *Codification of Statements on Auditing Standards* for Auditing (AU-C) Section 805, *Special Considerations – Audits of Single Financial Statements and Specific Elements, Accounts, or Items of a Financial Statement*.

[12]See AICPA AU-C Section 920, *Letters for Underwriters and Certain Other Requesting Parties.*

[13]See AICPA AU-C Section 935, *Compliance Audits.*

Statements on Auditing Standards (SAS).[14] Additional requirements for performing financial audits in accordance with GAGAS are contained in chapter 4. For financial audits performed in accordance with GAGAS, auditors should also comply with chapters 1 through 3.

Attestation Engagements

2.09 Attestation engagements can cover a broad range of financial or nonfinancial objectives about the subject matter or assertion depending on the users' needs.[15] GAGAS incorporates by reference the AICPA's Statements on Standards for Attestation Engagements (SSAE).[16] Additional requirements for performing attestation engagements in accordance with GAGAS are contained in chapter 5. The AICPA's standards recognize attestation engagements that result in an examination, a review, or an agreed-upon procedures report on a subject matter or on an assertion about a subject matter that is the responsibility of another party.[17] The three types of attestation engagements are:

a. Examination: Consists of obtaining sufficient, appropriate evidence to express an opinion on whether the subject matter is based on (or in conformity with) the

[14]See AICPA *Codification of Statements on Auditing Standards* and paragraph 2.20 for additional discussion on the relationship between GAGAS and other professional standards. References to the AICPA *Codification of Statements on Auditing Standards* use an "AU-C" identifier to refer to the clarified SASs instead of an "AU" identifier. "AU-C" is a temporary identifier to avoid confusion with references to existing "AU" sections, which remain effective through 2013. The "AU-C" identifier will revert to "AU" in 2014 AICPA *Codification of Statements on Auditing Standards*, by which time the clarified SASs become fully effective for all engagements.

[15]See A2.01 for examples of objectives for attestation engagements.

[16]See the AICPA *Codification of Statements on Standards for Attestation Engagements* (AT) Sections.

[17]See AICPA AT Section 101, *Attest Engagements* and AT Section 201, *Agreed-Upon Procedures Engagements*.

criteria in all material respects or the assertion is presented (or fairly stated), in all material respects, based on the criteria.

b. Review: Consists of sufficient testing to express a conclusion about whether any information came to the auditors' attention on the basis of the work performed that indicates the subject matter is not based on (or not in conformity with) the criteria or the assertion is not presented (or not fairly stated) in all material respects based on the criteria. Auditors should not perform review-level work for reporting on internal control or compliance with provisions of laws and regulations.[18]

c. Agreed-Upon Procedures: Consists of auditors performing specific procedures on the subject matter and issuing a report of findings based on the agreed-upon procedures. In an agreed-upon procedures engagement, the auditor does not express an opinion or conclusion, but only reports on agreed-upon procedures in the form of procedures and findings related to the specific procedures applied.

Performance Audits

2.10 Performance audits are defined as audits that provide findings or conclusions based on an evaluation of sufficient, appropriate evidence against criteria.[19] Performance audits provide objective analysis to assist management and those charged with governance and oversight in using the information to improve program performance and operations, reduce costs, facilitate decision making by parties with responsibility to oversee or initiate corrective action, and contribute to public accountability. The term "program" is used in

[18]See AICPA AT Sections 501, *Reporting on an Entity's Internal Control Over Financial Reporting* and 601, *Compliance Attestation.*

[19]See paragraphs 6.37 and A6.02 for discussion of criteria.

GAGAS to include government entities, organizations, programs, activities, and functions.

2.11 Performance audit objectives vary widely and include assessments of program effectiveness, economy, and efficiency; internal control; compliance; and prospective analyses. These overall objectives are not mutually exclusive. Thus, a performance audit may have more than one overall objective. For example, a performance audit with an objective of determining or evaluating program effectiveness may also involve an additional objective of evaluating internal controls to determine the reasons for a program's lack of effectiveness or how effectiveness can be improved. Examples of the various types of the performance audit objectives discussed below are included in Appendix I.[20]

a. Program effectiveness and results audit objectives are frequently interrelated with economy and efficiency objectives. Audit objectives that focus on program effectiveness and results typically measure the extent to which a program is achieving its goals and objectives. Audit objectives that focus on economy and efficiency address the costs and resources used to achieve program results.

b. Internal control audit objectives relate to an assessment of one or more components of an organization's system of internal control that is designed to provide reasonable assurance of achieving effective and efficient operations, reliable financial and performance reporting, or compliance with applicable laws and regulations. Internal control objectives also may be relevant when determining the cause of unsatisfactory program performance. Internal control

[20]See paragraphs A2.02 through A2.05 for discussion of performance audit objectives.

comprises the plans, policies, methods, and procedures used to meet the organization's mission, goals, and objectives. Internal control includes the processes and procedures for planning, organizing, directing, and controlling program operations, and management's system for measuring, reporting, and monitoring program performance.[21]

c. Compliance audit objectives relate to an assessment of compliance with criteria established by provisions of laws, regulations, contracts, or grant agreements, or other requirements that could affect the acquisition, protection, use, and disposition of the entity's resources and the quantity, quality, timeliness, and cost of services the entity produces and delivers. Compliance requirements can be either financial or nonfinancial.

d. Prospective analysis audit objectives provide analysis or conclusions about information that is based on assumptions about events that may occur in the future, along with possible actions that the entity may take in response to the future events.

Nonaudit Services Provided by Audit Organizations

2.12 GAGAS does not cover nonaudit services, which are defined as professional services other than audits or attestation engagements. Therefore, auditors do not report that the nonaudit services were conducted in accordance with GAGAS. When performing nonaudit services for an entity for which the audit organization performs a GAGAS audit, audit organizations should communicate with requestors and those charged with governance to clarify that the work performed does not constitute an audit conducted in accordance with GAGAS.

[21]See paragraphs A.03 through A.04 for additional discussion of internal control.

2.13 When audit organizations provide nonaudit services to entities for which they also provide GAGAS audits, they should assess the impact that providing those nonaudit services may have on auditor and audit organization independence and respond to any identified threats to independence in accordance with the GAGAS independence standard.[22]

Use of Terminology to Define GAGAS Requirements

2.14 GAGAS contains requirements together with related guidance in the form of application and other explanatory material. The terminology is consistent with the terminology defined in the AICPA's *Codification of Statements on Auditing Standards*.[23] Auditors have a responsibility to consider the entire text of GAGAS in carrying out their work and in understanding and applying the requirements in GAGAS. Not every paragraph of GAGAS carries a requirement that auditors and audit organizations are expected to fulfill. Rather, the requirements are identified through use of specific language.

2.15 GAGAS uses two categories of requirements, identified by specific terms, to describe the degree of responsibility they impose on auditors and audit organizations, as follows:

a. Unconditional requirements: Auditors and audit organizations must comply with an unconditional requirement in all cases where such requirement is relevant. GAGAS uses the word *must* to indicate an unconditional requirement.

[22]See paragraphs 3.02 through 3.59 for the GAGAS independence standard.

[23]See AICPA AU-C Section 200, *Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance With Generally Accepted Auditing Standards*.

b. Presumptively mandatory requirements: Auditors and audit organizations must comply with a presumptively mandatory requirement in all cases where such a requirement is relevant except in rare circumstances discussed in paragraph 2.16. GAGAS uses the word *should* to indicate a presumptively mandatory requirement.[24]

2.16 In rare circumstances, auditors and audit organizations may determine it necessary to depart from a relevant presumptively mandatory requirement. In such rare circumstances, auditors should perform alternative procedures to achieve the intent of that requirement. The need for the auditors to depart from a relevant presumptively mandatory requirement is expected to arise only when the requirement is for a specific procedure to be performed and, in the specific circumstances of the audit, that procedure would be ineffective in achieving the intent of the requirement. If, in rare circumstances, auditors judge it necessary to depart from a relevant presumptively mandatory requirement, they must document their justification for the departure and how the alternative procedures performed in the circumstances were sufficient to achieve the intent of that requirement.

2.17 In addition to requirements as identified in paragraph 2.15, GAGAS contains related guidance in the form of application and other explanatory material. The application and other explanatory material provides further explanation of the requirements and guidance for carrying them out. In particular, it may explain more precisely what a requirement means or is intended to cover or include examples of procedures that may be appropriate in the circumstances. Although such guidance does not in itself impose a requirement, it is

[24]See paragraph 2.25 for additional documentation requirements for departures from GAGAS requirements.

relevant to the proper application of the requirements. Auditors should have an understanding of the application and other explanatory material; how auditors apply the guidance in the audit depends on the exercise of professional judgment in the circumstances consistent with the objective of the requirement. The words "may," "might," and "could" are used to describe these actions and procedures. The application and other explanatory material may also provide background information on matters addressed in GAGAS.

2.18 Auditors also use "interpretive publications" in planning and performing GAGAS audits. Interpretive publications are recommendations on the application of GAGAS in specific circumstances, including audits for entities in specialized industries. Interpretive publications, such as related GAGAS guidance documents and interpretations, are issued under the authority of the Government Accountability Office (GAO) to provide additional guidance on the application of GAGAS.[25] Interpretive publications are not auditing standards, but have the same level of authority as application and other explanatory material in GAGAS.

Relationship between GAGAS and Other Professional Standards

2.19 Auditors may use GAGAS in conjunction with professional standards issued by other authoritative bodies.

2.20 The relationship between GAGAS and other professional standards for financial audits and attestation engagements is as follows:

[25]See http://www.gao.gov/yellowbook for a listing of related GAGAS interpretive publications.

a. The AICPA has established professional standards that apply to financial audits and attestation engagements for nonissuers (entities other than issuers[26] under the Sarbanes-Oxley Act of 2002, such as privately held companies, nonprofit entities, and government entities) performed by certified public accountants (CPA). For financial audits and attestation engagements, GAGAS incorporates by reference AICPA standards, as discussed in paragraph 2.08.

b. The International Auditing and Assurance Standards Board (IAASB) has established professional standards that apply to financial audits and assurance engagements. Auditors may elect to use the IAASB standards and the related International Standards on Auditing (ISA) and International Standards on Assurance Engagements (ISAE) in conjunction with GAGAS.

c. The Public Company Accounting Oversight Board (PCAOB) has established professional standards that apply to financial audits and attestation engagements for issuers (generally, publicly traded companies with a reporting obligation under the Securities Exchange Act of 1934). Auditors may elect to use the PCAOB standards in conjunction with GAGAS.

2.21 For performance audits, GAGAS does not incorporate other standards by reference, but recognizes that auditors may use or may be required to use other professional standards in conjunction with GAGAS, such as the following:

[26]See the Sarbanes-Oxley Act of 2002 (Public Law 107-204) for discussion of issuers.

a. *International Standards for the Professional Practice of Internal Auditing*, The Institute of Internal Auditors, Inc.;

b. *Guiding Principles for Evaluators*, American Evaluation Association;

c. *The Program Evaluation Standards*, Joint Committee on Standards for Education Evaluation;

d. *Standards for Educational and Psychological Testing*, American Psychological Association; and

e. *IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals*, ISACA.

2.22 When auditors cite compliance with both GAGAS and another set of standards, such as those listed in paragraphs 2.20 and 2.21, auditors should refer to paragraph 2.24 for the requirements for citing compliance with GAGAS. In addition to citing GAGAS, auditors may also cite the use of other standards in their reports when they have also met the requirements for citing compliance with the other standards.[27] Auditors should refer to the other set of standards for the basis for citing compliance with those standards.

Stating Compliance with GAGAS in the Auditors' Report

2.23 When auditors are required to perform an audit in accordance with GAGAS or are representing to others that they did so, they should cite compliance with GAGAS in the auditors' report as set forth in paragraphs 2.24 through 2.25.

[27]See paragraphs 4.18, 5.19, 5.51, and 5.61 for additional requirements for citing compliance with standards of the AICPA.

2.24 Auditors should include one of the following types of GAGAS compliance statements in reports on GAGAS audits, as appropriate.[28]

a. Unmodified GAGAS compliance statement: Stating that the auditor performed the audit in accordance with GAGAS. Auditors should include an unmodified GAGAS compliance statement in the auditors' report when they have (1) followed unconditional and applicable presumptively mandatory GAGAS requirements, or (2) have followed unconditional requirements, and documented justification for any departures from applicable presumptively mandatory requirements and have achieved the objectives of those requirements through other means.

b. Modified GAGAS compliance statement: Stating either that (1) the auditor performed the audit in accordance with GAGAS, except for specific applicable requirements that were not followed, or (2) because of the significance of the departure(s) from the requirements, the auditor was unable to and did not perform the audit in accordance with GAGAS. Situations when auditors use modified compliance statements also include scope limitations, such as restrictions on access to records, government officials, or other individuals needed to conduct the audit. When auditors use a modified GAGAS statement, they should disclose in the report the applicable requirement(s) not followed, the reasons for not following the requirement(s), and how not following the requirement(s) affected, or could have affected, the audit and the assurance provided.

[28]See paragraph A2.06 for additional discussion of GAGAS compliance statements.

2.25 When auditors do not comply with applicable requirement(s), they should (1) assess the significance of the noncompliance to the audit objectives, (2) document the assessment, along with their reasons for not following the requirement(s), and (3) determine the type of GAGAS compliance statement. The auditors' determination is a matter of professional judgment, which is affected by the significance of the requirement(s) not followed in relation to the audit objectives.

General Standards

Introduction

3.01 This chapter establishes general standards and provides guidance for performing financial audits, attestation engagements, and performance audits under generally accepted government auditing standards (GAGAS). These general standards, along with the overarching ethical principles presented in chapter 1, establish a foundation for the credibility of auditors' work. These general standards emphasize the importance of the independence of the audit organization and its individual auditors; the exercise of professional judgment in the performance of work and the preparation of related reports; the competence of staff; and quality control and assurance.

Independence

3.02 In all matters relating to the audit work, the audit organization and the individual auditor, whether government or public, must be independent.

3.03 Independence comprises:

a. Independence of Mind
The state of mind that permits the performance of an audit without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism.

b. Independence in Appearance
The absence of circumstances that would cause a reasonable and informed third party, having knowledge of the relevant information, to reasonably conclude that the integrity, objectivity, or professional skepticism of an audit organization or member of the audit team had been compromised.

3.04 Auditors and audit organizations maintain independence so that their opinions, findings,

conclusions, judgments, and recommendations will be impartial and viewed as impartial by reasonable and informed third parties. Auditors should avoid situations that could lead reasonable and informed third parties to conclude that the auditors are not independent and thus are not capable of exercising objective and impartial judgment on all issues associated with conducting the audit and reporting on the work.

3.05 Except under the limited circumstances discussed in paragraphs 3.47 and 3.48, auditors should be independent from an audited entity during:

a. any period of time that falls within the period covered by the financial statements or subject matter of the audit, and

b. the period of the professional engagement, which begins when the auditors either sign an initial engagement letter or other agreement to perform an audit or begin to perform an audit, whichever is earlier. The period lasts for the entire duration of the professional relationship (which, for recurring audits, could cover many periods) and ends with the formal or informal notification, either by the auditors or the audited entity, of the termination of the professional relationship or by the issuance of a report, whichever is later. Accordingly, the period of professional engagement does not necessarily end with the issuance of a report and recommence with the beginning of the following year's audit or a subsequent audit with a similar objective.

3.06 GAGAS's practical consideration of independence consists of four interrelated sections, providing:

a. a conceptual framework for making independence determinations based on facts and circumstances that are often unique to specific environments;

b. requirements for and guidance on independence for audit organizations that are structurally located within the entities they audit;

c. requirements for and guidance on independence for auditors performing nonaudit services, including indication of specific nonaudit services that always impair independence and others that would not normally impair independence; and

d. requirements for and guidance on documentation necessary to support adequate consideration of auditor independence.

GAGAS Conceptual Framework Approach to Independence

3.07 Many different circumstances, or combinations of circumstances, are relevant in evaluating threats to independence. Therefore, GAGAS establishes a conceptual framework that auditors use to identify, evaluate, and apply safeguards to address threats to independence.[29] The conceptual framework assists auditors in maintaining both independence of mind and independence in appearance. It can be applied to many variations in circumstances that create threats to independence and allows auditors to address threats to independence that result from activities that are not specifically prohibited by GAGAS.

3.08 Auditors should apply the conceptual framework at the audit organization, audit, and individual auditor levels to:

a. identify threats to independence;

[29]See Appendix II for a flowchart to assist in the application of the conceptual framework for independence.

b. evaluate the significance of the threats identified, both individually and in the aggregate; and

c. apply safeguards as necessary to eliminate the threats or reduce them to an acceptable level.

3.09 If no safeguards are available to eliminate an unacceptable threat or reduce it to an acceptable level, independence would be considered impaired.

3.10 The use of the term “audit organization” in GAGAS is described in paragraph 1.07. For consideration of auditor independence, offices or units of an audit organization, or related or affiliated entities under common control, are not differentiated from one another. Consequently, for the purposes of independence evaluation using the conceptual framework, an audit organization that includes multiple offices or units, or includes multiple entities related or affiliated through common control, is considered to be one audit organization. Common ownership may also affect independence in appearance regardless of the level of control.

3.11 The GAGAS section on nonaudit services in paragraphs 3.33 through 3.58 provides requirements and guidance on evaluating threats to independence related to nonaudit services provided by auditors to audited entities. That section also enumerates specific nonaudit services that always impair auditor independence with respect to audited entities and that auditors are prohibited from providing to audited entities.

3.12 The following sections discuss threats to independence, safeguards or controls to eliminate or reduce threats, and application of the conceptual framework for independence.

Threats

3.13 Threats to independence are circumstances that could impair independence. Whether independence is impaired depends on the nature of the threat, whether the threat is of such significance that it would compromise an auditor's professional judgment or create the appearance that the auditor's professional judgment may be compromised, and on the specific safeguards applied to eliminate the threat or reduce it to an acceptable level. Threats are conditions to be evaluated using the conceptual framework. Threats do not necessarily impair independence.

3.14 Threats to independence may be created by a wide range of relationships and circumstances. Auditors should evaluate the following broad categories of threats to independence when threats are being identified and evaluated:[30]

a. Self-interest threat - the threat that a financial or other interest will inappropriately influence an auditor's judgment or behavior;

b. Self-review threat - the threat that an auditor or audit organization that has provided nonaudit services will not appropriately evaluate the results of previous judgments made or services performed as part of the nonaudit services when forming a judgment significant to an audit;

c. Bias threat - the threat that an auditor will, as a result of political, ideological, social, or other convictions, take a position that is not objective;

d. Familiarity threat - the threat that aspects of a relationship with management or personnel of an

[30]See A3.02 through A3.09 for further discussion and examples of threats.

audited entity, such as a close or long relationship, or that of an immediate or close family member, will lead an auditor to take a position that is not objective;

e. Undue influence threat - the threat that external influences or pressures will impact an auditor's ability to make independent and objective judgments;

f. Management participation threat - the threat that results from an auditor's taking on the role of management or otherwise performing management functions on behalf of the entity undergoing an audit; and

g. Structural threat - the threat that an audit organization's placement within a government entity, in combination with the structure of the government entity being audited, will impact the audit organization's ability to perform work and report results objectively.

3.15 Circumstances that result in a threat to independence in one of the above categories may result in other threats as well. For example, a circumstance resulting in a structural threat to independence may also expose auditors to undue influence and management participation threats.

Safeguards

3.16 Safeguards are controls designed to eliminate or reduce to an acceptable level threats to independence. Under the conceptual framework, the auditor applies safeguards that address the specific facts and circumstances under which threats to independence exist. In some cases, multiple safeguards may be necessary to address a threat. The list of safeguards in this section provides examples that may be effective under certain circumstances. The list cannot provide safeguards for all circumstances. It may, however, provide a starting point for auditors who have identified threats to independence and are considering what

safeguards could eliminate those threats or reduce them to an acceptable level.

3.17 Examples of safeguards include:

a. consulting an independent third party, such as a professional organization, a professional regulatory body, or another auditor;

b. involving another audit organization to perform or reperform part of the audit;

c. having a professional staff member who was not a member of the audit team review the work performed; and

d. removing an individual from an audit team when that individual's financial or other interests or relationships pose a threat to independence.

3.18 Depending on the nature of the audit, an auditor may also be able to place limited reliance on safeguards that the entity has implemented. It is not possible to rely solely on such safeguards to eliminate threats or reduce them to an acceptable level.

3.19 Examples of safeguards within the entity's systems and procedures include:

a. an entity requirement that persons other than management ratify or approve the appointment of an audit organization to perform an audit;

b. internal procedures at the entity that ensure objective choices in commissioning nonaudit services; and

c. a governance structure at the entity that provides appropriate oversight and communications regarding the audit organization's services.

Application of the Conceptual Framework

3.20 Auditors should evaluate threats to independence using the conceptual framework when the facts and circumstances under which the auditors perform their work may create or augment threats to independence. Auditors should evaluate threats both individually and in the aggregate because threats can have a cumulative effect on an auditor's independence.

3.21 Facts and circumstances that create threats to independence can result from events such as the start of a new audit; assignment of new staff to an ongoing audit; and acceptance of a nonaudit service at an audited entity. Many other events can result in threats to independence. Auditors use professional judgment to determine whether the facts and circumstances created by an event warrant use of the conceptual framework. Whenever relevant new information about a threat to independence comes to the attention of the auditor during the audit, the auditor should evaluate the significance of the threat in accordance with the conceptual framework.

3.22 Auditors should determine whether identified threats to independence are at an acceptable level or have been eliminated or reduced to an acceptable level. A threat to independence is not acceptable if it either (a) could impact the auditor's ability to perform an audit without being affected by influences that compromise professional judgment or (b) could expose the auditor or audit organization to circumstances that would cause a reasonable and informed third party to conclude that the integrity, objectivity, or professional skepticism of the audit organization, or a member of the audit team, had been compromised.

3.23 When an auditor identifies threats to independence and, based on an evaluation of those threats, determines that they are not at an acceptable level, the auditor should determine whether appropriate

safeguards are available and can be applied to eliminate the threats or reduce them to an acceptable level. The auditor should exercise professional judgment in making that determination, and should take into account whether both independence of mind and independence in appearance are maintained. The auditor should evaluate both qualitative and quantitative factors when determining the significance of a threat.

3.24 In cases where threats to independence are not at an acceptable level, thereby requiring the application of safeguards, the auditors should document the threats identified and the safeguards applied to eliminate the threats or reduce them to an acceptable level.

3.25 Certain conditions may lead to threats that are so significant that they cannot be eliminated or reduced to an acceptable level through the application of safeguards, resulting in impaired independence. Under such conditions, auditors should decline to perform a prospective audit or terminate an audit in progress.[31]

3.26 If a threat to independence is initially identified after the auditors' report is issued, the auditor should evaluate the threat's impact on the audit and on GAGAS compliance. If the auditors determine that the newly identified threat had an impact on the audit that would have resulted in the auditors' report being different from the report issued had the auditors been aware of it, they should communicate in the same manner as that used to originally distribute the report to those charged with governance, the appropriate officials of the audited entity, the appropriate officials of the

[31]See paragraph 3.44 for a discussion of conditions under which an auditor may be required by law or regulation to perform both an audit and a nonaudit service and cannot decline to perform or terminate the service. See the discussion of nonaudit services beginning in paragraph 3.45 for consideration of threats related to nonaudit services that cannot be eliminated or reduced to an appropriate level.

organizations requiring or arranging for the audits, and other known users, so that they do not continue to rely on findings or conclusions that were impacted by the threat to independence. If the report was previously posted to the auditors' publicly accessible website, the auditors should remove the report and post a public notification that the report was removed. The auditors should then determine whether to conduct additional audit work necessary to reissue the report, including any revised findings or conclusions or repost the original report if the additional audit work does not result in a change in findings or conclusions.

Government Auditors and Audit Organization Structure

3.27 The ability of audit organizations in government entities to perform work and report the results objectively can be affected by placement within government and the structure of the government entity being audited. The independence standard applies to auditors in government entities whether they report to third parties externally (external auditors), to senior management within the audited entity (internal auditors), or to both.

External Auditor Independence

3.28 Audit organizations that are structurally located within government entities are often subject to constitutional or statutory safeguards that mitigate the effects of structural threats to independence. For external audit organizations, such safeguards may include governmental structures under which a government audit organization is:

a. at a level of government other than the one of which the audited entity is part (federal, state, or local); for example, federal auditors auditing a state government program; or

b. placed within a different branch of government from that of the audited entity; for example, legislative auditors auditing an executive branch program.

3.29 Safeguards other than those described above may mitigate threats resulting from governmental structures. For external auditors or auditors who report both externally and internally, structural threats may be mitigated if the head of an audit organization meets any of the following criteria in accordance with constitutional or statutory requirements:

a. directly elected by voters of the jurisdiction being audited;

b. elected or appointed by a legislative body, subject to removal by a legislative body, and reports the results of audits to and is accountable to a legislative body;

c. appointed by someone other than a legislative body, so long as the appointment is confirmed by a legislative body and removal from the position is subject to oversight or approval by a legislative body, and reports the results of audits to and is accountable to a legislative body; or

d. appointed by, accountable to, reports to, and can only be removed by a statutorily created governing body, the majority of whose members are independently elected or appointed and are outside the organization being audited.

3.30 In addition to the criteria in paragraphs 3.28 and 3.29, GAGAS recognizes that there may be other organizational structures under which external audit organizations in government entities could be considered to be independent. If appropriately designed and implemented, these structures provide safeguards that prevent the audited entity from interfering with the

audit organization's ability to perform the work and report the results impartially. For an external audit organization or one that reports both externally and internally to be considered independent under a structure different from the ones listed in paragraphs 3.28 and 3.29, the audit organization should have all of the following safeguards. In such situations, the audit organization should document how each of the following safeguards was satisfied and provide the documentation to those performing quality control monitoring and to the external peer reviewers to determine whether all the necessary safeguards are in place. The following safeguards may also be used to augment those listed in paragraphs 3.28 and 3.29:

a. statutory protections that prevent the audited entity from abolishing the audit organization;

b. statutory protections that require that if the head of the audit organization is removed from office, the head of the agency reports this fact and the reasons for the removal to the legislative body;

c. statutory protections that prevent the audited entity from interfering with the initiation, scope, timing, and completion of any audit;

d. statutory protections that prevent the audited entity from interfering with audit reporting, including the findings and conclusions or the manner, means, or timing of the audit organization's reports;

e. statutory protections that require the audit organization to report to a legislative body or other independent governing body on a recurring basis;

f. statutory protections that give the audit organization sole authority over the selection, retention, advancement, and dismissal of its staff; and

g. statutory access to records and documents related to the agency, program, or function being audited and access to government officials or other individuals as needed to conduct the audit.

Internal Auditor Independence

3.31 Certain entities employ auditors to work for entity management. These auditors may be subject to administrative direction from persons involved in the entity management process. Such audit organizations are internal audit functions and are encouraged to use the Institute of Internal Auditors (IIA) *International Standards for the Professional Practice of Internal Auditing* in conjunction with GAGAS. In accordance with GAGAS, internal auditors who work under the direction of the audited entity's management are considered independent for the purposes of reporting internally if the head of the audit organization meets all of the following criteria:

a. is accountable to the head or deputy head of the government entity or to those charged with governance;

b. reports the audit results both to the head or deputy head of the government entity and to those charged with governance;

c. is located organizationally outside the staff or line-management function of the unit under audit;

d. has access to those charged with governance; and

e. is sufficiently removed from political pressures to conduct audits and report findings, opinions, and conclusions objectively without fear of political reprisal.

3.32 When internal audit organizations perform audits of external parties such as auditing contractors or outside party agreements, and no impairments to independence exist, the audit organization can be

considered independent as an external audit organization of those external parties.

Provision of Nonaudit Services to Audited Entities

3.33 Auditors have traditionally provided a range of nonaudit services that are consistent with their skills and expertise to entities at which they perform audits. Providing such nonaudit services may create threats to an auditor's independence.

Requirements for Performing Nonaudit Services

3.34 Before an auditor agrees to provide a nonaudit service to an audited entity, the auditor should determine whether providing such a service would create a threat to independence, either by itself or in aggregate with other nonaudit services provided, with respect to any GAGAS audit it performs. A critical component of this determination is consideration of management's ability to effectively oversee the nonaudit service to be performed. The auditor should determine that the audited entity has designated an individual who possesses suitable skill, knowledge, or experience, and that the individual understands the services to be performed sufficiently to oversee them. The individual is not required to possess the expertise to perform or reperform the services. The auditor should document consideration of management's ability to effectively oversee nonaudit services to be performed.

3.35 If an auditor were to assume management responsibilities for an audited entity, the management participation threats created would be so significant that no safeguards could reduce them to an acceptable level. Management responsibilities involve leading and directing an entity, including making decisions regarding the acquisition, deployment and control of human, financial, physical, and intangible resources.

3.36 Whether an activity is a management responsibility depends on the facts and circumstances and auditors

exercise professional judgment in identifying these activities. Examples of activities that are considered management responsibilities and would therefore impair independence if performed for an audited entity include:

a. setting policies and strategic direction for the audited entity;

b. directing and accepting responsibility for the actions of the audited entity's employees in the performance of their routine, recurring activities;

c. having custody of an audited entity's assets;

d. reporting to those charged with governance on behalf of management;

e. deciding which of the auditor's or outside third party's recommendations to implement;

f. accepting responsibility for the management of an audited entity's project;

g. accepting responsibility for designing, implementing, or maintaining internal control;

h. providing services that are intended to be used as management's primary basis for making decisions that are significant to the subject matter of the audit;

i. developing an audited entity's performance measurement system when that system is material or significant to the subject matter of the audit; and

j. serving as a voting member of an audited entity's management committee or board of directors.

3.37 Auditors performing nonaudit services for entities for which they perform audits should obtain assurance that audited entity management performs the following functions in connection with the nonaudit services:

a. assumes all management responsibilities;

b. oversees the services, by designating an individual, preferably within senior management, who possess suitable skill, knowledge, or experience;[32]

c. evaluates the adequacy and results of the services performed; and

d. accepts responsibility for the results of the services.

3.38 In cases where the audited entity is unable or unwilling to assume these responsibilities (for example, the audited entity does not have an individual with suitable skill, knowledge, or experience to oversee the nonaudit services provided, or is unwilling to perform such functions due to lack of time or desire), the auditor's provision of these services would impair independence.

3.39 In connection with nonaudit services, auditors should establish and document their understanding with the audited entity's management or those charged with governance, as appropriate, regarding the following:

a. objectives of the nonaudit service;

b. services to be performed;

c. audited entity's acceptance of its responsibilities;

[32]See paragraph 3.34 for additional discussion of management's ability to effectively oversee the nonaudit service.

d. the auditor's responsibilities; and

e. any limitations of the nonaudit service.

3.40 Routine activities performed by auditors that relate directly to the performance of an audit, such as providing advice and responding to questions as part of an audit, are not considered nonaudit services under GAGAS. Such routine activities generally involve providing advice or assistance to the entity on an informal basis as part of an audit. Routine activities typically are insignificant in terms of time incurred or resources expended and generally do not result in a specific project or engagement or in the auditors producing a formal report or other formal work product. However, activities such as financial statement preparation, cash to accrual conversions, and reconciliations are considered nonaudit services under GAGAS, not routine activities related to the performance of an audit, and are evaluated using the conceptual framework as discussed in paragraph 3.46.

3.41 Routine activities directly related to an audit include the following:

a. providing advice to the audited entity on an accounting matter as an ancillary part of the overall financial audit;

b. researching and responding to the audited entity's technical questions on relevant tax laws as an ancillary part of providing tax services;

c. providing advice to the audited entity on routine business matters;

d. educating the audited entity on matters within the technical expertise of the auditors; and

e. providing information to the audited entity that is readily available to the auditors, such as best practices and benchmarking studies.

3.42 An auditor who previously performed nonaudit services for an entity that is a prospective subject of an audit should evaluate the impact of those nonaudit services on independence before accepting an audit. If the nonaudit services were performed in the period to be covered by the audit, the auditor should (1) determine if the nonaudit service is expressly prohibited by GAGAS and, if not, (2) determine whether a threat to independence exists and address any threats noted in accordance with the conceptual framework.

3.43 Nonaudit services provided by auditors can impact independence of mind and in appearance in periods subsequent to the period in which the nonaudit service was provided. For example, if auditors have designed and implemented an accounting and financial reporting system that is expected to be in place for many years, a threat to independence in appearance for future financial audits or attestation engagements performed by those auditors may exist in subsequent periods. For recurring audits, having another independent audit organization perform an audit of the areas affected by the nonaudit service may provide a safeguard that allows the audit organization that provided the nonaudit service to mitigate the threat to its independence. Auditors use professional judgment to determine whether the safeguards adequately mitigate the threats.

3.44 An auditor in a government entity may be required to perform a nonaudit service that could impair the auditor's independence with respect to a required audit. If the auditor cannot, as a consequence of constitutional or statutory requirements over which the auditor has no control, implement safeguards to reduce the resulting

threat to an acceptable level, or decline to perform or terminate a nonaudit service that is incompatible with audit responsibilities, the auditor should disclose the nature of the threat that could not be eliminated or reduced to an acceptable level and modify the GAGAS compliance statement accordingly.[33]

Consideration of Specific Nonaudit Services

3.45 By their nature, certain nonaudit services directly support the entity's operations and impair auditors' ability to maintain independence in mind and appearance. The nonaudit services discussed below are among those frequently requested of auditors working in a government environment. Some aspects of these services will impair an auditor's ability to perform audits for the entities for which the services are provided. The specific services indicated are not the only nonaudit services that would impair an auditor's independence.

3.46 Auditors may be able to provide nonaudit services in the broad areas indicated in paragraphs 3.49 through 3.58 without impairing independence if (1) the nonaudit services are not expressly prohibited, (2) the auditor has determined that the requirements for performing nonaudit services in paragraphs 3.34 through 3.44 have been met, and (3) any significant threats to independence have been eliminated or reduced to an acceptable level through the application of safeguards. Auditors should use the conceptual framework to evaluate independence given the facts and circumstances of individual services not specifically prohibited in this section.

3.47 For performance audits and agreed-upon procedures engagements, nonaudit services that are

[33]See paragraphs 2.24 and 2.25 for the discussion of modifications to the GAGAS compliance statement.

otherwise prohibited by GAGAS may be provided when such services do not relate to the specific subject matter of the engagement.

3.48 For financial statement audits and examination or review engagements, a nonaudit service performed during the period covered by the financial statements may not impair an auditor's independence with respect to those financial statements provided that the following conditions exist:

a. the nonaudit service was provided prior to the period of professional engagement;

b. the nonaudit service related only to periods prior to the period covered by the financial statements; and

c. the financial statements for the period to which the nonaudit service did relate were audited by another auditor (or in the case of an examination or review engagement, examined, reviewed, or audited by another auditor as appropriate).

Management Responsibilities

3.49 If performed on behalf of an audited entity by the entity's auditor, management responsibilities such as those listed in paragraph 3.36 would create management participation threats so significant that no safeguards could reduce them to an acceptable level. Consequently the auditor's independence would be impaired with respect to that entity.

Preparing Accounting Records and Financial Statements

3.50 Some services involving preparation of accounting records always impair an auditor's independence with respect to an audited entity. These services include:

a. determining or changing journal entries, account codes or classifications for transactions, or other accounting records for the entity without obtaining management's approval;

b. authorizing or approving the entity's transactions; and

c. preparing or making changes to source documents without management approval. Source documents include those providing evidence that transactions have occurred (for example, purchase orders, payroll time records, customer orders, and contracts). Such records also include an audited entity's general ledger and subsidiary records or equivalent.

3.51 Management is responsible for the preparation and fair presentation of the financial statements in accordance with the applicable financial reporting framework, even if the auditor assisted in drafting those financial statements. Consequently, an auditor's acceptance of responsibility for the preparation and fair presentation of financial statements that the auditor will subsequently audit would impair the auditor's independence.

3.52 Services related to preparing accounting records and financial statements that an auditor may be able to provide to an audited entity if the conditions in paragraph 3.46 are met include:

a. recording transactions for which management has determined or approved the appropriate account classification, or posting coded transactions to an audited entity's general ledger;

b. preparing financial statements based on information in the trial balance;

c. posting entries that have been approved by an audited entity's management to the entity's trial balance;

d. preparing account reconciliations that identify reconciling items for the audited entity management's evaluation; and

e. proposing standard, adjusting, or correcting journal entries or other changes affecting the financial statements to an audited entity's management provided management reviews and accepts the entries and the auditor is satisfied that management understands the nature of the proposed entries and the impact the entries have on the financial statements.

Internal Audit Assistance Services Provided by External Auditors

3.53 Internal audit assistance services involve assisting an entity in the performance of its internal audit activities. Certain internal audit assistance activities always impair an external auditor's independence with respect to an audited entity. These activities include:

a. setting internal audit policies or the strategic direction of internal audit activities;

b. performing procedures that form part of the internal control, such as reviewing and approving changes to employee data access privileges; and

c. determining the scope of the internal audit function and resulting work.

Internal Control Monitoring as a Nonaudit Service

3.54 Accepting responsibility for designing, implementing or maintaining internal control includes accepting responsibility for designing, implementing, or maintaining monitoring procedures.[34] Monitoring involves the use of either ongoing monitoring procedures or separate evaluations to gather and analyze persuasive information supporting conclusions about the effectiveness of the internal control system.

[34]See A.03 and A.04 for a discussion of internal control.

Ongoing monitoring procedures performed on behalf of management are built into the routine, recurring operating activities of an organization. Therefore, the management participation threat created if an auditor performs or supervises ongoing monitoring procedures is so significant that no safeguards could reduce the threat to an acceptable level.

3.55 Separate evaluations are sometimes performed as nonaudit services by individuals who are not directly involved in the operation of the controls being monitored. As such, it is possible for an auditor to provide an objective analysis of control effectiveness by performing separate evaluations without creating a management participation threat that would impair independence. However, in all such cases, the significance of the threat created by performing separate evaluations should be evaluated and safeguards applied when necessary to eliminate the threat or reduce it to an acceptable level. Auditors should assess the frequency of the separate evaluations as well as the scope or extent of the controls (in relation to the scope of the audit performed) being tested when evaluating the significance of the threat. An evaluation prepared as a nonaudit service is not a substitute for audit procedures in a GAGAS audit.

Information Technology Systems Services

3.56 Services related to information technology (IT) systems include the design or implementation of hardware or software systems. The systems may aggregate source data, form part of the internal control over the subject matter of the audit, or generate information that affects the subject matter of the audit. IT services that would impair independence if provided by an audit organization to an audited entity include:

a. designing or developing a financial or other IT system that will play a significant role in the management of an

area of operations that is or will be the subject matter of an audit;

b. providing services that entail making other than insignificant modifications to the source code underlying such a system; and

c. operating or supervising the operation of such a system.

Valuation Services

3.57 A valuation comprises the making of assumptions with regard to future developments, the application of appropriate methodologies and techniques, and the combination of both to compute a certain value, or range of values, for an asset, a liability, or an entity as a whole. If an audit organization provides valuation services to an audited entity and the valuations would have a material effect, separately or in the aggregate, on the financial statements or other information on which it is reporting, and the valuation involves a significant degree of subjectivity, the audit organization's independence would be impaired.

Other Nonaudit Services

3.58 Provision of certain other nonaudit services always impairs an external auditor's independence with respect to an audited entity. These activities include:

a. Non tax disbursement – prohibited nonaudit services

(1) Accepting responsibility to authorize payment of audited entity funds, electronically or otherwise.

(2) Accepting responsibility for signing or cosigning audited entity checks, even if only in emergency situations.

(3) Maintaining an audited entity's bank account or otherwise having custody of an audited entity's funds or

making credit or banking decisions for the audited entity.

(4) Approving vendor invoices for payment.

b. Benefit plan administration – prohibited nonaudit services

(1) Making policy decisions on behalf of audited entity management.

(2) When dealing with plan participants, interpreting the plan document on behalf of management without first obtaining management's concurrence.

(3) Making disbursements on behalf of the plan.

(4) Having custody of a plan's assets.

(5) Serving a plan as a fiduciary as defined by the Employee Retirement Income Security Act (ERISA).

c. Investment—advisory or management—prohibited nonaudit services

(1) Making investment decisions on behalf of audited entity management or otherwise having discretionary authority over an audited entity's investments.

(2) Executing a transaction to buy or sell an audited entity's investment.

(3) Having custody of an audited entity's assets, such as taking temporary possession of securities purchased by an audited entity.

d. Corporate finance—consulting or advisory – prohibited nonaudit services

(1) Committing the audited entity to the terms of a transaction or consummating a transaction on behalf of the audited entity.

(2) Acting as a promoter, underwriter, broker-dealer, or guarantor of audited entity securities, or distributor of private placement memoranda or offering documents.

(3) Maintaining custody of an audited entity's securities.

e. Executive or employee personnel matters – prohibited nonaudit services

(1) Committing the audited entity to employee compensation or benefit arrangements.

(2) Hiring or terminating audited entity employees.

f. Business risk consulting – prohibited nonaudit services

(1) Making or approving business risk decisions.

(2) Presenting business risk considerations to those charged with governance or others on behalf of management.

Documentation

3.59 Documentation of independence considerations provides evidence of the auditor's judgments in forming conclusions regarding compliance with independence requirements. GAGAS contains specific requirements for documentation related to independence which may be in addition to the documentation that auditors have previously maintained. While insufficient documentation of an auditor's compliance with the independence standard does not impair independence, appropriate documentation is required under the GAGAS quality

control and assurance requirements.[35] The independence standard includes the following documentation requirements:

a. document threats to independence that require the application of safeguards, along with safeguards applied, in accordance with the conceptual framework for independence as required by paragraph 3.24;

b. document the safeguards required by paragraph 3.30 if an audit organization is structurally located within a government entity and is considered independent based on those safeguards;

c. document consideration of audited entity management's ability to effectively oversee a nonaudit service to be provided by the auditor as indicated in paragraph 3.34; and

d. document the auditor's understanding with an audited entity for which the auditor will perform a nonaudit service as indicated in paragraph 3.39.

Professional Judgment

3.60 Auditors must use professional judgment in planning and performing audits and in reporting the results.

3.61 Professional judgment includes exercising reasonable care and professional skepticism. Reasonable care includes acting diligently in accordance with applicable professional standards and ethical principles. Professional skepticism is an attitude that includes a questioning mind and a critical

[35]See paragraph 3.84 for additional discussion of documenting compliance with quality control policies and procedures and paragraph 3.88 for additional discussion of policies and procedures on independence, legal, and ethical requirements.

assessment of evidence. Professional skepticism includes a mindset in which auditors assume neither that management is dishonest nor of unquestioned honesty.

3.62 Using the auditors' professional knowledge, skills, and experience to diligently perform, in good faith and with integrity, the gathering of information and the objective evaluation of the sufficiency and appropriateness of evidence is a critical component of audits. Professional judgment and competence are interrelated because judgments made are dependent upon the auditors' competence.

3.63 Professional judgment represents the application of the collective knowledge, skills, and experiences of all the personnel involved with an audit, as well as the professional judgment of individual auditors. In addition to personnel directly involved in the audit, professional judgment may involve collaboration with other stakeholders, external specialists, and management in the audit organization.

3.64 Using professional judgment is important to auditors in carrying out all aspects of their professional responsibilities, including following the independence standards and related conceptual framework; maintaining objectivity and credibility; assigning competent staff to the audit; defining the scope of work; evaluating, documenting, and reporting the results of the work; and maintaining appropriate quality control over the audit process.

3.65 Using professional judgment is important to auditors in applying the conceptual framework to determine independence in a given situation. This includes the consideration of any threats to the auditor's independence and related safeguards which may mitigate the identified threats. Auditors use professional

judgment in identifying and evaluating any threats to independence, including threats to the appearance of independence.[36]

3.66 Using professional judgment is important to auditors in determining the required level of understanding of the audit subject matter and related circumstances. This includes consideration about whether the audit team's collective experience, training, knowledge, skills, abilities, and overall understanding are sufficient to assess the risks that the subject matter of the audit may contain a significant inaccuracy or could be misinterpreted.

3.67 An auditor's consideration of the risk level of each audit, including the risk of arriving at improper conclusions, is also important. Within the context of audit risk, exercising professional judgment in determining the sufficiency and appropriateness of evidence to be used to support the findings and conclusions based on the audit objectives and any recommendations reported is an integral part of the audit process.

3.68 While this standard places responsibility on each auditor and audit organization to exercise professional judgment in planning and performing an audit, it does not imply unlimited responsibility, nor does it imply infallibility on the part of either the individual auditor or the audit organization. Absolute assurance is not attainable due to factors such as the nature of evidence and characteristics of fraud. Professional judgment does not mean eliminating all possible limitations or weaknesses associated with a specific audit, but rather identifying, assessing, mitigating, and explaining them.

[36]See paragraph 3.03 for a description of independence in appearance.

Competence

3.69 The staff assigned to perform the audit must collectively possess adequate professional competence needed to address the audit objectives and perform the work in accordance with GAGAS.

3.70 The audit organization's management should assess skill needs to consider whether its workforce has the essential skills that match those necessary to perform the particular audit. Accordingly, audit organizations should have a process for recruitment, hiring, continuous development, assignment, and evaluation of staff to maintain a competent workforce. The nature, extent, and formality of the process will depend on various factors such as the size of the audit organization, its structure, and its work.

3.71 Competence is derived from a blending of education and experience. Competencies are not necessarily measured by years of auditing experience because such a quantitative measurement may not accurately reflect the kinds of experiences gained by an auditor in any given time period. Maintaining competence through a commitment to learning and development throughout an auditor's professional life is an important element for auditors. Competence enables an auditor to make sound professional judgments.

Technical Knowledge

3.72 The staff assigned to conduct an audit in accordance with GAGAS should collectively possess the technical knowledge, skills, and experience necessary to be competent for the type of work being performed before beginning work on that audit. The staff assigned to a GAGAS audit should collectively possess

a. knowledge of GAGAS applicable to the type of work they are assigned and the education, skills, and

experience to apply this knowledge to the work being performed;

b. general knowledge of the environment in which the audited entity operates and the subject matter;

c. skills to communicate clearly and effectively, both orally and in writing; and

d. skills appropriate for the work being performed; for example, skills in

(1) statistical or nonstatistical sampling if the work involves use of sampling;

(2) information technology if the work involves review of information systems;

(3) engineering if the work involves review of complex engineering data;

(4) specialized audit methodologies or analytical techniques, such as the use of complex survey instruments, actuarial-based estimates, or statistical analysis tests, as applicable; or

(5) specialized knowledge in subject matters, such as scientific, medical, environmental, educational, or any other specialized subject matter, if the work calls for such expertise.

Additional Qualifications for Financial Audits and Attestation Engagements

3.73 Auditors performing financial audits should be knowledgeable in U.S. generally accepted accounting principles (GAAP), or with the applicable financial reporting framework being used, and the American Institute of Certified Public Accountants' (AICPA)

Statements on Auditing Standards (SAS)[37] and they should be competent in applying these SASs to the audit work.

3.74 Similarly, auditors performing attestation engagements should be knowledgeable in the AICPA general attestation standard related to criteria, the AICPA attestation standards for field work and reporting, and the related Statements on Standards for Attestation Engagements (SSAE),[38] and they should be competent in applying these standards and SSAE to the attestation work.[39]

3.75 Auditors engaged to perform financial audits or attestation engagements should be licensed certified public accountants, persons working for a licensed certified public accounting firm or for a government auditing organization, or licensed accountants in states that have multi-class licensing systems that recognize licensed accountants other than certified public accountants.

Continuing Professional Education

3.76 Auditors performing work in accordance with GAGAS, including planning, directing, performing audit procedures, or reporting on an audit conducted in accordance with GAGAS, should maintain their professional competence through continuing professional education (CPE). Therefore, each auditor performing work in accordance with GAGAS should complete, every 2 years, at least 24 hours of CPE that

[37]See paragraph 2.08 and 4.01 for discussion of the AICPA standards incorporated into GAGAS for financial audits.

[38]See paragraphs 2.09 and 5.01 for discussion of the AICPA standards incorporated into GAGAS for attestation engagements.

[39]See paragraphs 2.19 through 2.22 for additional information on the relationship between GAGAS and other professional standards for financial audits and attestation engagements.

directly relates to government auditing, the government environment, or the specific or unique environment in which the audited entity operates. Auditors who are involved in any amount of planning, directing, or reporting on GAGAS audits and auditors who are not involved in those activities but charge 20 percent or more of their time annually to GAGAS audits should also obtain at least an additional 56 hours of CPE (for a total of 80 hours of CPE in every 2-year period) that enhances the auditor's professional proficiency to perform audits. Auditors required to take the total 80 hours of CPE should complete at least 20 hours of CPE in each year of the 2-year periods. Auditors hired or initially assigned to GAGAS audits after the beginning of an audit organization's 2-year CPE period should complete a prorated number of CPE hours.

3.77 CPE programs are structured educational activities with learning objectives designed to maintain or enhance participants' knowledge, skills, and abilities in areas applicable to performing audits. Determining what subjects are appropriate for individual auditors to satisfy both the 80-hour and the 24-hour requirements is a matter of professional judgment to be exercised by auditors in consultation with appropriate officials in their audit organizations. Among the considerations in exercising that judgment are the auditors' experience, the responsibilities they assume in performing GAGAS audits, and the operating environment of the audited entity.

3.78 Meeting CPE requirements is primarily the responsibility of individual auditors. The audit organization should have quality control procedures to help ensure that auditors meet the continuing education requirements, including documentation of the CPE completed. The Government Accountability Office (GAO) has developed guidance pertaining to CPE requirements to assist auditors and audit organizations

in exercising professional judgment in complying with the CPE requirements.[40]

CPE Requirements for Specialists

3.79 The audit team should determine that external specialists assisting in performing a GAGAS audit are qualified and competent in their areas of specialization; however, external specialists are not required to meet the GAGAS CPE requirements.

3.80 The audit team should determine that internal specialists consulting on a GAGAS audit who are not involved in directing, performing audit procedures, or reporting on a GAGAS audit, are qualified and competent in their areas of specialization; however, these internal specialists are not required to meet the GAGAS CPE requirements.

3.81 The audit team should determine that internal specialists, who are performing work in accordance with GAGAS as part of the audit team, including directing, performing audit procedures, or reporting on a GAGAS audit, comply with GAGAS, including the CPE requirements.[41] The GAGAS CPE requirements become effective for internal specialists when an audit organization first assigns an internal specialist to an audit. Because internal specialists apply specialized knowledge in government audits, training in their areas of specialization qualify under the requirement for 24 hours of CPE that directly relates to government auditing, the government environment, or the specific or unique environment in which the audited entity operates.

[40]*Government Auditing Standards: Guidance on GAGAS Requirements for Continuing Professional Education*, GAO-05-568G (Washington, D.C.: April 2005), http://www.gao.gov/yellowbook.

[41]See paragraphs 3.76 through 3.81 for discussion of the CPE requirements.

Quality Control and Assurance

3.82 Each audit organization performing audits in accordance with GAGAS must:

a. establish and maintain a system of quality control that is designed to provide the audit organization with reasonable assurance that the organization and its personnel comply with professional standards and applicable legal and regulatory requirements,[42] and

b. have an external peer review performed by reviewers independent of the audit organization being reviewed at least once every 3 years.

System of Quality Control

3.83 An audit organization's system of quality control encompasses the audit organization's leadership, emphasis on performing high quality work, and the organization's policies and procedures designed to provide reasonable assurance of complying with professional standards and applicable legal and regulatory requirements. The nature, extent, and formality of an audit organization's quality control system will vary based on the audit organization's circumstances, such as the audit organization's size, number of offices and geographic dispersion, knowledge and experience of its personnel, nature and complexity of its audit work, and cost-benefit considerations.

3.84 Each audit organization should document its quality control policies and procedures and communicate those policies and procedures to its personnel. The audit organization should document compliance with its quality control policies and procedures and maintain such documentation for a

[42]See paragraph A3.10 for additional discussion of the system of quality control.

period of time sufficient to enable those performing monitoring procedures and peer reviews to evaluate the extent of the audit organization's compliance with its quality control policies and procedures. The form and content of such documentation are a matter of professional judgment and will vary based on the audit organization's circumstances.

3.85 An audit organization should establish policies and procedures in its system of quality control that collectively address

a. leadership responsibilities for quality within the audit organization,

b. independence, legal, and ethical requirements,

c. initiation, acceptance, and continuance of audits,

d. human resources,

e. audit performance, documentation, and reporting, and

f. monitoring of quality.

Leadership Responsibilities for Quality within the Audit Organization

3.86 Audit organizations should establish policies and procedures on leadership responsibilities for quality within the audit organization that include the designation of responsibility for quality of audits performed in accordance with GAGAS and communication of policies and procedures relating to quality. Appropriate policies and communications encourage a culture that recognizes that quality is essential in performing GAGAS audits and that leadership of the audit organization is ultimately responsible for the system of quality control.

3.87 The audit organization should establish policies and procedures designed to provide it with reasonable assurance that those assigned operational responsibility for the audit organization's system of quality control have sufficient and appropriate experience and ability, and the necessary authority, to assume that responsibility.

Independence, Legal, and Ethical Requirements

3.88 Audit organizations should establish policies and procedures on independence, legal, and ethical requirements that are designed to provide reasonable assurance that the audit organization and its personnel maintain independence and comply with applicable legal and ethical requirements.[43] Such policies and procedures assist the audit organization to

a. communicate its independence requirements to its staff, and

b. identify and evaluate circumstances and relationships that create threats to independence, and take appropriate action to eliminate those threats or reduce them to an acceptable level by applying safeguards, or, if considered appropriate, withdraw from the audit where withdrawal is not prohibited by law or regulation.

Initiation, Acceptance, and Continuance of Audits

3.89 Audit organizations should establish policies and procedures for the initiation, acceptance, and continuance of audits that are designed to provide reasonable assurance that the audit organization will undertake audits only if it can comply with professional standards, legal requirements, and ethical principles

[43]See paragraphs 3.02 through 3.59 for GAGAS independence requirements. See chapter 1 for GAGAS ethical principles.

and is acting within the legal mandate or authority of the audit organization.[44]

Human Resources

3.90 Audit organizations should establish policies and procedures for human resources that are designed to provide the audit organization with reasonable assurance that it has personnel with the capabilities and competence to perform its audits in accordance with professional standards and legal and regulatory requirements.[45]

Audit Performance, Documentation, and Reporting

3.91 Audit organizations should establish policies and procedures for audit performance, documentation, and reporting that are designed to provide the audit organization with reasonable assurance that audits are performed and reports are issued in accordance with professional standards and legal and regulatory requirements.[46]

3.92 When performing GAGAS audits, audit organizations should have policies and procedures for the safe custody and retention of audit documentation for a time sufficient to satisfy legal, regulatory, and administrative requirements for records retention. Whether audit documentation is in paper, electronic, or other media, the integrity, accessibility, and retrievability of the underlying information could be compromised if the documentation is altered, added to, or deleted without the auditors' knowledge, or if the documentation is lost or damaged. For audit documentation that is retained electronically, the audit organization should

[44]See paragraph A3.10a for discussion of initiation of audits by government audit organizations.

[45]See paragraphs 3.69 through 3.81 for requirements related to professional competence.

[46]For financial audits, chapters 2 through 4 apply; for attestation engagements, chapters 2, 3 and 5 apply; for performance audits, chapters 2, 3, 6, and 7 apply.

establish effective information systems controls concerning accessing and updating the audit documentation.

Monitoring of Quality

3.93 Audit organizations should establish policies and procedures for monitoring of quality in the audit organization.[47] Monitoring of quality is an ongoing, periodic assessment of work completed on audits designed to provide management of the audit organization with reasonable assurance that the policies and procedures related to the system of quality control are suitably designed and operating effectively in practice. The purpose of monitoring compliance with quality control policies and procedures is to provide an evaluation of whether the:

a. professional standards and legal and regulatory requirements have been followed,

b. quality control system has been appropriately designed, and

c. quality control policies and procedures are operating effectively and complied with in practice.

3.94 Monitoring procedures will vary based on the audit organization's facts and circumstances. The audit organization should perform monitoring procedures that enable it to assess compliance with applicable professional standards and quality control policies and procedures for GAGAS audits. Individuals performing monitoring should collectively have sufficient expertise and authority for this role.

3.95 The audit organization should analyze and summarize the results of its monitoring process at least

[47]See paragraph A3.10c for additional discussion of monitoring.

annually, with identification of any systemic or repetitive issues needing improvement, along with recommendations for corrective action. The audit organization should communicate to appropriate personnel any deficiencies noted during the monitoring process and make recommendations for appropriate remedial action.

External Peer Review

3.96 The audit organization should obtain an external peer review at least once every 3 years that is sufficient in scope to provide a reasonable basis for determining whether, for the period under review, the reviewed audit organization's system of quality control was suitably designed and whether the audit organization is complying with its quality control system in order to provide the audit organization with reasonable assurance of conforming with applicable professional standards.

3.97 The first peer review for an audit organization not already subject to a peer review requirement covers a review period ending no later than 3 years from the date an audit organization begins its first audit in accordance with GAGAS. The period under review generally covers 1 year, although peer review programs may choose a longer review period. Generally, the deadlines for peer review reports are established by the entity that administers the peer review program. Extensions of the deadlines for submitting the peer review report exceeding 3 months beyond the due date are granted by the entity that administers the peer review program and GAO.

3.98 The peer review team should include the following elements in the scope of the peer review:

a. review of the audit organization's quality control policies and procedures;

b. consideration of the adequacy and results of the audit organization's internal monitoring procedures;

c. review of selected auditors' reports and related documentation;

d. review of other documents necessary for assessing compliance with standards, for example, independence documentation, CPE records, and relevant human resource management files; and

e. interviews with a selection of the reviewed audit organization's professional staff at various levels to assess their understanding of and compliance with relevant quality control policies and procedures.

3.99 The peer review team should perform an assessment of peer review risk to help determine the number and types of audits to select for review.[48] Based on the risk assessment, the team should use one or a combination of the following approaches to select individual audits for review with greater emphasis on those audits with higher assessed levels of peer review risk: (1) select GAGAS audits that provide a reasonable cross-section of the GAGAS audits performed by the reviewed audit organization; or (2) select audits that provide a reasonable cross-section from all types of work subject to the reviewed audit organization's quality control system, including one or more audits performed in accordance with GAGAS. The second approach is generally applicable to audit organizations that perform only a small number of GAGAS audits in relation to other types of audits. In these cases, one or more GAGAS audits may represent more than what would be

[48]See paragraph A3.11 for examples of factors to consider in assessing peer review risk.

selected when looking at a cross-section of the audit organization's work as a whole.

3.100 The peer review team should prepare one or more written reports communicating the results of the peer review, including the following:

a. a description of the scope of the peer review, including any limitations;

b. an opinion on whether the system of quality control of the reviewed audit organization's audit practices was adequately designed and complied with during the period reviewed to provide the audit organization with reasonable assurance of conforming with applicable professional standards;

c. specification of the professional standards to which the reviewed audit organization is being held; and

d. reference to a separate written communication, if issued under the peer review program.

3.101 The peer review team uses professional judgment in deciding the type of peer review report. The following are the types of peer review reports.

a. Peer Review Rating of Pass: A conclusion that the audit organization's system of quality control has been suitably designed and complied with to provide the audit organization with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects.

b. Peer Review Rating of Pass with Deficiencies: A conclusion that the audit organization's system of quality control has been suitably designed and complied with to provide the audit organization with reasonable assurance of performing and reporting in conformity

with applicable professional standards in all material respects with the exception of a certain deficiency or deficiencies that are described in the report.

c. Peer Review Rating of Fail: A conclusion, based on the significant deficiencies that are described in the report, that the audit organization's system of quality control is not suitably designed to provide the audit organization with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects, or the audit organization has not complied with its system of quality control to provide the audit organization with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects.

3.102 When the scope of the review is limited by conditions that preclude the application of one or more peer review procedures considered necessary in the circumstances and the peer reviewer cannot accomplish the objectives of those procedures through alternative procedures, the types of reports described in paragraphs 3.101 a-c are modified by including statements in the report's scope paragraph, body and opinion paragraph. These statements describe the relationship of the excluded audit(s) or functional area(s) to the reviewed organization's full scope of practice and system of quality control and the effects of the exclusion on the scope and results of the review.

3.103 For any deficiencies or significant deficiencies included in the peer review report or other written communication, the peer review team should include, either in the peer review report or in a separate written communication, a detailed description of the findings, conclusions, and recommendations related to the deficiencies or significant deficiencies.

3.104 The peer review team should meet the following criteria:

a. The review team collectively has current knowledge of GAGAS and government auditing.

b. The organization conducting the peer review and individual review team members are independent (as defined in GAGAS)[49] of the audit organization being reviewed, its staff, and the audits selected for the peer review.

c. The review team collectively has sufficient knowledge of how to perform a peer review. Such knowledge may be obtained from on-the-job training, training courses, or a combination of both. Having personnel on the peer review team with prior experience on a peer review or internal inspection team is desirable.

3.105 An external audit organization[50] should make its most recent peer review report publicly available.[51] For example, an audit organization may satisfy this requirement by posting the peer review report on a publicly available web site or to a publicly available file designed for public transparency of peer review results. Alternatively, if neither of these options is available to the audit organization, then it should use the same transparency mechanism it uses to make other information public. The audit organization should provide the peer review report to others upon request. If a separate communication detailing findings, conclusions, and recommendations is issued, public

[49]See paragraphs 3.02 through 3.32 for discussion of independence.

[50]See paragraph 1.07b for the definition of "audit organizations" and paragraph 1.08 for discussion of external audit organizations.

[51]See paragraph A3.12 for additional discussion of peer review report transparency.

availability of that communication is not required. Internal audit organizations that report internally to management and those charged with governance should provide a copy of the peer review report to those charged with governance.

3.106 Information in peer review reports may be relevant to decisions on procuring audits. Therefore, audit organizations seeking to enter into a contract to perform an audit in accordance with GAGAS should provide the following to the party contracting for such services when requested:

a. the audit organization's most recent peer review report, and

b. any subsequent peer review reports received during the period of the contract.

3.107 Auditors who are using another audit organization's work should request a copy of the audit organization's latest peer review report and any other written communication issued, and the audit organization should provide these documents when requested.[52]

[52]See paragraphs 6.40 through 6.44 for additional discussion on using the work of other auditors.

Standards for Financial Audits

Introduction

4.01 This chapter contains requirements, guidance, and considerations for performing and reporting on financial audits conducted in accordance with generally accepted government auditing standards (GAGAS). GAGAS incorporates by reference the American Institute of Certified Public Accountants (AICPA) Statements on Auditing Standards (SAS), as discussed in paragraph 2.08.[53] All sections of the SASs are incorporated, including the introduction, objectives, definitions, requirements, and application and other explanatory material. Auditors performing financial audits in accordance with GAGAS should comply with the incorporated SASs and the additional requirements in this chapter. The requirements and guidance contained in chapters 1 through 3 also apply to financial audits performed in accordance with GAGAS.

Additional GAGAS Requirements for Performing Financial Audits

4.02 GAGAS establishes requirements for performing financial audits in addition to the requirements contained in the AICPA standards. Auditors should comply with these additional requirements, along with the incorporated SASs, when citing GAGAS in their reports. The additional requirements for performing financial audits relate to:

a. auditor communication;

b. previous audits and attestation engagements;

[53]See the AICPA *Codification of Statements on Auditing Standards* and paragraph 2.20 for additional discussion on the relationship between GAGAS and other professional standards. References to the AICPA *Codification of Statements on Auditing Standards* use an "AU-C" identifier to refer to the clarified SASs instead of an "AU" identifier. "AU-C" is a temporary identifier to avoid confusion with references to existing "AU" sections, which remain effective through 2013. The "AU-C" identifier will revert to "AU" in 2014 AICPA *Codification of Statements on Auditing Standards*, by which time the clarified SASs become fully effective for all engagements.

c. fraud, noncompliance with provisions of laws, regulations, contracts, and grant agreements, and abuse;

d. developing elements of a finding; and

e. audit documentation.[54]

Auditor Communication

4.03 In addition to the AICPA requirements for auditor communication,[55] when performing a GAGAS financial audit, auditors should communicate pertinent information that in the auditors' professional judgment needs to be communicated to individuals contracting for or requesting the audit, and to cognizant legislative committees when auditors perform the audit pursuant to a law or regulation, or they conduct the work for the legislative committee that has oversight of the audited entity. This requirement does not apply if the law or regulation requiring an audit of the financial statements does not specifically identify the entities to be audited, such as audits required by the Single Audit Act Amendments of 1996.

4.04 In those situations where there is not a single individual or group that both oversees the strategic direction of the audited entity and the fulfillment of its accountability obligations or in other situations where the identity of those charged with governance is not clearly evident, auditors should document the process followed and conclusions reached for identifying the appropriate individuals to receive the required auditor communications.

[54]See paragraphs 4.03 through 4.16 for additional discussion of paragraph 4.02 a-e.

[55]See AICPA AU-C Section 260, *The Auditor's Communication With Those Charged With Governance.*

Previous Audits and Attestation Engagements

4.05 When performing a GAGAS audit, auditors should evaluate whether the audited entity has taken appropriate corrective action to address findings and recommendations from previous engagements that could have a material effect on the financial statements or other financial data significant to the audit objectives. When planning the audit, auditors should ask management of the audited entity to identify previous audits, attestation engagements, and other studies that directly relate to the objectives of the audit, including whether related recommendations have been implemented. Auditors should use this information in assessing risk and determining the nature, timing, and extent of current audit work, including determining the extent to which testing the implementation of the corrective actions is applicable to the current audit objectives.

Fraud, Noncompliance with Provisions of Laws, Regulations, Contracts, and Grant Agreements, and Abuse

4.06 In addition to the AICPA requirements concerning fraud[56] and noncompliance with provisions of laws and regulations,[57] when performing a GAGAS financial audit, auditors should extend the AICPA requirements pertaining to the auditors' responsibilities for laws and regulations to also apply to consideration of compliance with provisions of contracts or grant agreements.

4.07 Abuse involves behavior that is deficient or improper when compared with behavior that a prudent person would consider reasonable and necessary business practice given the facts and circumstances. Abuse also includes misuse of authority or position for personal financial interests or those of an immediate or

[56]See AICPA AU-C Section 240, *Consideration of Fraud in a Financial Statement Audit*.

[57]See AICPA AU-C Section 250, *Consideration of Laws and Regulations in an Audit of Financial Statements.*

close family member or business associate.[58] Abuse does not necessarily involve fraud, or noncompliance with provisions of laws, regulations, contracts, or grant agreements.

4.08 Because the determination of abuse is subjective, auditors are not required to detect abuse in financial audits. However, as part of a GAGAS audit, if auditors become aware of abuse that could be quantitatively or qualitatively material to the financial statements or other financial data significant to the audit objectives, auditors should apply audit procedures specifically directed to ascertain the potential effect on the financial statements or other financial data significant to the audit objectives. After performing additional work, auditors may discover that the abuse represents potential fraud or noncompliance with provisions of laws, regulations, contracts, or grant agreements.

4.09 Avoiding interference with investigations or legal proceedings is important in pursuing indications of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse. Laws, regulations, or policies may require auditors to report indications of certain types of fraud, noncompliance with provisions of laws, regulations, contracts or grant agreements, or abuse to law enforcement or investigatory authorities before performing additional audit procedures. When investigations or legal proceedings are initiated or in process, auditors should evaluate the impact on the current audit. In some cases, it may be appropriate for the auditors to work with investigators or legal authorities, or withdraw from or defer further work on the audit engagement or a portion of the engagement to

[58]See paragraph A.08 for additional examples of abuse.

avoid interfering with an ongoing investigation or legal proceeding.

Developing Elements of a Finding

4.10 In a financial audit, findings may involve deficiencies in internal control; noncompliance with provisions of laws, regulations, contracts, or grant agreements; fraud; or abuse. As part of a GAGAS audit, when auditors identify findings, auditors should plan and perform procedures to develop the elements of the findings that are relevant and necessary to achieve the audit objectives. The elements of a finding are discussed in paragraphs 4.11 through 4.14 below.

4.11 Criteria: The laws, regulations, contracts, grant agreements, standards, measures, expected performance, defined business practices, and benchmarks against which performance is compared or evaluated. Criteria identify the required or desired state or expectation with respect to the program or operation. Criteria provide a context for evaluating evidence and understanding the findings.

4.12 Condition: Condition is a situation that exists. The condition is determined and documented during the audit.

4.13 Cause: The cause identifies the reason or explanation for the condition or the factor or factors responsible for the difference between the situation that exists (condition) and the required or desired state (criteria), which may also serve as a basis for recommendations for corrective actions. Common factors include poorly designed policies, procedures, or criteria; inconsistent, incomplete, or incorrect implementation; or factors beyond the control of program management. Auditors may assess whether the evidence provides a reasonable and convincing argument for why the stated cause is the key factor or

factors contributing to the difference between the condition and the criteria.

4.14 Effect or potential effect: The effect is a clear, logical link to establish the impact or potential impact of the difference between the situation that exists (condition) and the required or desired state (criteria). The effect or potential effect identifies the outcomes or consequences of the condition. When the audit objectives include identifying the actual or potential consequences of a condition that varies (either positively or negatively) from the criteria identified in the audit, "effect" is a measure of those consequences. Effect or potential effect may be used to demonstrate the need for corrective action in response to identified problems or relevant risks.

Audit Documentation

4.15 In addition to the AICPA requirements for audit documentation,[59] auditors should comply with the following additional requirements when performing a GAGAS financial audit.[60]

a. Document supervisory review, before the report release date, of the evidence that supports the findings, conclusions, and recommendations contained in the auditors' report.

b. Document any departures from the GAGAS requirements and the impact on the audit and on the auditors' conclusions when the audit is not in compliance with applicable GAGAS requirements due to law, regulation, scope limitations, restrictions on access to records, or other issues impacting the audit.

[59]See AICPA AU-C Section 230, *Audit Documentation.*

[60]See paragraphs 4.04, 4.06, 4.26, and 4.45 for additional documentation requirements regarding financial audits.

This applies to departures from unconditional requirements and presumptively mandatory requirements when alternative procedures performed in the circumstances were not sufficient to achieve the objectives of the requirements.[61]

4.16 When performing GAGAS financial audits and subject to applicable provisions of laws and regulations, auditors should make appropriate individuals, as well as audit documentation, available upon request and in a timely manner to other auditors or reviewers. Underlying GAGAS audits is the premise that audit organizations in federal, state, and local governments and public accounting firms engaged to perform a financial audit in accordance with GAGAS cooperate in auditing programs of common interest so that auditors may use others' work and avoid duplication of efforts. The use of auditors' work by other auditors may be facilitated by contractual arrangements for GAGAS audits that provide for full and timely access to appropriate individuals, as well as audit documentation.

Additional GAGAS Requirements for Reporting on Financial Audits

4.17 In addition to the AICPA requirements for reporting,[62] auditors should comply with the following additional requirements when citing GAGAS in their reports. The additional requirements relate to

a. reporting auditors' compliance with GAGAS;

[61]See paragraphs 2.24 and 2.25 for additional requirements on citing compliance with GAGAS.

[62]See AICPA AU-C Sections 700 *Forming an Opinion and Reporting on Financial Statements;* 705 *Modifications to the Opinion in the Independent Auditor's Report,* and 706 *Emphasis-of-Matter Paragraphs and Other-Matter Paragraphs in the Independent Auditor's Report.*

b. reporting on internal control and compliance with provisions of laws, regulations, contracts, and grant agreements;

c. communicating deficiencies in internal control, fraud, noncompliance with provisions of laws, regulations, contracts, and grant agreements, and abuse;

d. reporting views of responsible officials;

e. reporting confidential or sensitive information; and

f. distributing reports.[63]

Reporting Auditors' Compliance with GAGAS

4.18 When auditors comply with all applicable GAGAS requirements for financial audits, they should include a statement in the auditors' report that they performed the audit in accordance with GAGAS.[64] Because GAGAS incorporates by reference the AICPA SASs,[65] GAGAS does not require auditors to cite compliance with the AICPA standards when citing compliance with GAGAS. Additionally, an entity receiving a GAGAS auditors' report may also request auditors to issue a financial audit report for purposes other than complying with requirements for a GAGAS audit. GAGAS does not prohibit auditors from issuing a separate report conforming only to AICPA or other standards.[66]

[63]See paragraphs 4.18 through 4.45 for additional discussion paragraph of 4.17 a-f.

[64]See paragraphs 2.24 and 2.25 for additional requirements on citing compliance with GAGAS.

[65]See paragraph 2.08 for a discussion of the AICPA SASs incorporated into GAGAS.

[66]See AICPA AU-C Section 700, *Forming an Opinion and Reporting on Financial Statements.*

Reporting on Internal Control and Compliance with Provisions of Laws, Regulations, Contracts, and Grant Agreements

4.19 When providing an opinion or a disclaimer on financial statements, auditors should also report on internal control over financial reporting[67] and on compliance with provisions of laws, regulations, contracts, or grant agreements that have a material effect on the financial statements.[68] Auditors report on internal control and compliance, regardless of whether or not they identify internal control deficiencies or instances of noncompliance.

4.20 Auditors should include either in the same or in separate report(s) a description of the scope of the auditors' testing of internal control over financial reporting and of compliance with provisions of laws, regulations, contracts, or grant agreements. Auditors should also state in the reports whether the tests they performed provided sufficient, appropriate evidence to support opinions on the effectiveness of internal control and on compliance with provisions of laws, regulations, contracts, or grant agreements.

4.21 The objective of the GAGAS requirement for reporting on internal control over financial reporting differs from the objective of an examination of internal control in accordance with the AICPA Statement on Standards for Attestation Engagements (SSAE), which is to express an opinion on the design or the design and operating effectiveness of an entity's internal control, as applicable. To form a basis for expressing such an opinion, the auditor would need to plan and perform the examination to provide a high level of assurance about whether the entity maintained, in all material respects, effective internal control over financial reporting as of a

[67]See paragraph A.05 for examples of deficiencies in internal control.

[68]See paragraph A.11 for additional discussion of laws, regulations, and provisions of contract and grant agreements.

point in time or for a specified period of time.[69] If auditors issue an opinion on internal control, the opinion would satisfy the GAGAS requirement for reporting on internal control.

4.22 If auditors report separately (including separate reports bound in the same document) on internal control over financial reporting and on compliance with provisions of laws, regulations, contracts, and grant agreements, they should state in the auditors' report on the financial statements that they are issuing those additional reports. They should include a reference to the separate reports and also state that the reports on internal control over financial reporting and on compliance with provisions of laws, regulations, contracts, and grant agreements are an integral part of a GAGAS audit in considering the audited entity's internal control over financial reporting and compliance.

Communicating Deficiencies in Internal Control, Fraud, Noncompliance with Provisions of Laws, Regulations, Contracts, and Grant Agreements, and Abuse

4.23 When performing GAGAS financial audits, auditors should communicate in the report on internal control over financial reporting and compliance, based upon the work performed, (1) significant deficiencies and material weaknesses in internal control; (2) instances of fraud and noncompliance with provisions of laws or regulations that have a material effect on the audit and any other instances that warrant the attention of those charged with governance; (3) noncompliance with provisions of contracts or grant agreements that has a material effect on the audit; and (4) abuse that has a material effect on the audit.

Deficiencies in Internal Control

4.24 The AICPA requirements to communicate in writing significant deficiencies and material weaknesses

[69]See AICPA AT Section 501, *An Examination of an Entity's Internal Control Over Financial Reporting That Is Integrated With an Audit of Its Financial Statements.*

identified during an audit[70] form the basis for reporting significant deficiencies and material weaknesses in the GAGAS report on internal control over financial reporting when deficiencies are identified during the audit.

Fraud, Noncompliance with Provisions of Laws, Regulations, Contracts, and Grant Agreements, and Abuse

4.25 When performing a GAGAS financial audit, and auditors conclude, based on sufficient, appropriate evidence, that any of the following either has occurred or is likely to have occurred, they should include in their report on internal control and compliance the relevant information about

a. fraud[71] and noncompliance with provisions of laws or regulations that have a material effect on the financial statements or other financial data significant to the audit objectives and any other instances that warrant the attention of those charged with governance;

b. noncompliance with provisions of contracts or grant agreements that has a material effect on the determination of financial statement amounts or other financial data significant to the audit objectives; or

c. abuse[72] that is material, either quantitatively or qualitatively.[73]

4.26 When auditors detect instances of noncompliance with provisions of contracts or grant agreements or abuse that have an effect on the financial statements or other financial data significant to the audit objectives

[70]See AICPA AU-C Section 265, *Communicating Internal Control Related Matters Identified in an Audit.*

[71]See paragraph A.10 for examples of indicators of fraud risk.

[72]See paragraph A.08 for examples of abuse.

[73]See paragraphs 4.07 and 4.08 for a discussion of abuse.

that are less than material but warrant the attention of those charged with governance, they should communicate those findings in writing to audited entity officials. When auditors detect any instances of fraud, noncompliance with provisions of laws, regulations, contracts or grant agreements, or abuse that do not warrant the attention of those charged with governance, the auditors' determination of whether and how to communicate such instances to audited entity officials is a matter of professional judgment.

4.27 When fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse either have occurred or are likely to have occurred, auditors may consult with authorities or legal counsel about whether publicly reporting such information would compromise investigative or legal proceedings. Auditors may limit their public reporting to matters that would not compromise those proceedings, and for example, report only on information that is already a part of the public record.

Presenting Findings in the Auditors' Report

4.28 When performing a GAGAS financial audit and presenting findings such as deficiencies in internal control, fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse, auditors should develop the elements of the findings to the extent necessary, including findings related to deficiencies from the previous year that have not been remediated. Clearly developed findings, as discussed in paragraphs 4.10 through 4.14, assist management or oversight officials of the audited entity in understanding the need for taking corrective action, and assist auditors in making recommendations for corrective action. If auditors sufficiently develop the elements of a finding, they may provide recommendations for corrective action.

4.29 Auditors should place their findings in perspective by describing the nature and extent of the issues being reported and the extent of the work performed that resulted in the finding. To give the reader a basis for judging the prevalence and consequences of these findings, auditors should, as appropriate, relate the instances identified to the population or the number of cases examined and quantify the results in terms of dollar value or other measures. If the results cannot be projected, auditors should limit their conclusions appropriately.

Reporting Findings Directly to Parties Outside the Audited Entity

4.30 Auditors should report known or likely fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse directly to parties outside the audited entity in the following two circumstances.

a. When entity management fails to satisfy legal or regulatory requirements to report such information to external parties specified in law or regulation, auditors should first communicate the failure to report such information to those charged with governance. If the audited entity still does not report this information to the specified external parties as soon as practicable after the auditors' communication with those charged with governance, then the auditors should report the information directly to the specified external parties.

b. When entity management fails to take timely and appropriate steps to respond to known or likely fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that (1) is likely to have a material effect on the financial statements and (2) involves funding received directly or indirectly from a government agency, auditors should first report management's failure to take timely and appropriate steps to those charged with governance. If the audited entity still does not take timely and

appropriate steps as soon as practicable after the auditors' communication with those charged with governance, then the auditors should report the entity's failure to take timely and appropriate steps directly to the funding agency.

4.31 The reporting in paragraph 4.30 is in addition to any legal requirements to report such information directly to parties outside the audited entity. Auditors should comply with these requirements even if they have resigned or been dismissed from the audit prior to its completion.

4.32 Auditors should obtain sufficient, appropriate evidence, such as confirmation from outside parties, to corroborate assertions by management of the audited entity that it has reported such findings in accordance with laws, regulations, or funding agreements. When auditors are unable to do so, they should report such information directly as discussed in paragraphs 4.30 and 4.31.

Reporting Views of Responsible Officials

4.33 When performing a GAGAS financial audit, if the auditors' report discloses deficiencies in internal control, fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse, auditors should obtain and report the views of responsible officials of the audited entity concerning the findings, conclusions, and recommendations, as well as any planned corrective actions.

4.34 Providing a draft report with findings for review and comment by responsible officials of the audited entity and others helps the auditors develop a report that is fair, complete, and objective. Including the views of responsible officials results in a report that presents not only the auditors' findings, conclusions, and recommendations, but also the perspectives of the

responsible officials of the audited entity and the corrective actions they plan to take. Obtaining the comments in writing is preferred, but oral comments are acceptable.

4.35 When auditors receive written comments from the responsible officials, they should include in their report a copy of the officials' written comments, or a summary of the comments received. When the responsible officials provide oral comments only, auditors should prepare a summary of the oral comments and provide a copy of the summary to the responsible officials to verify that the comments are accurately stated.

4.36 Auditors should also include in the report an evaluation of the comments, as appropriate. In cases in which the audited entity provides technical comments in addition to its written or oral comments on the report, auditors may disclose in the report that such comments were received.

4.37 Obtaining oral comments may be appropriate when, for example, there is a reporting date critical to meeting a user's needs; auditors have worked closely with the responsible officials throughout the work and the parties are familiar with the findings and issues addressed in the draft report; or the auditors do not expect major disagreements with findings, conclusions, or recommendations in the draft report, or major controversies with regard to the issues discussed in the draft report.

4.38 When the audited entity's comments are inconsistent or in conflict with the findings, conclusions, or recommendations in the draft report, or when planned corrective actions do not adequately address the auditors' recommendations, the auditors should evaluate the validity of the audited entity's comments. If the auditors disagree with the comments, they should

explain in the report their reasons for disagreement. Conversely, the auditors should modify their report as necessary if they find the comments valid and supported with sufficient, appropriate evidence.

4.39 If the audited entity refuses to provide comments or is unable to provide comments within a reasonable period of time, the auditors may issue the report without receiving comments from the audited entity. In such cases, the auditors should indicate in the report that the audited entity did not provide comments.

Reporting Confidential and Sensitive Information

4.40 When performing a GAGAS financial audit, if certain pertinent information is prohibited from public disclosure or is excluded from a report due to the confidential or sensitive nature of the information, auditors should disclose in the report that certain information has been omitted and the reason or other circumstances that make the omission necessary.

4.41 Certain information may be classified or may otherwise be prohibited from general disclosure by federal, state, or local laws or regulations. In such circumstances, auditors may issue a separate, classified, or limited use report containing such information and distribute the report only to persons authorized by law or regulation to receive it.

4.42 Additional circumstances associated with public safety, privacy, or security concerns could also justify the exclusion of certain information from a publicly available or widely distributed report. For example, detailed information related to computer security for a particular program may be excluded from publicly available reports because of the potential damage that could be caused by the misuse of this information. In such circumstances, auditors may issue a limited use report containing such information and distribute the

report only to those parties responsible for acting on the auditors' recommendations. In some instances, it may be appropriate to issue both a publicly available report with the sensitive information excluded and a limited use report. The auditors may consult with legal counsel regarding any requirements or other circumstances that may necessitate the omission of certain information.

4.43 Considering the broad public interest in the program or activity under audit assists auditors when deciding whether to exclude certain information from publicly available reports. When circumstances call for omission of certain information, auditors should evaluate whether this omission could distort the audit results or conceal improper or illegal practices.

4.44 When audit organizations are subject to public records laws, auditors should determine whether public records laws could impact the availability of classified or limited use reports and determine whether other means of communicating with management and those charged with governance would be more appropriate. For example, the auditors may communicate general information in a written report and communicate detailed information orally. The auditors may consult with legal counsel regarding applicable public records laws.

Distributing Reports

4.45 Distribution of reports completed in accordance with GAGAS depends on the relationship of the auditors to the audited organization and the nature of the information contained in the report. Auditors should document any limitation on report distribution.[74] The following discussion outlines distribution for reports completed in accordance with GAGAS:

[74]See paragraphs 4.41 and 4.42 for discussion of limited use reports containing confidential or sensitive information.

a. Audit organizations in government entities should distribute auditors' reports to those charged with governance, to the appropriate audited entity officials, and to the appropriate oversight bodies or organizations requiring or arranging for the audits. As appropriate, auditors should also distribute copies of the reports to other officials who have legal oversight authority or who may be responsible for acting on audit findings and recommendations, and to others authorized to receive such reports.

b. Internal audit organizations in government entities may also follow the Institute of Internal Auditors (IIA) *International Standards for the Professional Practice of Internal Auditing*.[75] In accordance with GAGAS and IIA standards, the head of the internal audit organization should communicate results to the parties who can ensure that the results are given due consideration. If not otherwise mandated by statutory or regulatory requirements, prior to releasing results to parties outside the organization, the head of the internal audit organization should: (1) assess the potential risk to the organization, (2) consult with senior management or legal counsel as appropriate, and (3) control dissemination by indicating the intended users in the report.

c. Public accounting firms contracted to perform an audit in accordance with GAGAS should clarify report distribution responsibilities with the engaging organization. If the contracting firm is responsible for the distribution, it should reach agreement with the party contracting for the audit about which officials or

[75]See paragraph 2.21 for additional discussion about using the IIA standards in conjunction with GAGAS and paragraph 2.22 for additional discussion about citing compliance with another set of standards.

organizations will receive the report and the steps being taken to make the report available to the public.

Additional GAGAS Considerations for Financial Audits

4.46 Due to the objectives and public accountability of GAGAS audits, additional considerations for financial audits completed in accordance with GAGAS may apply. These considerations relate to

a. materiality in GAGAS financial audits; and

b. early communication of deficiencies.[76]

Materiality in GAGAS Financial Audits

4.47 The AICPA standards require the auditor to apply the concept of materiality appropriately in planning and performing the audit.[77] Additional considerations may apply to GAGAS financial audits of government entities or entities that receive government awards. For example, in audits performed in accordance with GAGAS, auditors may find it appropriate to use lower materiality levels as compared with the materiality levels used in non-GAGAS audits because of the public accountability of government entities and entities receiving government funding, various legal and regulatory requirements, and the visibility and sensitivity of government programs.

[76]See paragraphs 4.47 through 4.48 for additional discussion of paragraph 4.46 a-b.

[77]See AICPA AU-C Section 320, *Materiality in Planning and Performing an Audit.*

Early Communication of Deficiencies

4.48 For some matters, early communication to those charged with governance or management may be important because of the relative significance and the urgency for corrective follow-up action.[78] Further, when a control deficiency results in noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse, early communication is important to allow management to take prompt corrective action to prevent further noncompliance. When a deficiency is communicated early, the reporting requirements in paragraphs 4.19 through 4.23 still apply.

[78]See AICPA AU-C Section 265, *Communicating Internal Control Related Matters Identified in an Audit.*

Standards for Attestation Engagements

Introduction

5.01 This chapter contains requirements, guidance, and considerations for performing and reporting on attestation engagements conducted in accordance with generally accepted government auditing standards (GAGAS). Auditors performing attestation engagements in accordance with GAGAS should comply with the American Institute of Certified Public Accountants (AICPA) general attestation standard on criteria, the field work and reporting attestation standards, and the corresponding statements on standards for attestation engagements (SSAEs), which are incorporated in this chapter by reference.[79] Auditors performing attestation engagements in accordance with GAGAS should also comply with the additional requirements in this chapter. The requirements and guidance contained in chapters 1 through 3 also apply to attestation engagements performed in accordance with GAGAS.

5.02 An attestation engagement can provide one of three levels of service as defined by the AICPA, namely an examination engagement, a review engagement, or an agreed-upon procedures engagement.[80] Auditors performing an attestation engagement should determine which of the three levels of service apply to that engagement and refer to the appropriate AICPA standards and GAGAS section below for applicable requirements and considerations.

[79]See AICPA AT Section 50, *SSAE Hierarchy.*

[80]See paragraph 2.09 and AICPA AT Section 101, *Attest Engagements*.

Examination Engagements

Additional Field Work Requirements for Examination Engagements

5.03 GAGAS establishes field work requirements for performing examination engagements in addition to the requirements contained in the AICPA standards. Auditors should comply with these additional requirements, along with the relevant AICPA standards for examination attestation engagements, when citing GAGAS in their examination reports. The additional field work requirements relate to:

a. auditor communication;

b. previous audits and attestation engagements;

c. fraud, noncompliance with provisions of laws, regulations, contracts, and grant agreements, and abuse;

d. developing elements of a finding; and

e. examination engagement documentation.[81]

Auditor Communication

5.04 In addition to the AICPA requirements for auditor communication,[82] when performing a GAGAS examination engagement, auditors should communicate pertinent information that in the auditors' professional judgment needs to be communicated to individuals contracting for or requesting the examination engagement, and to cognizant legislative committees

[81]See paragraphs 5.04 through 5.17 for additional discussion of 5.03 a-e.

[82]See AICPA AT Section 101.14 and 101.46, *Attest Engagements.*

when auditors perform the examination engagement pursuant to a law or regulation, or they conduct the work for the legislative committee that has oversight of the audited entity.

5.05 In those situations where there is not a single individual or group that both oversees the strategic direction of the audited entity and the fulfillment of its accountability obligations or in other situations where the identity of those charged with governance is not clearly evident, auditors should document the process followed and conclusions reached for identifying the appropriate individuals to receive the required auditor communications.

Previous Audits and Attestation Engagements

5.06 When performing a GAGAS examination engagement, auditors should evaluate whether the audited entity has taken appropriate corrective action to address findings and recommendations from previous engagements that could have a material effect on the subject matter, or an assertion about the subject matter, of the examination engagement. When planning the engagement, auditors should ask audited entity management to identify previous audits, attestation engagements, and other studies that directly relate to the subject matter or an assertion about the subject matter of the examination engagement being undertaken, including whether related recommendations have been implemented. Auditors should use this information in assessing risk and determining the nature, timing, and extent of current work, including determining the extent to which testing the implementation of the corrective actions is applicable to the current examination engagement objectives.

Fraud, Noncompliance with Provisions of Laws, Regulations, Contracts, and Grant Agreements, and Abuse

5.07 In addition to the AICPA requirements concerning fraud,[83] when performing a GAGAS examination engagement, auditors should design the engagement to detect instances of fraud and noncompliance with provisions of laws, regulations, contracts, and grant agreements that may have a material effect on the subject matter or the assertion thereon of the examination engagement. Auditors should assess the risk and possible effects of fraud and noncompliance with provisions of laws, regulations, contracts, and grant agreements that could have a material effect on the subject matter or an assertion about the subject matter of the examination engagement. When risk factors are identified, auditors should document the risk factors identified, the auditors' response to those risk factors individually or in combination, and the auditors' conclusions.[84]

5.08 Abuse involves behavior that is deficient or improper when compared with behavior that a prudent person would consider a reasonable and necessary business practice given the facts and circumstances. Abuse also includes misuse of authority or position for personal financial interests or those of an immediate or close family member or business associate.[85] Abuse does not necessarily involve fraud, or noncompliance with provisions of laws, regulations, contracts, or grant agreements.

[83]See AICPA AT Sections 501.27, *An Examination of an Entity's Internal Control Over Financial Reporting That Is Integrated With an Audit of Its Financial Statements*, 601.33, *Compliance Attestation*, and 701.42, *Management's Discussion and Analysis*.

[84]See paragraphs A.09 through A.13 for additional discussion of indicators of fraud risk and significance of provisions of laws, regulations, and contracts and grant agreements.

[85]See A.08 for additional examples of abuse.

5.09 Because the determination of abuse is subjective, auditors are not required to detect abuse in examination engagements. However, as part of a GAGAS examination engagement, if auditors become aware of abuse that could be quantitatively or qualitatively material, auditors should apply procedures specifically directed to ascertain the potential effect on the subject matter, or the assertion thereon, or other data significant to the objective of the examination engagement. After performing additional work, auditors may discover that the abuse represents potential fraud or noncompliance with provisions of laws, regulations, contracts, or grant agreements.

5.10 Avoiding interference with investigations or legal proceedings is important in pursuing indications of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse. Laws, regulations, or policies may require auditors to report indications of certain types of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse to law enforcement or investigatory authorities before performing additional audit procedures. When investigations or legal proceedings are initiated or in process, auditors should evaluate the impact on the current examination engagement. In some cases, it may be appropriate for the auditors to work with investigators or legal authorities, or withdraw from or defer further work on the examination engagement or a portion of the examination engagement to avoid interfering with an ongoing investigation or legal proceeding.

Developing Elements of a Finding

5.11 In an examination engagement, findings may involve deficiencies in internal control; noncompliance with provisions of laws, regulations, contracts, or grant agreements; fraud; or abuse. As part of a GAGAS examination engagement, when auditors identify

findings, auditors should plan and perform procedures to develop the elements of the findings that are relevant and necessary to achieve the examination engagement objectives. The elements of a finding are discussed in paragraphs 5.12 through 5.15 below.

5.12 Criteria: The laws, regulations, contracts, grant agreements, standards, measures, expected performance, defined business practices, and benchmarks against which performance is compared or evaluated. Criteria identify the required or desired state or expectation with respect to the program or operation. Criteria provide a context for evaluating evidence and understanding the findings.

5.13 Condition: Condition is a situation that exists. The condition is determined and documented during the engagement.

5.14 Cause: The cause identifies the reason or explanation for the condition or the factor or factors responsible for the difference between the situation that exists (condition) and the required or desired state (criteria), which may also serve as a basis for recommendations for corrective actions. Common factors include poorly designed policies, procedures, or criteria; inconsistent, incomplete, or incorrect implementation; or factors beyond the control of program management. Auditors may assess whether the evidence provides a reasonable and convincing argument for why the stated cause is the key factor or factors contributing to the difference between the condition and the criteria.

5.15 Effect or potential effect: The effect is a clear, logical link to establish the impact or potential impact of the difference between the situation that exists (condition) and the required or desired state (criteria). The effect or potential effect identifies the outcomes or

consequences of the condition. When the engagement objectives include identifying the actual or potential consequences of a condition that varies (either positively or negatively) from the criteria identified in the engagement, "effect" is a measure of those consequences. Effect or potential effect may be used to demonstrate the need for corrective action in response to identified problems or relevant risks.

Examination Engagement Documentation

5.16 In addition to AICPA requirements for audit documentation,[86] auditors should comply with the following additional requirements when performing a GAGAS examination engagement.[87]

a. Prepare attest documentation in sufficient detail to enable an experienced auditor, having no previous connection to the examination engagement, to understand from the documentation the nature, timing, extent, and results of procedures performed and the evidence obtained and its source and the conclusions reached, including evidence that supports the auditors' significant judgments and conclusions. An experienced auditor means an individual (whether internal or external to the audit organization) who possesses the competencies and skills to be able to perform the examination engagement. These competencies and skills include an understanding of (1) examination engagement processes and related SSAEs,[88] (2) GAGAS and applicable legal and regulatory requirements, (3) the subject matter that the auditors are engaged to report on, (4) the suitability and

[86]See AICPA AT Section 101.100–101.107, *Attest Engagements.*

[87]See paragraphs 5.05, 5.07, 5.25, and 5.44 for additional documentation requirements regarding attestation engagements.

[88]See paragraphs 3.74 and 3.75 for additional discussion of qualifications for attestation engagements.

availability of criteria, and (5) issues related to the audited entity's environment.

b. Document supervisory review, before the date of the examination report, of the evidence that supports findings, conclusions, and recommendations contained in the examination report.

c. Document any departures from the GAGAS requirements and the impact on the engagement and on the auditors' conclusions when the examination engagement is not in compliance with applicable GAGAS requirements due to law, regulation, scope limitations, restrictions on access to records, or other issues impacting the audit. This applies to departures from unconditional requirements and from presumptively mandatory requirements when alternative procedures performed in the circumstances were not sufficient to achieve the objectives of the requirement.[89]

5.17 When performing GAGAS examination engagements and subject to applicable laws and regulations, auditors should make appropriate individuals, as well as attest documentation, available upon request and in a timely manner to other auditors or reviewers. Underlying GAGAS engagements is the premise that audit organizations in federal, state, and local governments and public accounting firms engaged to perform an engagement in accordance with GAGAS cooperate in performing examination engagements of programs of common interest so that auditors may use others' work and avoid duplication of efforts. The use of auditors' work by other auditors may be facilitated by contractual arrangements for GAGAS engagements

[89]See paragraph 2.15 for a definition of GAGAS requirements.

that provide for full and timely access to appropriate individuals, as well as attest documentation.

Additional GAGAS Reporting Requirements for Examination Engagements

5.18 In addition to the AICPA requirements for reporting on examination engagements,[90] auditors should comply with the following additional requirements when citing GAGAS in their examination reports. The additional reporting requirements relate to

a. reporting auditors' compliance with GAGAS;

b. reporting deficiencies in internal control, fraud, noncompliance with provisions of laws, regulations, contracts, and grant agreements, and abuse;

c. reporting views of responsible officials;

d. reporting confidential or sensitive information; and

e. distributing reports.[91]

Reporting Auditors' Compliance with GAGAS

5.19 When auditors comply with all applicable GAGAS requirements for examination engagements, they should include a statement in the examination report that they performed the examination engagement in accordance with GAGAS.[92] Because GAGAS incorporates by reference the AICPA's general attestation standard on criteria, the field work and reporting attestation standards, and the corresponding SSAEs, GAGAS does not require auditors to cite

[90]See AICPA AT Section 101.63-101.87, *Attest Engagements*.

[91]See paragraphs 5.19 through 5.44 for additional discussion of paragraph 5.18 a-e.

[92]See paragraphs 2.24 and 2.25 for additional requirements on citing compliance with GAGAS.

compliance with the AICPA standards when citing compliance with GAGAS. GAGAS does not prohibit auditors from issuing a separate report conforming only to the requirements of AICPA or other standards.[93]

Reporting Deficiencies in Internal Control, Fraud, Noncompliance with Provisions of Laws, Regulations, Contracts, and Grant Agreements, and Abuse

5.20 When performing GAGAS examination engagements, auditors should report, based upon the work performed, (1) significant deficiencies and material weaknesses in internal control;[94] (2) instances of fraud[95] and noncompliance with provisions of laws or regulations that have a material effect on the subject matter or an assertion about the subject matter and any other instances that warrant the attention of those charged with governance; (3) noncompliance with provisions of contracts or grant agreements that has a material effect on the subject matter or an assertion about the subject matter of the examination engagement; and (4) abuse that has a material effect on the subject matter or an assertion about the subject matter of the examination engagement. Auditors should include this information either in the same or in separate report(s).

5.21 If auditors report separately (including separate reports bound in the same document) on the items discussed in paragraph 5.20, they should state in the examination report that they are issuing those additional reports. They should include a reference to the separate reports and also state that the reports are an integral part of a GAGAS examination engagement.

[93]See AICPA AT Sections 101.85e, *Attest Engagements.*

[94]See paragraph A.06 for examples of deficiencies in internal control.

[95]See paragraph A.10 for examples of indicators of fraud risk.

Deficiencies in Internal Control

5.22 In addition to the AICPA requirements concerning internal control, [96] when performing GAGAS examination engagements, including attestation engagements related to internal control,[97] auditors should include in the examination report all deficiencies, even those communicated early,[98] that are considered to be significant deficiencies or material weaknesses.

5.23 Determining whether and how to communicate to officials of the audited entity internal control deficiencies that warrant the attention of those charged with governance, but are not considered significant deficiencies or material weaknesses, is a matter of professional judgment.

Fraud, Noncompliance with Provisions of Laws, Regulations, Contracts, and Grant Agreements, and Abuse

5.24 When performing a GAGAS examination engagement, and auditors conclude, based on sufficient, appropriate evidence, that any of the following either has occurred or is likely to have occurred, they should include in their examination report the relevant information about

a. fraud[99] and noncompliance with provisions of laws or regulations that have a material effect on the subject matter or an assertion about the subject matter and any other instances that warrant the attention of those charged with governance,

[96]See AICPA AT Section 101.52 through 101.53, *Attest Engagements*.

[97]See AICPA AT Section 501.07, *An Examination of an Entity's Internal Control Over Financial Reporting That Is Integrated With an Audit of Its Financial Statements*.

[98]See paragraph 5.47 for a discussion of early communication of deficiencies.

[99]See paragraph A.10 for examples of indicators of fraud risk.

b. noncompliance with provisions of contracts or grant agreements that has a material effect on the subject matter or an assertion about the subject matter, or

c. abuse[100] that is material to the subject matter or an assertion about the subject matter, either quantitatively or qualitatively.[101]

5.25 When auditors detect instances of noncompliance with provisions of contracts or grant agreements, or abuse that have an effect on the subject matter or an assertion about the subject matter that are less than material but warrant the attention of those charged with governance, they should communicate those findings in writing to audited entity officials. When auditors detect any instances of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that do not warrant the attention of those charged with governance, the auditors' determination of whether and how to communicate such instances to audited entity officials is a matter of professional judgment.

5.26 When fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse either have occurred or are likely to have occurred, auditors may consult with authorities or legal counsel about whether publicly reporting such information would compromise investigative or legal proceedings. Auditors may limit their public reporting to matters that would not compromise those proceedings and, for example, report only on information that is already a part of the public record.

[100]See paragraph A.08 for examples of abuse.

[101]See paragraphs 5.08 and 5.09 for a discussion of abuse.

Presenting Findings in the Examination Report

5.27 When performing a GAGAS examination engagement and presenting findings such as deficiencies in internal control, fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse, auditors should develop the elements of the findings to the extent necessary. Clearly developed findings, as discussed in paragraphs 5.11 through 5.15, assist management or oversight officials of the audited entity in understanding the need for taking corrective action, and assist auditors in making recommendations for corrective action. If auditors sufficiently develop the elements of a finding, they may provide recommendations for corrective action.

5.28 Auditors should place their findings in perspective by describing the nature and extent of the issues being reported and the extent of the work performed that resulted in the finding. To give the reader a basis for judging the prevalence and consequences of these findings, auditors should, as appropriate, relate the instances identified to the population or the number of cases examined and quantify the results in terms of dollar value or other measures. If the results cannot be projected, auditors should limit their conclusions appropriately.

Reporting Findings Directly to Parties Outside the Audited Entity

5.29 Auditors should report known or likely fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse directly to parties outside the audited entity in the following two circumstances.

a. When entity management fails to satisfy legal or regulatory requirements to report such information to external parties specified in law or regulation, auditors should first communicate the failure to report such information to those charged with governance. If the audited entity still does not report this information to the specified external parties as soon as practicable after

the auditors' communication with those charged with governance, then the auditors should report the information directly to the specified external parties.

b. When entity management fails to take timely and appropriate steps to respond to known or likely fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that (1) is likely to have a material effect on the subject matter or an assertion about the subject matter and (2) involves funding received directly or indirectly from a government agency, auditors should first report management's failure to take timely and appropriate steps to those charged with governance. If the audited entity still does not take timely and appropriate steps as soon as practicable after the auditors' communication with those charged with governance, then the auditors should report the entity's failure to take timely and appropriate steps directly to the funding agency.

5.30 The reporting in paragraph 5.29 is in addition to any legal requirements to report such information directly to parties outside the audited entity. Auditors should comply with these requirements even if they have resigned or been dismissed from the engagement prior to its completion.

5.31 Auditors should obtain sufficient, appropriate evidence, such as confirmation from outside parties, to corroborate assertions by management of the audited entity that it has reported such findings in accordance with laws, regulations, or funding agreements. When auditors are unable to do so, they should report such information directly as discussed in paragraph 5.29.

Reporting Views of Responsible Officials

5.32 When performing a GAGAS examination engagement, if the examination report discloses deficiencies in internal control, fraud, noncompliance

with provisions of laws, regulations, contracts, or grant agreements, or abuse, auditors should obtain and report the views of responsible officials of the audited entity concerning the findings, conclusions, and recommendations, as well as any planned corrective actions.

5.33 Providing a draft report with findings for review and comment by responsible officials of the audited entity and others helps the auditors develop a report that is fair, complete, and objective. Including the views of responsible officials results in a report that presents not only the auditors' findings, conclusions, and recommendations, but also the perspectives of the responsible officials of the audited entity and the corrective actions they plan to take. Obtaining the comments in writing is preferred, but oral comments are acceptable.

5.34 When auditors receive written comments from the responsible officials, they should include in their report a copy of the officials' written comments, or a summary of the comments received. When the responsible officials provide oral comments only, auditors should prepare a summary of the oral comments and provide a copy of the summary to the responsible officials to verify that the comments are accurately stated.

5.35 Auditors should also include in the report an evaluation of the comments, as appropriate. In cases in which the audited entity provides technical comments in addition to its written or oral comments on the report, auditors may disclose in the report that such comments were received.

5.36 Obtaining oral comments may be appropriate when, for example, there is a reporting date critical to meeting a user's needs; auditors have worked closely with the responsible officials throughout the work and

the parties are familiar with the findings and issues addressed in the draft report; or the auditors do not expect major disagreements with findings, conclusions, or recommendations in the draft report, or major controversies with regard to the issues discussed in the draft report.

5.37 When the audited entity's comments are inconsistent or in conflict with the findings, conclusions, or recommendations in the draft report, or when planned corrective actions do not adequately address the auditors' recommendations, the auditors should evaluate the validity of the audited entity's comments. If the auditors disagree with the comments, they should explain in the report their reasons for disagreement. Conversely, the auditors should modify their report as necessary if they find the comments valid and supported with sufficient, appropriate evidence.

5.38 If the audited entity refuses to provide comments or is unable to provide comments within a reasonable period of time, the auditors may issue the report without receiving comments from the audited entity. In such cases, the auditors should indicate in the report that the audited entity did not provide comments.

Reporting Confidential and Sensitive Information

5.39 When performing a GAGAS examination engagement, if certain pertinent information is prohibited from public disclosure or is excluded from a report due to the confidential or sensitive nature of the information, auditors should disclose in the report that certain information has been omitted and the reason or other circumstances that make the omission necessary.

5.40 Certain information may be classified or may be otherwise prohibited from general disclosure by federal, state, or local laws or regulations. In such circumstances, auditors may issue a separate classified

or limited use report containing such information and distribute the report only to persons authorized by law or regulation to receive it.

5.41 Additional circumstances associated with public safety, privacy, or security concerns could also justify the exclusion of certain information from a publicly available or widely distributed report. For example, detailed information related to computer security for a particular program may be excluded from publicly available reports because of the potential damage that could be caused by the misuse of this information. In such circumstances, auditors may issue a limited use report containing such information and distribute the report only to those parties responsible for acting on the auditors' recommendations. In some instances, it may be appropriate to issue both a publicly available report with the sensitive information excluded and a limited use report. The auditors may consult with legal counsel regarding any requirements or other circumstances that may necessitate the omission of certain information.

5.42 Considering the broad public interest in the program or activity under review assists auditors when deciding whether to exclude certain information from publicly available reports. When circumstances call for omission of certain information, auditors should evaluate whether this omission could distort the examination engagement results or conceal improper or illegal practices.

5.43 When audit organizations are subject to public records laws, auditors should determine whether public records laws could impact the availability of classified or limited use reports and determine whether other means of communicating with management and those charged with governance would be more appropriate. For example, the auditors may communicate general information in a written report and communicate

detailed information orally. The auditors may consult with legal counsel regarding applicable public records laws.

Distributing Reports

5.44 Distribution of reports completed in accordance with GAGAS depends on the relationship of the auditors to the audited organization and the nature of the information contained in the report. Auditors should document any limitation on report distribution.[102] The following discussion outlines distribution for reports completed in accordance with GAGAS:

a. Audit organizations in government entities should distribute reports to those charged with governance, to the appropriate audited entity officials, and to the appropriate oversight bodies or organizations requiring or arranging for the engagements. As appropriate, auditors should also distribute copies of the reports to other officials who have legal oversight authority or who may be responsible for acting on engagement findings and recommendations, and to others authorized to receive such reports.

b. Internal audit organizations in government entities may also follow the Institute of Internal Auditors (IIA) *International Standards for the Professional Practice of Internal Auditing*.[103] In accordance with GAGAS and IIA standards, the head of the internal audit organization should communicate results to the parties who can ensure that the results are given due consideration. If not otherwise mandated by statutory or regulatory

[102]See paragraphs 5.40 and 5.41 for discussion of limited use reports containing confidential or sensitive information.

[103]See paragraph 2.21 for additional discussion about using the IIA standards in conjunction with GAGAS and paragraph 2.22 for additional discussion about citing compliance with another set of standards.

requirements, prior to releasing results to parties outside the organization, the head of the internal audit organization should: (1) assess the potential risk to the organization, (2) consult with senior management or legal counsel as appropriate, and (3) control dissemination by indicating the intended users in the report.

c. Public accounting firms contracted to perform an examination engagement in accordance with GAGAS should clarify report distribution responsibilities with the engaging organization. If the contracting firm is responsible for the distribution, it should reach agreement with the party contracting for the engagement about which officials or organizations will receive the report and the steps being taken to make the report available to the public.

Additional GAGAS Considerations for Examination Engagements

5.45 Due to the objectives and public accountability of GAGAS examination engagements, additional considerations for examination engagements completed in accordance with GAGAS may apply. These considerations relate to

a. Materiality in GAGAS examination engagements, and

b. Early communication of deficiencies.[104]

Materiality in GAGAS Examination Engagements

5.46 The AICPA standards require that one of the factors to be considered when planning an attest engagement includes preliminary judgments about attestation risk and materiality for attest purposes.[105]

[104]See paragraphs 5.46 and 5.47 for additional discussion of paragraph 5.45 a-b.

[105]See AICPA AT Section 101.45b and 101.67, *Attest Engagements.*

Additional considerations may apply to GAGAS examination engagements of government entities or entities that receive government awards. For example, in engagements performed in accordance with GAGAS, auditors may find it appropriate to use lower materiality levels as compared with the materiality levels used in non-GAGAS engagements because of the public accountability of government entities and entities receiving government funding, various legal and regulatory requirements, and the visibility and sensitivity of government programs.

Early Communication of Deficiencies

5.47 For some matters, early communication to those charged with governance or management may be important because of the relative significance and the urgency for corrective follow-up action.[106] Further, when a control deficiency results in noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse, early communication is important to allow management to take prompt corrective action to prevent further noncompliance. When a deficiency is communicated early, the reporting requirements in paragraph 5.20 still apply.

[106]See AICPA AT Section 501.103, *An Examination of an Entity's Internal Control Over Financial Reporting That Is Integrated With an Audit of Its Financial Statements*.

Review Engagements

Additional GAGAS Field Work Requirements for Review Engagements

5.48 GAGAS establishes a field work requirement for review engagements in addition to the requirements contained in the AICPA standards. Auditors should comply with this additional requirement, along with the relevant AICPA standards for review engagements, when citing GAGAS in their review engagement reports. The additional requirement relates to communicating significant deficiencies, material weaknesses, instances of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that come to the auditors' attention during a review engagement.

Communicating Significant Deficiencies, Material Weaknesses, Instances of Fraud, Noncompliance with Provisions of Laws, Regulations, Contracts, and Grant Agreements, and Abuse

5.49 If, on the basis of conducting the procedures necessary to perform a review, significant deficiencies; material weaknesses; instances of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements; or abuse come to the auditors' attention that warrant the attention of those charged with governance, GAGAS requires that auditors should communicate such matters to audited entity officials. When auditors detect any instances of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that do not warrant the attention of those charged with governance, the auditors' determination of whether and how to communicate such instances to audited entity officials is a matter of professional judgment. Additionally, auditors should determine whether the existence of such matters affects the auditors' ability to conduct or report on the review.

Additional GAGAS Reporting Requirements for Review Engagements

5.50 GAGAS establishes reporting requirements for review engagements in addition to the requirements contained in the AICPA standards.[107] Auditors should comply with these additional requirements when citing GAGAS in their review engagement reports. The additional requirements relate to

a. reporting auditors' compliance with GAGAS; and

b. distributing reports.[108]

Reporting Auditors' Compliance with GAGAS

5.51 When auditors comply with all applicable requirements for a review engagement conducted in accordance with GAGAS, they should include a statement in the review report that they performed the engagement in accordance with GAGAS.[109] Because GAGAS incorporates by reference the general standard on criteria, and the field work and reporting standards of the AICPA SSAEs, GAGAS does not require auditors to cite compliance with the AICPA standards when citing compliance with GAGAS. GAGAS does not prohibit auditors from issuing a separate report conforming only to the requirements of AICPA or other standards.[110]

Distributing Reports

5.52 Distribution of reports completed in accordance with GAGAS depends on the relationship of the auditors to the audited organization and the nature of the

[107]See AICPA AT Section 101.63-101.83 and 101.88-101.90, *Attest Engagements*.

[108]See paragraphs 5.51 and 5.52 for additional discussion of paragraph 5.50 a-b.

[109]See paragraphs 2.24 and 2.25 for additional requirements on citing compliance with GAGAS.

[110]See AICPA AT Section 101.89d, *Attest Engagements.*

information contained in the report. For GAGAS review engagements, if the subject matter or the assertion involves material that is classified for security purposes or contains confidential or sensitive information, auditors should limit the report distribution. Auditors should document any limitation on report distribution. The following discussion outlines distribution for reports completed in accordance with GAGAS:

a. Audit organizations in government entities should distribute reports to those charged with governance, to the appropriate audited entity officials, and to the appropriate oversight bodies or organizations requiring or arranging for the engagements. As appropriate, auditors should also distribute copies of the reports to other officials who have legal oversight authority, and to others authorized to receive such reports.

b. Internal audit organizations in government entities may also follow the Institute of Internal Auditors (IIA) *International Standards for the Professional Practice of Internal Auditing*.[111] In accordance with GAGAS and IIA standards, the head of the internal audit organization should communicate results to the parties who can ensure that the results are given due consideration. If not otherwise mandated by statutory or regulatory requirements, prior to releasing results to parties outside the organization, the head of the internal audit organization should: (1) assess the potential risk to the organization, (2) consult with senior management or legal counsel as appropriate, and (3) control dissemination by indicating the intended users in the report.

[111]See paragraph 2.21 for additional discussion about using the IIA standards in conjunction with GAGAS and paragraph 2.22 for additional discussion about citing compliance with another set of standards.

c. Public accounting firms contracted to perform a review engagement in accordance with GAGAS should clarify report distribution responsibilities with the engaging organization. If the contracting firm is responsible for the distribution, it should reach agreement with the party contracting for the engagement about which officials or organizations will receive the report and the steps being taken to make the report available to the public.

Additional GAGAS Considerations for Review Engagements

5.53 Due to the objectives and public accountability of GAGAS review engagements, additional considerations for review engagements performed in accordance with GAGAS may apply. These considerations relate to

a. establishing an understanding regarding services to be performed; and

b. reporting on review engagements.[112]

Establishing an Understanding Regarding Services to be Performed

5.54 The AICPA standards require auditors to establish an understanding with the audited entity (client) regarding the services to be performed for each attestation engagement. Such an understanding reduces the risk that either the auditors (practitioner) or the audited entity may misinterpret the needs or expectations of the other party. The understanding includes the objectives of the engagement, responsibilities of entity management, responsibilities of auditors, and limitations of the engagement.[113]

[112]See paragraphs 5.54 through 5.57 for additional discussion of 5.53 a-b.

[113]See AICPA AT Section 101.46, *Attest Engagements*.

5.55 Auditors often perform GAGAS engagements under a contract with a party other than the officials of the audited entity or pursuant to a third-party request. In such cases, auditors may also find it appropriate to communicate information regarding the services to be performed to the individuals contracting for or requesting the engagement. Such an understanding can help auditors avoid any misunderstandings regarding the nature of the review engagement. For example, review engagements only provide a moderate level of assurance expressed as a conclusion in the form of negative assurance, and, as a result, auditors do not perform sufficient work to be able to develop elements of a finding or provide recommendations that are common in other types of GAGAS engagements. Under such circumstances, for example, requesting parties may find that a different type of attestation engagement or a performance audit may provide the appropriate level of assurance to meet their needs.

Reporting on Review Engagements

5.56 The AICPA standards require that the auditors' review report be in the form of a conclusion expressed in the form of negative assurance.[114]

5.57 Because reviews are substantially less in scope than audits and examination engagements, it is important to include all required reporting elements contained in the SSAEs.[115] For example, a required element of the review report is a statement that a review engagement is substantially less in scope than an examination, the objective of which is an expression of opinion on the subject matter, and accordingly, review reports express no such opinion. Including only those elements that the AICPA reporting standards for review

[114]See AICPA AT Section 101.68, *Attest Engagements*.

[115]See AICPA AT Section 101.89, *Attest Engagements.*

engagements require or permit ensures that auditors comply with the AICPA standards and that users of GAGAS reports have an understanding of the nature of the work performed and the results of the review engagement.

Agreed-Upon Procedures Engagements

Additional GAGAS Field Work Requirements for Agreed-Upon Procedures Engagements

5.58 GAGAS establishes a field work requirement for agreed-upon procedures engagements in addition to the requirements contained in the AICPA standards. Auditors should comply with this additional requirement, along with the relevant AICPA standards for agreed-upon procedures engagements, when citing GAGAS in their agreed-upon procedures engagement reports. The additional requirement relates to communicating significant deficiencies, material weaknesses, instances of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that comes to the auditors' attention during an agreed-upon procedures engagement.

Communicating Significant Deficiencies, Material Weaknesses, Instances of Fraud, Noncompliance with Provisions of Laws, Regulations, Contracts, and Grant Agreements, and Abuse

5.59 If, on the basis of conducting the procedures necessary to perform an agreed-upon procedures engagement,[116] significant deficiencies, material weaknesses, instances of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse come to the auditors' attention that warrant the attention of those charged with governance, GAGAS requires that auditors should communicate such matters to audited entity officials. When auditors detect any instances of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that do not warrant the attention of those charged with governance, the auditors' determination of whether and how to communicate such instances to audited entity officials is a matter of professional judgment. Additionally, auditors should determine whether the existence of such matters affects the auditors' ability to conduct or report on the agreed-upon procedures engagement.

Additional GAGAS Reporting Requirements for Agreed-Upon Procedures Engagements

5.60 GAGAS establishes reporting requirements for agreed-upon procedures engagements in addition to the requirements contained in the AICPA standards.[117] Auditors should comply with these additional requirements when citing GAGAS in their agreed-upon procedures engagement reports. The additional requirements relate to

a. reporting auditors' compliance with GAGAS; and

[116]See AICPA AT Section 201.03, *Agreed-Upon Procedures Engagements*.

[117]See AICPA AT Section 201.31-201.36, *Agreed-Upon Procedures Engagements*.

b. distributing reports.[118]

Reporting Auditors' Compliance with GAGAS

5.61 When auditors comply with all applicable GAGAS requirements for agreed-upon procedures engagements, they should include a statement in the agreed-upon procedures engagement report that they performed the engagement in accordance with GAGAS.[119] Because GAGAS incorporates by reference the AICPA's general attestation standard on criteria, the field work and reporting attestation standards, and the corresponding SSAEs, GAGAS does not require auditors to cite compliance with the AICPA standards when citing compliance with GAGAS. GAGAS does not prohibit auditors from issuing a separate report conforming only to the requirements of AICPA or other standards.[120]

Distributing Reports

5.62 Distribution of reports completed in accordance with GAGAS depends on the relationship of the auditors to the audited organization and the nature of the information contained in the report. For GAGAS agreed-upon procedures engagements, if the subject matter or the assertion involves material that is classified for security purposes or contains confidential or sensitive information, auditors should limit the report distribution. Auditors should document any limitation on report distribution. The following discussion outlines distribution for reports completed in accordance with GAGAS:

[118]See paragraphs 5.61 and 5.62 for additional discussion of paragraph 5.60 a-b.

[119]See paragraphs 2.24 and 2.25 for additional requirements on citing compliance with GAGAS.

[120]See AICPA AT Section 201.31 g, *Agreed-Upon Procedures Engagements.*

a. Audit organizations in government entities should distribute reports to those charged with governance, to the appropriate audited entity officials, and to the appropriate oversight bodies or organizations requiring or arranging for the engagements. As appropriate, auditors should also distribute copies of the reports to other officials who have legal oversight authority, and to others authorized to receive such reports.

b. Internal audit organizations in government entities may also follow the Institute of Internal Auditors (IIA) *International Standards for the Professional Practice of Internal Auditing*.[121] In accordance with GAGAS and IIA standards, the head of the internal audit organization should communicate results to the parties who can ensure that the results are given due consideration. If not otherwise mandated by statutory or regulatory requirements, prior to releasing results to parties outside the organization, the head of the internal audit organization should: (1) assess the potential risk to the organization, (2) consult with senior management or legal counsel as appropriate, and (3) control dissemination by indicating the intended users in the report.

c. Public accounting firms contracted to perform an agreed-upon procedures engagement in accordance with GAGAS should clarify report distribution responsibilities with the engaging organization. If the contracting firm is responsible for the distribution, it should reach agreement with the party contracting for the engagement about which officials or organizations will receive the report and the steps being taken to make the report available to the public.

[121]See paragraph 2.21 for additional discussion about using the IIA standards in conjunction with GAGAS and paragraph 2.22 for additional discussion about citing compliance with another set of standards.

Additional GAGAS Considerations for Agreed-Upon Procedures Engagements

5.63 Due to the objectives and public accountability of GAGAS agreed-upon procedures engagements, additional considerations for agreed-upon procedures engagements performed in accordance with GAGAS may apply. These considerations relate to

a. establishing an understanding regarding services to be performed; and

b. reporting on agreed-upon procedures engagements.[122]

Establishing an Understanding Regarding Services to be Performed

5.64 The AICPA standards require auditors to establish an understanding with the audited entity (client) regarding the services to be performed for each attestation engagement. Such an understanding reduces the risk that either the auditors (practitioner) or the audited entity may misinterpret the needs or expectations of the other party. The understanding includes the objectives of the engagement, responsibilities of entity management, responsibilities of auditors, and limitations of the engagement.[123]

5.65 Auditors often perform GAGAS engagements under a contract with a party other than the officials of the audited entity or pursuant to a third-party request. In such cases, auditors may also find it appropriate to communicate information regarding the services to be performed to the individuals contracting for or requesting the engagement. Such an understanding can help auditors avoid any misunderstandings regarding the nature of the agreed-upon procedures

[122]See paragraphs 5.64 through 5.67 for additional discussion of paragraph 5.63 a-b.

[123]See AICPA AT Sections 101.46, *Attest Engagements,* and 201.10, *Agreed-Upon Procedures Engagements*.

engagement. For example, agreed-upon procedures engagements provide neither a high nor moderate level of assurance, and, as a result, auditors do not perform sufficient work to be able to develop elements of a finding or provide recommendations that are common in other types of GAGAS engagements. Under such circumstances, for example, requesting parties may find that a different type of attestation engagement or a performance audit may provide the appropriate level of assurance to meet their needs.

Reporting on Agreed-Upon Procedures Engagements

5.66 The AICPA standards require that the auditors' report on agreed-upon procedures engagements be in the form of procedures and findings and specifies the required elements to be contained in the report.[124]

5.67 Because GAGAS agreed-upon procedures engagements are substantially less in scope than audits and examination engagements, it is important not to deviate from the required reporting elements contained in the SSAEs. For example, a required element of the report on agreed-upon procedures is a statement that the auditors were not engaged to and did not conduct an examination or a review of the subject matter, the objectives of which would be the expression of an opinion or limited assurance and that if the auditors had performed additional procedures, other matters might have come to their attention that would have been reported.[125] Another required element is a statement that the sufficiency of the procedures is solely the responsibility of the specified parties and a disclaimer of

[124]See AICPA AT Section 201.31, *Agreed-Upon Procedures Engagements*.

[125]See AICPA AT Section 201.31k, *Agreed-Upon Procedures Engagements*.

responsibility for the sufficiency of those procedures.[126] Including only those elements that the AICPA reporting standards for agreed-upon procedure engagements require or permit ensures that auditors comply with the AICPA standards and that users of GAGAS reports have an understanding of the nature of the work performed and the results of the agreed-upon procedures engagement.

[126]See AICPA AT Section 201.31h and 201.11-201.14, *Agreed-Upon Procedures Engagements*.

Field Work Standards for Performance Audits

Introduction

6.01 This chapter contains field work requirements and guidance for performance audits conducted in accordance with generally accepted government auditing standards (GAGAS). The purpose of field work requirements is to establish an overall approach for auditors to apply in obtaining reasonable assurance that the evidence is sufficient and appropriate to support the auditors' findings and conclusions. The field work requirements for performance audits relate to planning the audit; supervising staff; obtaining sufficient, appropriate evidence; and preparing audit documentation. The concepts of reasonable assurance, significance, and audit risk form a framework for applying these requirements and are included throughout the discussion of performance audits.

6.02 For performance audits conducted in accordance with GAGAS, the requirements and guidance in chapters 1 through 3, 6, and 7 apply.

Reasonable Assurance

6.03 In performance audits that comply with GAGAS, auditors obtain reasonable assurance that evidence is sufficient and appropriate to support the auditors' findings and conclusions in relation to the audit objectives.[127] Thus, the sufficiency and appropriateness of evidence needed and tests of evidence will vary based on the audit objectives, findings, and conclusions. Objectives for performance audits range from narrow to broad and involve varying types and quality of evidence. In some engagements, sufficient, appropriate evidence is available, but in others, information may have limitations. Professional judgment assists auditors in determining the audit scope and methodology needed to address the audit objectives,

[127]See paragraphs 2.11 and A2.02 for additional discussion of performance audit objectives.

and in evaluating whether sufficient, appropriate evidence has been obtained to address the audit objectives.

Significance in a Performance Audit

6.04 The concept of significance assists auditors throughout a performance audit, including when deciding the type and extent of audit work to perform, when evaluating results of audit work, and when developing the report and related findings and conclusions. Significance is defined as the relative importance of a matter within the context in which it is being considered, including quantitative and qualitative factors. Such factors include the magnitude of the matter in relation to the subject matter of the audit, the nature and effect of the matter, the relevance of the matter, the needs and interests of an objective third party with knowledge of the relevant information, and the impact of the matter to the audited program or activity. Professional judgment assists auditors when evaluating the significance of matters within the context of the audit objectives. In the performance audit requirements, the term “significant” is comparable to the term “material” as used in the context of financial statement engagements.

Audit Risk

6.05 Audit risk is the possibility that the auditors’ findings, conclusions, recommendations, or assurance may be improper or incomplete, as a result of factors such as evidence that is not sufficient and/or appropriate, an inadequate audit process, or intentional omissions or misleading information due to misrepresentation or fraud. The assessment of audit risk involves both qualitative and quantitative considerations. Factors impacting audit risk include the time frames, complexity, or sensitivity of the work; size of the program in terms of dollar amounts and number of citizens served; adequacy of the audited entity’s

systems and processes to detect inconsistencies, significant errors, or fraud; and auditors' access to records. Audit risk includes the risk that auditors will not detect a mistake, inconsistency, significant error, or fraud in the evidence supporting the audit. Audit risk can be reduced by taking actions such as increasing the scope of work; adding specialists, additional reviewers, and other resources to perform the audit; changing the methodology to obtain additional evidence, higher quality evidence, or alternative forms of corroborating evidence; or aligning the findings and conclusions to reflect the evidence obtained.

Planning

6.06 Auditors must adequately plan and document the planning of the work necessary to address the audit objectives.

6.07 Auditors must plan the audit to reduce audit risk to an appropriate level for the auditors to obtain reasonable assurance that the evidence is sufficient and appropriate[128] to support the auditors' findings and conclusions. This determination is a matter of professional judgment. In planning the audit, auditors should assess significance and audit risk and apply these assessments in defining the audit objectives and the scope and methodology to address those objectives. Planning is a continuous process throughout the audit. Therefore, auditors may need to adjust the audit objectives, scope, and methodology as work is being completed. In situations where the audit objectives are established by statute or legislative oversight, auditors may not have latitude to define or adjust the audit objectives or scope.

[128]See paragraphs 6.56 through 6.72 for a discussion about assessing the sufficiency and appropriateness of evidence.

6.08 The objectives are what the audit is intended to accomplish. They identify the audit subject matter and performance aspects to be included, and may also include the potential findings and reporting elements that the auditors expect to develop. Audit objectives can be thought of as questions about the program that the auditors seek to answer based on evidence obtained and assessed against criteria. The term “program” is used in GAGAS to include government entities, organizations, programs, activities, and functions.

6.09 Scope is the boundary of the audit and is directly tied to the audit objectives. The scope defines the subject matter that the auditors will assess and report on, such as a particular program or aspect of a program, the necessary documents or records, the period of time reviewed, and the locations that will be included.

6.10 The methodology describes the nature and extent of audit procedures for gathering and analyzing evidence to address the audit objectives. Audit procedures are the specific steps and tests auditors perform to address the audit objectives. Auditors should design the methodology to obtain reasonable assurance that the evidence is sufficient and appropriate to support the auditors’ findings and conclusions in relation to the audit objectives and to reduce audit risk to an acceptable level.

6.11 Auditors should assess audit risk and significance within the context of the audit objectives by gaining an understanding of the following:

a. the nature and profile of the programs and the needs of potential users of the audit report;

b. internal control as it relates to the specific objectives and scope of the audit;

c. information systems controls for purposes of assessing audit risk and planning the audit within the context of the audit objectives;

d. provisions of laws, regulations, contracts, and grant agreements, and potential fraud, and abuse that are significant within the context of the audit objectives;

e. ongoing investigations or legal proceedings within the context of the audit objectives; and

f. the results of previous audits and attestation engagements that directly relate to the current audit objectives.[129]

6.12 During planning, auditors should also

a. identify the potential criteria needed to evaluate matters subject to audit;

b. identify sources of audit evidence and determine the amount and type of evidence needed given audit risk and significance;

c. evaluate whether to use the work of other auditors and specialists to address some of the audit objectives;

d. assign sufficient staff and specialists with adequate collective professional competence and identify other resources needed to perform the audit;

e. communicate about planning and performance of the audit to management officials, those charged with governance, and others as applicable; and

[129]See paragraphs 6.13 through 6.36 for additional discussion of 6.11 a-f.

f. prepare a written audit plan.[130]

Nature and Profile of the Program and User Needs

6.13 Auditors should obtain an understanding of the nature of the program or program component under audit and the potential use that will be made of the audit results or report as they plan a performance audit. The nature and profile of a program include

a. visibility, sensitivity, and relevant risks associated with the program under audit;

b. age of the program or changes in its conditions;

c. the size of the program in terms of total dollars, number of citizens affected, or other measures;

d. level and extent of review or other forms of independent oversight;

e. program's strategic plan and objectives; and

f. external factors or conditions that could directly affect the program.

6.14 One group of users of the auditors' report is government officials who may have authorized or requested the audit. Other important users of the auditors' report are the audited entity, those responsible for acting on the auditors' recommendations, oversight organizations, and legislative bodies. Other potential users of the auditors' report include government legislators or officials (other than those who may have authorized or requested the audit), the media, interest groups, and individual citizens. In addition to an interest

[130]See paragraphs 6.37 through 6.52 for additional discussion of 6.12 a-f.

in the program, potential users may have an ability to influence the conduct of the program. An awareness of these potential users' interests and influence can help auditors judge whether possible findings could be significant to relevant users.

6.15 Obtaining an understanding of the program under audit helps auditors to assess the relevant risks associated with the program and the impact of the risks on the audit objectives, scope, and methodology. The auditors' understanding may come from knowledge they already have about the program or knowledge they gain from inquiries, observations, and reviewing documents while planning the audit. The extent and breadth of those inquiries and observations will vary among audits based on the audit objectives, as will the need to understand individual aspects of the program, such as the following:

a. Provisions of laws, regulations, contracts and grant agreements: Government programs are usually created by law and are subject to specific laws and regulations. Laws and regulations usually set forth what is to be done, who is to do it, the purpose to be achieved, the population to be served, and related funding guidelines or restrictions. Government programs may also be subject to contracts or grant agreements. Thus, understanding the laws and legislative history establishing a program and the provisions of any contracts or grant agreements is essential to understanding the program itself. Obtaining that understanding is also a necessary step in identifying the provisions of laws, regulations, contracts, or grant agreements that are significant within the context of the audit objectives.

b. Purpose and goals: Purpose is the result or effect that is intended or desired from a program's operation. Legislatures usually establish the program's purpose

when they provide authority for the program. Entity officials may provide more detailed information on the program's purpose to supplement the authorizing legislation. Entity officials are sometimes asked to set goals for program performance and operations, including both output and outcome goals. Auditors may use the stated program purpose and goals as criteria for assessing program performance or may develop additional criteria to use when assessing performance.

c. Internal control: Internal control, sometimes referred to as management control, in the broadest sense includes the plan, policies, methods, and procedures adopted by management to meet its missions, goals, and objectives. Internal control includes the processes for planning, organizing, directing, and controlling program operations. It includes the systems for measuring, reporting, and monitoring program performance. Internal control serves as a defense in safeguarding assets and in preventing and detecting errors; fraud; noncompliance with provisions of laws, regulations, contracts or grant agreements; or abuse.[131]

d. Inputs: Inputs are the amount of resources (in terms of money, material, personnel, etc.) that are put into a program. These resources may come from within or outside the entity operating the program. Measures of inputs can have a number of dimensions, such as cost, timing, and quality. Examples of measures of inputs are dollars spent, employee-hours expended, and square feet of building space.

e. Program operations: Program operations are the strategies, processes, and activities management uses

[131]See paragraphs 6.16 through 6.27 for guidance pertaining to internal control.

to convert inputs into outputs. Program operations may be subject to internal control.

f. Outputs: Outputs represent the quantity of goods or services produced by a program. For example, an output measure for a job training program could be the number of persons completing training, and an output measure for an aviation safety inspection program could be the number of safety inspections completed.

g. Outcomes: Outcomes are accomplishments or results of a program. For example, an outcome measure for a job training program could be the percentage of trained persons obtaining a job and still in the work place after a specified period of time. An example of an outcome measure for an aviation safety inspection program could be the percentage reduction in safety problems found in subsequent inspections or the percentage of problems deemed corrected in follow-up inspections. Such outcome measures show the progress made in achieving the stated program purpose of helping unemployable citizens obtain and retain jobs, and improving the safety of aviation operations. Outcomes may be influenced by cultural, economic, physical, or technological factors outside the program. Auditors may use approaches drawn from other disciplines, such as program evaluation, to isolate the effects of the program from these other influences. Outcomes also include unexpected and/or unintentional effects of a program, both positive and negative.

Internal Control

6.16 Auditors should obtain an understanding of internal control[132] that is significant within the context of the audit objectives. For internal control that is significant within the context of the audit objectives, auditors should assess whether internal control has been properly designed and implemented and should perform procedures designed to obtain sufficient, appropriate evidence to support their assessment about the effectiveness of those controls. Information systems controls are often an integral part of an entity's internal control. The effectiveness of significant internal controls is frequently dependent on the effectiveness of information systems controls. Thus, when obtaining an understanding of internal control significant to the audit objectives, auditors should also determine whether it is necessary to evaluate information systems controls.[133]

6.17 The effectiveness of internal control that is significant within the context of the audit objectives can affect audit risk. Consequently, auditors may determine that it is necessary to modify the nature, timing, or extent of the audit procedures based on the auditors' assessment of internal control and the results of internal control testing. For example, poorly controlled aspects of a program have a higher risk of failure, so auditors may choose to focus more efforts in these areas. Conversely, effective controls at the audited entity may enable the auditors to limit the extent and type of audit testing needed.

6.18 Auditors may obtain an understanding of internal control through inquiries, observations, inspection of documents and records, review of other auditors'

[132]See paragraphs A.03 and A.04 for additional discussion on internal control.

[133]See paragraphs 6.23 through 6.27 for additional discussion on evaluating the effectiveness of information systems controls.

reports, or direct tests. The nature and extent of procedures auditors perform to obtain an understanding of internal control may vary among audits based on audit objectives, audit risk, known or potential internal control deficiencies, and the auditors' knowledge about internal control gained in prior audits.

6.19 The following discussion of the principal types of internal control objectives is intended to help auditors better understand internal controls and determine whether or to what extent they are significant to the audit objectives.

a. Effectiveness and efficiency of program operations: Controls over program operations include policies and procedures that the audited entity has implemented to provide reasonable assurance that a program meets its objectives, while considering cost-effectiveness and efficiency. Understanding these controls can help auditors understand the program operations that convert inputs to outputs and outcomes.

b. Relevance and reliability of information: Controls over the relevance and reliability of information include policies and procedures that officials of the audited entity have implemented to provide themselves reasonable assurance that operational and financial information they use for decision making and reporting externally is relevant and reliable and fairly disclosed in reports. Understanding these controls can help auditors (1) assess the risk that the information gathered by the entity may not be relevant or reliable and (2) design appropriate tests of the information considering the audit objectives.

c. Compliance with applicable laws, regulations, contracts, and grant agreements: Controls over compliance include policies and procedures that the audited entity has implemented to provide reasonable

assurance that program implementation is in accordance with provisions of laws, regulations, contracts, and grant agreements. Understanding the relevant controls concerning compliance with those laws, regulations, contracts or grant agreements that the auditors have determined are significant within the context of the audit objectives can help them assess the risk of noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse.

6.20 A subset of these categories of internal control objectives is the safeguarding of assets and resources. Controls over the safeguarding of assets and resources include policies and procedures that the audited entity has implemented to reasonably prevent or promptly detect unauthorized acquisition, use, or disposition of assets and resources.

6.21 In performance audits, a deficiency in internal control[134] exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct (1) impairments of effectiveness or efficiency of operations, (2) misstatements in financial or performance information, or (3) noncompliance with provisions of laws, regulations, contracts, or grant agreements on a timely basis. A deficiency in design exists when (a) a control necessary to meet the control objective is missing or (b) an existing control is not properly designed so that, even if the control operates as designed, the control objective is not met. A deficiency in operation exists when a properly designed control does not operate as designed, or when the person performing the control does not possess the

[134]See paragraph A.05 for additional discussion of internal control deficiencies.

necessary authority or qualifications to perform the control effectively.

6.22 Internal auditing is an important part of overall governance, accountability, and internal control. A key role of many internal audit organizations is to provide assurance that internal controls are in place to adequately mitigate risks and achieve program goals and objectives. The auditor may determine that it is appropriate to use the work of the internal auditors in the auditor's assessment of the effectiveness of design or operation of internal controls that are significant within the context of the audit objectives.[135]

Information Systems Controls

6.23 Understanding information systems controls is important when information systems are used extensively throughout the program under audit and the fundamental business processes related to the audit objectives rely on information systems. Information systems controls consist of those internal controls that are dependent on information systems processing and include general controls, application controls, and user controls.

a. Information systems general controls (entitywide, system, and application levels) are the policies and procedures that apply to all or a large segment of an entity's information systems. General controls help ensure the proper operation of information systems by creating the environment for proper operation of application controls. General controls include security management, logical and physical access, configuration management, segregation of duties, and contingency planning.

[135]See paragraphs 6.40 through 6.44 for standards and guidance for using the work of other auditors.

b. Application controls, sometimes referred to as business process controls, are those controls that are incorporated directly into computer applications to help ensure the validity, completeness, accuracy, and confidentiality of transactions and data during application processing. Application controls include controls over input, processing, output, master file, interface, and data management system controls.

c. User controls are portions of controls that are performed by people interacting with information system controls. A user control is an information system control if its effectiveness depends on information systems processing or the reliability (accuracy, completeness, and validity) of information processed by information systems.

6.24 An organization's use of information systems controls may be extensive; however, auditors are primarily interested in those information systems controls that are significant to the audit objectives. Information systems controls are significant to the audit objectives if auditors determine that it is necessary to evaluate the effectiveness of information systems controls in order to obtain sufficient, appropriate evidence. When information systems controls are determined to be significant to the audit objectives or when the effectiveness of significant controls is dependent on the effectiveness of information systems controls, auditors should then evaluate the design and operating effectiveness of such controls. This evaluation would include other information systems controls that impact the effectiveness of the significant controls or the reliability of information used in performing the significant controls. Auditors should obtain a sufficient understanding of information systems

controls necessary to assess audit risk and plan the audit within the context of the audit objectives.[136]

6.25 Audit procedures to evaluate the effectiveness of significant information systems controls include (1) gaining an understanding of the system as it relates to the information and (2) identifying and evaluating the general, application, and user controls that are critical to providing assurance over the reliability of the information required for the audit.

6.26 The evaluation of information systems controls may be done in conjunction with the auditors' consideration of internal control within the context of the audit objectives[137] or as a separate audit objective or audit procedure, depending on the objectives of the audit. Depending on the significance of information systems controls to the audit objectives, the extent of audit procedures to obtain such an understanding may be limited or extensive. In addition, the nature and extent of audit risk related to information systems controls are affected by the nature of the hardware and software used, the configuration of the entity's systems and networks, and the entity's information systems strategy.

6.27 Auditors should determine which audit procedures related to information systems controls are needed to obtain sufficient, appropriate evidence to support the audit findings and conclusions. The following factors may assist auditors in making this determination:

[136]Refer to additional criteria and guidance in *Federal Information System Controls Audit Manual* (FISCAM), GAO-09-232G (Washington, D.C.: February 2009) and *IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals*, published by ISACA.

[137]See paragraphs 6.16 through 6.22 for additional discussion on internal control.

a. The extent to which internal controls that are significant to the audit depend on the reliability of information processed or generated by information systems.

b. The availability of evidence outside the information system to support the findings and conclusions: It may not be possible for auditors to obtain sufficient, appropriate evidence without evaluating the effectiveness of relevant information systems controls. For example, if information supporting the findings and conclusions is generated by information systems or its reliability is dependent on information systems controls, there may not be sufficient supporting or corroborating information or documentary evidence that is available other than that produced by the information systems.

c. The relationship of information systems controls to data reliability: To obtain evidence about the reliability of computer-generated information, auditors may decide to evaluate the effectiveness of information systems controls as part of obtaining evidence about the reliability of the data. If the auditor concludes that information systems controls are effective, the auditor may reduce the extent of direct testing of data.

d. Evaluating the effectiveness of information systems controls as an audit objective: When evaluating the effectiveness of information systems controls is directly a part of an audit objective, auditors should test information systems controls necessary to address the audit objectives. For example, the audit may involve the effectiveness of information systems controls related to certain systems, facilities, or organizations.

Provisions of Laws, Regulations, Contracts, and Grant Agreements, Fraud, and Abuse

Provisions of Laws, Regulations, Contracts, and Grant Agreements

6.28 Auditors should identify any provisions of laws, regulations, contracts or grant agreements that are significant within the context of the audit objectives and assess the risk that noncompliance with provisions of laws, regulations, contracts or grant agreements could occur.[138] Based on that risk assessment, the auditors should design and perform procedures to obtain reasonable assurance of detecting instances of noncompliance with provisions of laws, regulations, contracts, or grant agreements that are significant within the context of the audit objectives.

6.29 The auditors' assessment of audit risk may be affected by such factors as the complexity or newness of the laws, regulations, contracts or grant agreements. The auditors' assessment of audit risk also may be affected by whether the entity has controls that are effective in preventing or detecting noncompliance with provisions of laws, regulations, contracts, or grant agreements. If auditors obtain sufficient, appropriate evidence of the effectiveness of these controls, they can reduce the extent of their tests of compliance.

Fraud

6.30 In planning the audit, auditors should assess risks of fraud occurring that is significant within the context of the audit objectives.[139] Fraud involves obtaining something of value through willful misrepresentation.

[138]See paragraphs A.11 through A.13 for additional discussion on the significance of provisions of laws, regulations, contracts, or grant agreements.

[139]See paragraph A.10 for examples of indicators of fraud risk.

Whether an act is, in fact, fraud is a determination to be made through the judicial or other adjudicative system and is beyond auditors' professional responsibility. Audit team members should discuss among the team fraud risks, including factors such as individuals' incentives or pressures to commit fraud, the opportunity for fraud to occur, and rationalizations or attitudes that could allow individuals to commit fraud. Auditors should gather and assess information to identify risks of fraud that are significant within the scope of the audit objectives or that could affect the findings and conclusions. For example, auditors may obtain information through discussion with officials of the audited entity or through other means to determine the susceptibility of the program to fraud, the status of internal controls the audited entity has established to prevent and detect fraud, or the risk that officials of the audited entity could override internal control. An attitude of professional skepticism in assessing these risks assists auditors in assessing which factors or risks could significantly affect the audit objectives.

6.31 When auditors identify factors or risks related to fraud that has occurred or is likely to have occurred that they believe are significant within the context of the audit objectives, they should design procedures to obtain reasonable assurance of detecting any such fraud. Assessing the risk of fraud is an ongoing process throughout the audit and relates not only to planning the audit but also to evaluating evidence obtained during the audit.

6.32 When information comes to the auditors' attention indicating that fraud, significant within the context of the audit objectives, may have occurred, auditors should extend the audit steps and procedures, as necessary, to (1) determine whether fraud has likely occurred and (2) if so, determine its effect on the audit findings. If the fraud that may have occurred is not significant within the context of the audit objectives, the auditors may

conduct additional audit work as a separate engagement, or refer the matter to other parties with oversight responsibility or jurisdiction.

Abuse

6.33 Abuse involves behavior that is deficient or improper when compared with behavior that a prudent person would consider reasonable and necessary business practice given the facts and circumstances. Abuse also includes misuse of authority or position for personal financial interests or those of an immediate or close family member or business associate.[140] Abuse does not necessarily involve fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements.

6.34 Because the determination of abuse is subjective, auditors are not required to detect abuse in performance audits. However, as part of a GAGAS audit, if auditors become aware of abuse that could be quantitatively or qualitatively significant to the program under audit, auditors should apply audit procedures specifically directed to ascertain the potential effect on the program under audit within the context of the audit objectives. After performing additional work, auditors may discover that the abuse represents potential fraud or noncompliance with provisions of laws, regulations, contracts, or grant agreements.

Ongoing Investigations and Legal Proceedings

6.35 Avoiding interference with investigations or legal proceedings is important in pursuing indications of fraud, noncompliance with provisions of laws, regulations, contracts or grant agreements, or abuse. Laws, regulations, and policies may require auditors to report indications of certain types of fraud, noncompliance with provisions of laws, regulations,

[140]See A.08 for additional examples of abuse.

contracts, or grant agreements, or abuse to law enforcement or investigatory authorities before performing additional audit procedures. When investigations or legal proceedings are initiated or in process, auditors should evaluate the impact on the current audit. In some cases, it may be appropriate for the auditors to work with investigators or legal authorities, or withdraw from or defer further work on the audit or a portion of the audit to avoid interfering with an ongoing investigation or legal proceeding.

Previous Audits and Attestation Engagements

6.36 Auditors should evaluate whether the audited entity has taken appropriate corrective action to address findings and recommendations from previous engagements that are significant within the context of the audit objectives. When planning the audit, auditors should ask management of the audited entity to identify previous audits, attestation engagements, performance audits, or other studies that directly relate to the objectives of the audit, including whether related recommendations have been implemented. Auditors should use this information in assessing risk and determining the nature, timing, and extent of current audit work, including determining the extent to which testing the implementation of the corrective actions is applicable to the current audit objectives.

Identifying Audit Criteria

6.37 Auditors should identify criteria. Criteria represent the laws, regulations, contracts, grant agreements, standards, specific requirements, measures, expected performance, defined business practices, and benchmarks against which performance is compared or evaluated. Criteria identify the required or desired state or expectation with respect to the program or operation. Criteria provide a context for evaluating evidence and understanding the findings, conclusions, and recommendations included in the report. Auditors should use criteria that are relevant to the audit

objectives and permit consistent assessment of the subject matter.[141]

Identifying Sources of Evidence and the Amount and Type of Evidence Required

6.38 Auditors should identify potential sources of information that could be used as evidence. Auditors should determine the amount and type of evidence needed to obtain sufficient, appropriate evidence to address the audit objectives and adequately plan audit work.

6.39 If auditors believe that it is likely that sufficient, appropriate evidence will not be available, they may revise the audit objectives or modify the scope and methodology and determine alternative procedures to obtain additional evidence or other forms of evidence to address the current audit objectives. Auditors should also evaluate whether the lack of sufficient, appropriate evidence is due to internal control deficiencies or other program weaknesses, and whether the lack of sufficient, appropriate evidence could be the basis for audit findings.[142]

Using the Work of Others

6.40 Auditors should determine whether other auditors have conducted, or are conducting, audits of the program that could be relevant to the current audit objectives. The results of other auditors' work may be useful sources of information for planning and performing the audit. If other auditors have identified areas that warrant further audit work or follow-up, their work may influence the auditors' selection of objectives, scope, and methodology.

[141]See paragraph A6.02 for examples of criteria.

[142]See paragraphs 6.56 through 6.72 for standards concerning evidence.

6.41 If other auditors have completed audit work related to the objectives of the current audit, the current auditors may be able to use the work of the other auditors to support findings or conclusions for the current audit and, thereby, avoid duplication of efforts. If auditors use the work of other auditors, they should perform procedures that provide a sufficient basis for using that work. Auditors should obtain evidence concerning the other auditors' qualifications and independence and should determine whether the scope, quality, and timing of the audit work performed by the other auditors is adequate for reliance in the context of the current audit objectives. Procedures that auditors may perform in making this determination include reviewing the other auditors' report, audit plan, or audit documentation, and/or performing tests of the other auditors' work. The nature and extent of evidence needed will depend on the significance of the other auditors' work to the current audit objectives and the extent to which the auditors will use that work.[143]

6.42 Some audits may necessitate the use of specialized techniques or methods that require the skills of a specialist. Specialists to whom this section applies include, but are not limited to, actuaries, appraisers, attorneys, engineers, environmental consultants, medical professionals, statisticians, geologists, and information technology experts. If auditors intend to use the work of specialists, they should assess the professional qualifications and independence of the specialists.

6.43 Auditors' assessment of professional qualifications of the specialist involves the following:

[143]See paragraph 3.107 for additional discussion on using the work of other auditors and peer review reports.

a. the professional certification, license, or other recognition of the competence of the specialist in his or her field, as appropriate;

b. the reputation and standing of the specialist in the views of peers and others familiar with the specialist's capability or performance;

c. the specialist's experience and previous work in the subject matter; and

d. the auditors' prior experience in using the specialist's work.

6.44 Auditors' assessment of the independence of specialists who perform audit work includes identifying threats and applying any necessary safeguards in the same manner as they would for auditors performing work on those audits.[144]

Assigning Staff and Other Resources

6.45 Audit management should assign sufficient staff and specialists with adequate collective professional competence to perform the audit.[145] Staffing an audit includes, among other things:

a. assigning staff and specialists with the collective knowledge, skills, and experience appropriate for the job,

b. assigning a sufficient number of staff and supervisors to the audit,

[144]See paragraphs 3.02 through 3.26 for additional discussion related to independence and applying the conceptual framework approach to independence.

[145]See paragraphs 3.72 and 3.79 through 3.81 for additional discussion of using specialists in a GAGAS audit.

c. providing for on-the-job training of staff, and

d. engaging specialists when necessary.

6.46 If planning to use the work of a specialist, auditors should document the nature and scope of the work to be performed by the specialist, including

a. the objectives and scope of the specialist's work,

b. the intended use of the specialist's work to support the audit objectives,

c. the specialist's procedures and findings so they can be evaluated and related to other planned audit procedures, and

d. the assumptions and methods used by the specialist.

Communicating with Management, Those Charged with Governance, and Others

6.47 Auditors should communicate an overview of the objectives, scope, and methodology and the timing of the performance audit and planned reporting (including any potential restrictions on the report), unless doing so could significantly impair the auditors' ability to obtain sufficient, appropriate evidence to address the audit objectives, such as when the auditors plan to conduct unannounced cash counts or perform procedures related to indications of fraud. Auditors should communicate with the following parties, as applicable:

a. management of the audited entity, including those with sufficient authority and responsibility to implement corrective action in the program or activity being audited;

b. those charged with governance;[146]

c. the individuals contracting for or requesting audit services, such as contracting officials or grantees; and

d. the cognizant legislative committee, when auditors perform the audit pursuant to a law or regulation or they conduct the work for the legislative committee that has oversight of the audited entity.

6.48 In those situations where there is not a single individual or group that both oversees the strategic direction of the audited entity and the fulfillment of its accountability obligations or in other situations where the identity of those charged with governance is not clearly evident, auditors should document the process followed and conclusions reached for identifying the appropriate individuals to receive the required auditor communications.

6.49 Determining the form, content, and frequency of the communication is a matter of professional judgment, although written communication is preferred. Auditors may use an engagement letter to communicate the information. Auditors should document this communication.

6.50 If an audit is terminated before it is completed and an audit report is not issued, auditors should document the results of the work to the date of termination and why the audit was terminated. Determining whether and how to communicate the reason for terminating the audit to those charged with governance, appropriate officials of the audited entity, the entity contracting for or requesting the audit, and other appropriate officials will

[146]See paragraphs A1.05 through A1.07 for a discussion of the role of those charged with governance.

depend on the facts and circumstances and, therefore, is a matter of professional judgment.

Preparing a Written Audit Plan

6.51 Auditors must prepare a written audit plan for each audit. The form and content of the written audit plan may vary among audits and may include an audit strategy, audit program, project plan, audit planning paper, or other appropriate documentation of key decisions about the audit objectives, scope, and methodology and the auditors' basis for those decisions. Auditors should update the plan, as necessary, to reflect any significant changes to the plan made during the audit.

6.52 A written audit plan provides an opportunity for audit organization management to supervise audit planning and to determine whether

a. the proposed audit objectives are likely to result in a useful report;

b. the audit plan adequately addresses relevant risks;

c. the proposed audit scope and methodology are adequate to address the audit objectives;

d. available evidence is likely to be sufficient and appropriate for purposes of the audit; and

e. sufficient staff, supervisors, and specialists with adequate collective professional competence and other resources are available to perform the audit and to meet expected time frames for completing the work.

Supervision

6.53 Audit supervisors or those designated to supervise auditors must properly supervise audit staff.

6.54 Audit supervision involves providing sufficient guidance and direction to staff assigned to the audit to address the audit objectives and follow applicable requirements, while staying informed about significant problems encountered, reviewing the work performed, and providing effective on-the-job training.[147]

6.55 The nature and extent of the supervision of staff and the review of audit work may vary depending on a number of factors, such as the size of the audit organization, the significance of the work, and the experience of the staff.

Obtaining Sufficient, Appropriate Evidence

6.56 Auditors must obtain sufficient, appropriate evidence to provide a reasonable basis for their findings and conclusions.

6.57 The concept of sufficient, appropriate evidence is integral to an audit. Appropriateness is the measure of the quality of evidence that encompasses its relevance, validity, and reliability in providing support for findings and conclusions related to the audit objectives.[148] In assessing the overall appropriateness of evidence, auditors should assess whether the evidence is relevant, valid, and reliable. Sufficiency is a measure of the quantity of evidence used to support the findings and conclusions related to the audit objectives. In assessing the sufficiency of evidence, auditors should determine whether enough evidence has been obtained to persuade a knowledgeable person that the findings are reasonable.

[147]See paragraph 6.83c for the documentation requirement related to supervision.

[148]See paragraph A6.05 for additional discussion of the appropriateness of evidence.

6.58 In assessing evidence, auditors should evaluate whether the evidence taken as a whole is sufficient and appropriate for addressing the audit objectives and supporting findings and conclusions. Audit objectives may vary widely, as may the level of work necessary to assess the sufficiency and appropriateness of evidence to address the objectives. For example, in establishing the appropriateness of evidence, auditors may test its reliability by obtaining supporting evidence, using statistical testing, or obtaining corroborating evidence. The concepts of audit risk and significance assist auditors with evaluating the audit evidence.[149]

6.59 Professional judgment assists auditors in determining the sufficiency and appropriateness of evidence taken as a whole. Interpreting, summarizing, or analyzing evidence is typically used in the process of determining the sufficiency and appropriateness of evidence and in reporting the results of the audit work. When appropriate, auditors may use statistical methods to analyze and interpret evidence to assess its sufficiency.

Appropriateness

6.60 Appropriateness is the measure of the quality of evidence that encompasses the relevance, validity, and reliability of evidence used for addressing the audit objectives and supporting findings and conclusions.[150]

a. Relevance refers to the extent to which evidence has a logical relationship with, and importance to, the issue being addressed.

[149]See paragraphs 6.04 and 6.05 for a discussion of significance and audit risk.

[150]See paragraph A6.05 for additional guidance regarding assessing the appropriateness of evidence in relation to the audit objectives.

b. Validity refers to the extent to which evidence is a meaningful or reasonable basis for measuring what is being evaluated. In other words, validity refers to the extent to which evidence represents what it is purported to represent.

c. Reliability refers to the consistency of results when information is measured or tested and includes the concepts of being verifiable or supported.[151]

6.61 There are different types and sources of evidence that auditors may use, depending on the audit objectives. Evidence may be obtained by observation, inquiry, or inspection. Each type of evidence has its own strengths and weaknesses.[152] The following contrasts are useful in judging the appropriateness of evidence. However, these contrasts are not adequate in themselves to determine appropriateness. The nature and types of evidence to support auditors' findings and conclusions are matters of the auditors' professional judgment based on the audit objectives and audit risk.

a. Evidence obtained when internal control is effective is generally more reliable than evidence obtained when internal control is weak or nonexistent.

b. Evidence obtained through the auditors' direct physical examination, observation, computation, and inspection is generally more reliable than evidence obtained indirectly.

c. Examination of original documents is generally more reliable than examination of copies.

[151]See paragraph 6.66 for a discussion of computer-processed information and guidance on data reliability.

[152]See paragraph A6.04 for additional guidance regarding the types of evidence.

d. Testimonial evidence obtained under conditions in which persons may speak freely is generally more reliable than evidence obtained under circumstances in which the persons may be intimidated.

e. Testimonial evidence obtained from an individual who is not biased and has direct knowledge about the area is generally more reliable than testimonial evidence obtained from an individual who is biased or has indirect or partial knowledge about the area.

f. Evidence obtained from a knowledgeable, credible, and unbiased third party is generally more reliable than evidence obtained from management of the audited entity or others who have a direct interest in the audited entity.

6.62 Testimonial evidence may be useful in interpreting or corroborating documentary or physical information. Auditors should evaluate the objectivity, credibility, and reliability of the testimonial evidence. Documentary evidence may be used to help verify, support, or challenge testimonial evidence.

6.63 Surveys generally provide self-reported information about existing conditions or programs. Evaluation of the survey design and administration assists auditors in evaluating the objectivity, credibility, and reliability of the self-reported information.

6.64 When sampling is used, the method of selection that is appropriate will depend on the audit objectives. When a representative sample is needed, the use of statistical sampling approaches generally results in stronger evidence than that obtained from nonstatistical techniques. When a representative sample is not needed, a targeted selection may be effective if the auditors have isolated risk factors or other criteria to target the selection.

6.65 When auditors use information provided by officials of the audited entity as part of their evidence, they should determine what the officials of the audited entity or other auditors did to obtain assurance over the reliability of the information. The auditor may find it necessary to perform testing of management's procedures to obtain assurance or perform direct testing of the information. The nature and extent of the auditors' procedures will depend on the significance of the information to the audit objectives and the nature of the information being used.

6.66 Auditors should assess the sufficiency and appropriateness of computer-processed information regardless of whether this information is provided to auditors or auditors independently extract it. The nature, timing, and extent of audit procedures to assess sufficiency and appropriateness is affected by the effectiveness of the audited entity's internal controls over the information, including information systems controls, and the significance of the information and the level of detail presented in the auditors' findings and conclusions in light of the audit objectives.[153] The assessment of the sufficiency and appropriateness of computer-processed information includes considerations regarding the completeness and accuracy of the data for the intended purposes.[154]

Sufficiency

6.67 Sufficiency is a measure of the quantity of evidence used for addressing the audit objectives and supporting findings and conclusions. Sufficiency also depends on the appropriateness of the evidence. In

[153]See paragraphs 6.23 through 6.27 for additional discussion on assessing the effectiveness of information systems controls.

[154]Refer to additional guidance in *Assessing the Reliability of Computer-Processed Data*, GAO-09-680G (Washington, D.C.: July 2009).

determining the sufficiency of evidence, auditors should determine whether enough appropriate evidence exists to address the audit objectives and support the findings and conclusions.

6.68 The following presumptions are useful in judging the sufficiency of evidence. The sufficiency of evidence required to support the auditors' findings and conclusions is a matter of the auditors' professional judgment.

a. The greater the audit risk, the greater the quantity and quality of evidence required.

b. Stronger evidence may allow less evidence to be used.

c. Having a large volume of audit evidence does not compensate for a lack of relevance, validity, or reliability.

Overall Assessment of Evidence

6.69 Auditors should determine the overall sufficiency and appropriateness of evidence to provide a reasonable basis for the findings and conclusions, within the context of the audit objectives. Professional judgments about the sufficiency and appropriateness of evidence are closely interrelated, as auditors interpret the results of audit testing and evaluate whether the nature and extent of the evidence obtained is sufficient and appropriate. Auditors should perform and document an overall assessment of the collective evidence used to support findings and conclusions, including the results of any specific assessments conducted to conclude on the validity and reliability of specific evidence.

6.70 Sufficiency and appropriateness of evidence are relative concepts, which may be thought of in terms of a

continuum rather than as absolutes. Sufficiency and appropriateness are evaluated in the context of the related findings and conclusions. For example, even though the auditors may have some limitations or uncertainties about the sufficiency or appropriateness of some of the evidence, they may nonetheless determine that in total there is sufficient, appropriate evidence to support the findings and conclusions.

6.71 When assessing the sufficiency and appropriateness of evidence, auditors should evaluate the expected significance of evidence to the audit objectives, findings, and conclusions, available corroborating evidence, and the level of audit risk. The steps to assess evidence may depend on the nature of the evidence, how the evidence is used in the audit or report, and the audit objectives.

a. Evidence is sufficient and appropriate when it provides a reasonable basis for supporting the findings or conclusions within the context of the audit objectives.

b. Evidence is not sufficient or not appropriate when (1) using the evidence carries an unacceptably high risk that it could lead the auditor to reach an incorrect or improper conclusion, (2) the evidence has significant limitations, given the audit objectives and intended use of the evidence, or (3) the evidence does not provide an adequate basis for addressing the audit objectives or supporting the findings and conclusions. Auditors should not use such evidence as support for findings and conclusions.

6.72 Evidence has limitations or uncertainties when the validity or reliability of the evidence has not been assessed or cannot be assessed, given the audit objectives and the intended use of the evidence. Limitations also include errors identified by the auditors in their testing. When the auditors identify limitations or

uncertainties in evidence that is significant to the audit findings and conclusions, they should apply additional procedures, as appropriate. Such procedures include

a. seeking independent, corroborating evidence from other sources;

b. redefining the audit objectives or limiting the audit scope to eliminate the need to use the evidence;

c. presenting the findings and conclusions so that the supporting evidence is sufficient and appropriate and describing in the report the limitations or uncertainties with the validity or reliability of the evidence, if such disclosure is necessary to avoid misleading the report users about the findings or conclusions;[155] and

d. determining whether to report the limitations or uncertainties as a finding, including any related, significant internal control deficiencies.

Developing Elements of a Finding

6.73 Auditors should plan and perform procedures to develop the elements of a finding necessary to address the audit objectives.[156] In addition, if auditors are able to sufficiently develop the elements of a finding, they should develop recommendations for corrective action if they are significant within the context of the audit objectives. The elements needed for a finding are related to the objectives of the audit. Thus, a finding or set of findings is complete to the extent that the audit objectives are addressed and the report clearly relates those objectives to the elements of a finding. For

[155]See paragraph 7.15 for additional reporting requirements when there are limitations or uncertainties with the validity or reliability of evidence.

[156]See paragraph A6.06 for additional discussion on findings.

example, an audit objective may be to determine the current status or condition of program operations or progress in implementing legislative requirements, and not the related cause or effect. In this situation, developing the condition would address the audit objective and development of the other elements of a finding would not be necessary.

6.74 The element of criteria is discussed in paragraph 6.37, and the other elements of a finding—condition, effect, and cause—are discussed in paragraphs 6.75 through 6.77.

6.75 Condition: Condition is a situation that exists. The condition is determined and documented during the audit.

6.76 Cause: The cause identifies the reason or explanation for the condition or the factor or factors responsible for the difference between the situation that exists (condition) and the required or desired state (criteria), which may also serve as a basis for recommendations for corrective actions. Common factors include poorly designed policies, procedures, or criteria; inconsistent, incomplete, or incorrect implementation; or factors beyond the control of program management. Auditors may assess whether the evidence provides a reasonable and convincing argument for why the stated cause is the key factor or factors contributing to the difference between the condition and the criteria.[157]

6.77 Effect or potential effect: The effect is a clear, logical link to establish the impact or potential impact of the difference between the situation that exists (condition) and the required or desired state (criteria).

[157]See paragraph A6.06 for additional discussion on cause.

The effect or potential effect identifies the outcomes or consequences of the condition. When the audit objectives include identifying the actual or potential consequences of a condition that varies (either positively or negatively) from the criteria identified in the audit, "effect" is a measure of those consequences. Effect or potential effect may be used to demonstrate the need for corrective action in response to identified problems or relevant risks.[158]

Early Communication of Deficiencies

6.78 Auditors report deficiencies in internal control, fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse. For some matters, early communication to those charged with governance or management may be important because of their relative significance and the urgency for corrective follow-up action. Further, when a control deficiency results in noncompliance with provisions of laws, regulations, contracts or grant agreements, or abuse, early communication is important to allow management to take prompt corrective action to prevent further noncompliance. When a deficiency is communicated early, the reporting requirements in paragraphs 7.18 through 7.23 still apply.

Audit Documentation

6.79 Auditors must prepare audit documentation related to planning, conducting, and reporting for each audit. Auditors should prepare audit documentation in sufficient detail to enable an experienced auditor, having no previous connection to the audit, to understand from the audit documentation the nature, timing, extent, and results of audit procedures performed, the audit evidence obtained and its source

[158]See paragraph A6.07 for additional discussion on effect.

and the conclusions reached, including evidence that supports the auditors' significant judgments and conclusions. An experienced auditor means an individual (whether internal or external to the audit organization) who possesses the competencies and skills that would have enabled him or her to conduct the performance audit. These competencies and skills include an understanding of (1) the performance audit processes, (2) GAGAS and applicable legal and regulatory requirements, (3) the subject matter associated with achieving the audit objectives, and (4) issues related to the audited entity's environment.

6.80 Auditors should prepare audit documentation that contains evidence that supports the findings, conclusions, and recommendations before they issue their report.

6.81 Auditors should design the form and content of audit documentation to meet the circumstances of the particular audit. The audit documentation constitutes the principal record of the work that the auditors have performed in accordance with standards and the conclusions that the auditors have reached. The quantity, type, and content of audit documentation are a matter of the auditors' professional judgment.

6.82 Audit documentation is an essential element of audit quality. The process of preparing and reviewing audit documentation contributes to the quality of an audit. Audit documentation serves to (1) provide the principal support for the auditors' report, (2) aid auditors in conducting and supervising the audit, and (3) allow for the review of audit quality.

6.83 Auditors should document[159] the following:

a. the objectives, scope, and methodology of the audit;

b. the work performed and evidence obtained to support significant judgments and conclusions, including descriptions of transactions and records examined (for example, by listing file numbers, case numbers, or other means of identifying specific documents examined, but copies of documents examined or detailed listings of information from those documents are not required); and

c. supervisory review, before the audit report is issued, of the evidence that supports the findings, conclusions, and recommendations contained in the audit report.

6.84 When auditors do not comply with applicable GAGAS requirements due to law, regulation, scope limitations, restrictions on access to records, or other issues impacting the audit, the auditors should document the departure from the GAGAS requirements and the impact on the audit and on the auditors' conclusions. This applies to departures from unconditional requirements and from presumptively mandatory requirements when alternative procedures performed in the circumstances were not sufficient to achieve the objectives of the standard.[160]

6.85 Underlying GAGAS audits is the premise that audit organizations in federal, state, and local governments and public accounting firms engaged to perform audits in accordance with GAGAS cooperate in auditing

[159]See paragraphs 6.06, 6.46, 6.48, 6.49, 6.50, 6.69, 6.84, 7.19, 7.22, and 7.44 for additional documentation requirements regarding performance audits.

[160]See paragraphs 2.24 and 2.25 for additional requirements on citing compliance with GAGAS.

programs of common interest so that auditors may use others' work and avoid duplication of efforts. Subject to applicable laws and regulations, auditors should make appropriate individuals, as well as audit documentation, available upon request and in a timely manner to other auditors or reviewers to satisfy these objectives. The use of auditors' work by other auditors may be facilitated by contractual arrangements for GAGAS audits that provide for full and timely access to appropriate individuals, as well as audit documentation.

Reporting Standards for Performance Audits

Introduction

7.01 This chapter contains reporting requirements and guidance for performance audits conducted in accordance with generally accepted government auditing standards (GAGAS). The purpose of reporting requirements is to establish the overall approach for auditors to apply in communicating the results of the performance audit. The reporting requirements for performance audits relate to the form of the report, the report contents, and report issuance and distribution.[161]

7.02 For performance audits conducted in accordance with GAGAS, the requirements and guidance in chapters 1 through 3, 6, and 7 apply.

Reporting

7.03 Auditors must issue audit reports communicating the results of each completed performance audit.

7.04 Auditors should use a form of the audit report that is appropriate for its intended use and is in writing or in some other retrievable form.[162] For example, auditors may present audit reports using electronic media that are retrievable by report users and the audit organization. The users' needs will influence the form of the audit report. Different forms of audit reports include written reports, letters, briefing slides, or other presentation materials.

[161]See paragraph A7.02 for a description of report quality elements.

[162]See paragraph 7.43 for situations when audit organizations are subject to public records laws.

7.05 The purposes of audit reports are to (1) communicate the results of audits to those charged with governance, the appropriate officials of the audited entity, and the appropriate oversight officials; (2) make the results less susceptible to misunderstanding; (3) make the results available to the public, unless specifically limited;[163] and (4) facilitate follow-up to determine whether appropriate corrective actions have been taken.

7.06 If an audit is terminated before it is completed and an audit report is not issued, auditors should follow the guidance in paragraph 6.50.

7.07 If, after the report is issued, the auditors discover that they did not have sufficient, appropriate evidence to support the reported findings or conclusions, they should communicate in the same manner as that used to originally distribute the report to those charged with governance, the appropriate officials of the audited entity, the appropriate officials of the organizations requiring or arranging for the audits, and other known users, so that they do not continue to rely on the findings or conclusions that were not supported. If the report was previously posted to the auditors' publicly accessible website, the auditors should remove the report and post a public notification that the report was removed. The auditors should then determine whether to conduct additional audit work necessary to reissue the report, including any revised findings or conclusions or repost the original report if the additional audit work does not result in a change in findings or conclusions.

[163]See paragraph 7.40 for additional guidance on classified or limited use reports and paragraph 7.44b for distribution of reports for internal auditors.

Report Contents

7.08 Auditors should prepare audit reports that contain (1) the objectives, scope, and methodology of the audit; (2) the audit results, including findings, conclusions, and recommendations, as appropriate; (3) a statement about the auditors' compliance with GAGAS; (4) a summary of the views of responsible officials; and (5) if applicable, the nature of any confidential or sensitive information omitted.

Objectives, Scope, and Methodology

7.09 Auditors should include in the report a description of the audit objectives and the scope and methodology used for addressing the audit objectives. Report users need this information to understand the purpose of the audit, the nature and extent of the audit work performed, the context and perspective regarding what is reported, and any significant limitations in audit objectives, scope, or methodology.

7.10 Audit objectives for performance audits may vary widely. Auditors should communicate audit objectives in the audit report in a clear, specific, neutral, and unbiased manner that includes relevant assumptions. When audit objectives are limited but broader objectives could be inferred by users, auditors should state in the audit report that certain issues were outside the scope of the audit in order to avoid potential misunderstanding.

7.11 Auditors should describe the scope of the work performed and any limitations, including issues that would be relevant to likely users, so that they could reasonably interpret the findings, conclusions, and recommendations in the report without being misled. Auditors should also report any significant constraints imposed on the audit approach by information limitations or scope impairments, including denials or excessive delays of access to certain records or individuals.

7.12 In describing the work conducted to address the audit objectives and support the reported findings and conclusions, auditors should, as applicable, explain the relationship between the population and the items tested; identify organizations, geographic locations, and the period covered; report the kinds and sources of evidence; and explain any significant limitations or uncertainties based on the auditors' overall assessment of the sufficiency and appropriateness of the evidence in the aggregate.

7.13 In reporting audit methodology, auditors should explain how the completed audit work supports the audit objectives, including the evidence gathering and analysis techniques, in sufficient detail to allow knowledgeable users of their reports to understand how the auditors addressed the audit objectives. Auditors may include a description of the procedures performed as part of their assessment of the sufficiency and appropriateness of information used as audit evidence. Auditors should identify significant assumptions made in conducting the audit; describe comparative techniques applied; describe the criteria used; and, when sampling significantly supports the auditors' findings, conclusions, or recommendations, describe the sample design and state why the design was chosen, including whether the results can be projected to the intended population.

Reporting Findings

7.14 In the audit report, auditors should present sufficient, appropriate evidence to support the findings and conclusions in relation to the audit objectives. Clearly developed findings[164] assist management and oversight officials of the audited entity in understanding the need for taking corrective action. If auditors are able

[164]See paragraphs 6.73 through 6.77 for additional discussion on developing the elements of a finding.

to sufficiently develop the elements of a finding, they should provide recommendations for corrective action if they are significant within the context of the audit objectives. However, the extent to which the elements for a finding are developed depends on the audit objectives. Thus, a finding or set of findings is complete to the extent that the auditors address the audit objectives.

7.15 Auditors should describe in their report limitations or uncertainties with the reliability or validity of evidence if (1) the evidence is significant to the findings and conclusions within the context of the audit objectives and (2) such disclosure is necessary to avoid misleading the report users about the findings and conclusions. As discussed in paragraphs 6.69 through 6.72, even though the auditors may have some uncertainty about the sufficiency or appropriateness of some of the evidence, they may nonetheless determine that in total there is sufficient, appropriate evidence given the findings and conclusions. Auditors should describe the limitations or uncertainties regarding evidence in conjunction with the findings and conclusions, in addition to describing those limitations or uncertainties as part of the objectives, scope, and methodology. Additionally, this description provides report users with a clear understanding regarding how much responsibility the auditors are taking for the information.

7.16 Auditors should place their findings in perspective by describing the nature and extent of the issues being reported and the extent of the work performed that resulted in the finding. To give the reader a basis for judging the prevalence and consequences of these findings, auditors should, as appropriate, relate the instances identified to the population or the number of cases examined and quantify the results in terms of dollar value, or other measures. If the results cannot be

projected, auditors should limit their conclusions appropriately.

7.17 Auditors may provide background information to establish the context for the overall message and to help the reader understand the findings and significance of the issues discussed. Appropriate background information may include information on how programs and operations work; the significance of programs and operations (e.g., dollars, impact, purposes, and past audit work, if relevant); a description of the audited entity's responsibilities; and explanation of terms, organizational structure, and the statutory basis for the program and operations. When reporting on the results of their work, auditors should disclose significant facts relevant to the objectives of their work and known to them which, if not disclosed, could mislead knowledgeable users, misrepresent the results, or conceal significant improper or illegal practices.

7.18 Auditors should also report deficiencies in internal control, instances of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that have occurred or are likely to have occurred and are significant within the context of the audit objectives.

Deficiencies in Internal Control

7.19 Auditors should include in the audit report (1) the scope of their work on internal control and (2) any deficiencies in internal control that are significant within the context of the audit objectives and based upon the audit work performed.[165] When auditors detect deficiencies in internal control that are not significant to the objectives of the audit but warrant the attention of those charged with governance, they should include

[165]See paragraph 6.21 for a discussion of internal control deficiencies in performance audits and paragraph A.06 for examples of deficiencies in internal control.

those deficiencies either in the report or communicate those deficiencies in writing to audited entity officials. Auditors should refer to that written communication in the audit report if the written communication is separate from the audit report. When auditors detect deficiencies that do not warrant the attention of those charged with governance, the determination of whether and how to communicate such deficiencies to audited entity officials is a matter of professional judgment.

7.20 In a performance audit, auditors may conclude that identified deficiencies in internal control that are significant within the context of the audit objectives are the cause of deficient performance of the program or operations being audited. In reporting this type of finding, the internal control deficiency would be described as the cause.

Fraud, Noncompliance with Provisions of Laws, Regulations, Contracts, and Grant Agreements, and Abuse

7.21 When auditors conclude, based on sufficient, appropriate evidence, that fraud,[166] noncompliance with provisions of laws, regulations, contracts or grant agreements, or abuse[167] either has occurred or is likely to have occurred which is significant within the context of the audit objectives, they should report the matter as a finding. Whether a particular act is, in fact, fraud or noncompliance with provisions of laws, regulations, contracts or grant agreements may have to await final determination by a court of law or other adjudicative body.

7.22 When auditors detect instances of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that are not significant within the context of the audit objectives but warrant the attention of those charged with governance,

[166]See paragraph A.10 for examples of indicators of fraud risk.

[167]See paragraph A.08 for examples of abuse.

they should communicate those findings in writing to audited entity officials. When auditors detect any instances of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that do not warrant the attention of those charged with governance, the auditors' determination of whether and how to communicate such instances to audited entity officials is a matter of professional judgment.

7.23 When fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse either have occurred or are likely to have occurred, auditors may consult with authorities or legal counsel about whether publicly reporting such information would compromise investigative or legal proceedings. Auditors may limit their public reporting to matters that would not compromise those proceedings and, for example, report only on information that is already a part of the public record.

Reporting Findings Directly to Parties Outside the Audited Entity

7.24 Auditors should report known or likely fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse directly to parties outside the audited entity in the following two circumstances.

a. When entity management fails to satisfy legal or regulatory requirements to report such information to external parties specified in law or regulation, auditors should first communicate the failure to report such information to those charged with governance. If the audited entity still does not report this information to the specified external parties as soon as practicable after the auditors' communication with those charged with governance, then the auditors should report the information directly to the specified external parties.

b. When entity management fails to take timely and appropriate steps to respond to known or likely fraud,

noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that (1) is significant to the findings and conclusions and (2) involves funding received directly or indirectly from a government agency, auditors should first report management's failure to take timely and appropriate steps to those charged with governance. If the audited entity still does not take timely and appropriate steps as soon as practicable after the auditors' communication with those charged with governance, then the auditors should report the entity's failure to take timely and appropriate steps directly to the funding agency.

7.25 The reporting in paragraph 7.24 is in addition to any legal requirements for the auditor to report such information directly to parties outside the audited entity. Auditors should comply with these requirements even if they have resigned or been dismissed from the audit prior to its completion. Internal audit organizations do not have a duty to report outside the audited entity unless required by law, rule, regulation, or policy.[168]

7.26 Auditors should obtain sufficient, appropriate evidence, such as confirmation from outside parties, to corroborate assertions by management of the audited entity that it has reported such findings in accordance with laws, regulations, or funding agreements. When auditors are unable to do so, they should report such information directly as discussed in paragraphs 7.24 and 7.25.

Conclusions

7.27 Auditors should report conclusions based on the audit objectives and the audit findings. Report conclusions are logical inferences about the program based on the auditors' findings, not merely a summary

[168]See paragraph 7.44b for reporting standards for internal audit organizations when reporting externally.

of the findings. The strength of the auditors' conclusions depends on the sufficiency and appropriateness of the evidence supporting the findings and the soundness of the logic used to formulate the conclusions. Conclusions are more compelling if they lead to the auditors' recommendations and convince the knowledgeable user of the report that action is necessary.

Recommendations

7.28 Auditors should recommend actions to correct deficiencies and other findings identified during the audit and to improve programs and operations when the potential for improvement in programs, operations, and performance is substantiated by the reported findings and conclusions. Auditors should make recommendations that flow logically from the findings and conclusions, are directed at resolving the cause of identified deficiencies and findings, and clearly state the actions recommended.

7.29 Effective recommendations encourage improvements in the conduct of government programs and operations. Recommendations are effective when they are addressed to parties that have the authority to act and when the recommended actions are specific, practical, cost effective, and measurable.

Reporting Auditors' Compliance with GAGAS

7.30 When auditors comply with all applicable GAGAS requirements, they should use the following language, which represents an unmodified GAGAS compliance statement, in the audit report to indicate that they performed the audit in accordance with GAGAS.[169]

[169]See paragraphs 2.24 and 2.25 for additional standards on citing compliance with GAGAS.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

7.31 When auditors do not comply with all applicable GAGAS requirements, they should include a modified GAGAS compliance statement in the audit report. For performance audits, auditors should use a statement that includes either (1) the language in 7.30, modified to indicate the requirements that were not followed or (2) language that the auditor did not follow GAGAS.[170]

Reporting Views of Responsible Officials

7.32 Auditors should obtain and report the views of responsible officials of the audited entity concerning the findings, conclusions, and recommendations included in the audit report, as well as any planned corrective actions.

7.33 Providing a draft report with findings for review and comment by responsible officials of the audited entity and others helps the auditors develop a report that is fair, complete, and objective. Including the views of responsible officials results in a report that presents not only the auditors' findings, conclusions, and recommendations, but also the perspectives of the responsible officials of the audited entity and the corrective actions they plan to take. Obtaining the comments in writing is preferred, but oral comments are acceptable.

[170]See paragraphs 2.24 and 2.25 for additional standards on citing compliance with GAGAS.

7.34 When auditors receive written comments from the responsible officials, they should include in their report a copy of the officials' written comments, or a summary of the comments received. When the responsible officials provide oral comments only, auditors should prepare a summary of the oral comments and provide a copy of the summary to the responsible officials to verify that the comments are accurately stated.

7.35 Auditors should also include in the report an evaluation of the comments, as appropriate. In cases in which the audited entity provides technical comments in addition to its written or oral comments on the report, auditors may disclose in the report that such comments were received.

7.36 Obtaining oral comments may be appropriate when, for example, there is a reporting date critical to meeting a user's needs; auditors have worked closely with the responsible officials throughout the work and the parties are familiar with the findings and issues addressed in the draft report; or the auditors do not expect major disagreements with the findings, conclusions, and recommendations in the draft, or major controversies with regard to the issues discussed in the draft report.

7.37 When the audited entity's comments are inconsistent or in conflict with the findings, conclusions, or recommendations in the draft report, or when planned corrective actions do not adequately address the auditors' recommendations, the auditors should evaluate the validity of the audited entity's comments. If the auditors disagree with the comments, they should explain in the report their reasons for disagreement. Conversely, the auditors should modify their report as necessary if they find the comments valid and supported with sufficient, appropriate evidence.

7.38 If the audited entity refuses to provide comments or is unable to provide comments within a reasonable period of time, the auditors may issue the report without receiving comments from the audited entity. In such cases, the auditors should indicate in the report that the audited entity did not provide comments.

Reporting Confidential and Sensitive Information

7.39 If certain pertinent information is prohibited from public disclosure or is excluded from a report due to the confidential or sensitive nature of the information, auditors should disclose in the report that certain information has been omitted and the reason or other circumstances that make the omission necessary.

7.40 Certain information may be classified or may be otherwise prohibited from general disclosure by federal, state, or local laws or regulations. In such circumstances, auditors may issue a separate, classified or limited use report containing such information and distribute the report only to persons authorized by law or regulation to receive it.

7.41 Additional circumstances associated with public safety, privacy, or security concerns could also justify the exclusion of certain information from a publicly available or widely distributed report. For example, detailed information related to computer security for a particular program may be excluded from publicly available reports because of the potential damage that could be caused by the misuse of this information. In such circumstances, auditors may issue a limited use report containing such information and distribute the report only to those parties responsible for acting on the auditors' recommendations. In some instances, it may be appropriate to issue both a publicly available report with the sensitive information excluded and a limited use report. The auditors may consult with legal counsel regarding any requirements or other circumstances that may necessitate the omission of certain information.

7.42 Considering the broad public interest in the program or activity under audit assists auditors when deciding whether to exclude certain information from publicly available reports. When circumstances call for omission of certain information, auditors should evaluate whether this omission could distort the audit results or conceal improper or illegal practices.

7.43 When audit organizations are subject to public records laws, auditors should determine whether public records laws could impact the availability of classified or limited use reports and determine whether other means of communicating with management and those charged with governance would be more appropriate. For example, the auditors may communicate general information in a written report and communicate detailed information orally. The auditor may consult with legal counsel regarding applicable public records laws.

Distributing Reports

7.44 Distribution of reports completed in accordance with GAGAS depends on the relationship of the auditors to the audited organization and the nature of the information contained in the report. Auditors should document any limitation on report distribution.[171] The following discussion outlines distribution for reports completed in accordance with GAGAS:

a. Audit organizations in government entities should distribute audit reports to those charged with governance, to the appropriate audited entity officials, and to the appropriate oversight bodies or organizations requiring or arranging for the audits. As appropriate, auditors should also distribute copies of the reports to other officials who have legal oversight authority or who

[171]See paragraphs 7.40 and 7.41 for discussion of limited use reports containing confidential or sensitive information.

may be responsible for acting on audit findings and recommendations, and to others authorized to receive such reports.

b. Internal audit organizations in government entities may also follow the Institute of Internal Auditors' (IIA) *International Standards for the Professional Practice of Internal Auditing*.[172] In accordance with GAGAS and IIA standards, the head of the internal audit organization should communicate results to parties who can ensure that the results are given due consideration. If not otherwise mandated by statutory or regulatory requirements, prior to releasing results to parties outside the organization, the head of the internal audit organization should: (1) assess the potential risk to the organization, (2) consult with senior management or legal counsel as appropriate, and (3) control dissemination by indicating the intended users of the report.

c. Public accounting firms contracted to perform an audit in accordance with GAGAS should clarify report distribution responsibilities with the engaging organization. If the contracting firm is responsible for the distribution, it should reach agreement with the party contracting for the audit about which officials or organizations will receive the report and the steps being taken to make the report available to the public.

[172]See paragraph 2.21 for additional discussion about using the IIA standards in conjunction with GAGAS and paragraph 2.22 for additional discussion about citing compliance with another set of standards.

Supplemental Guidance

Introduction

A.01 The following sections provide supplemental guidance for auditors and the audited entities to assist in the implementation of generally accepted government auditing standards (GAGAS). The guidance does not establish additional requirements but instead is intended to facilitate auditor implementation of GAGAS requirements in chapters 2 through 7. The supplemental guidance in the first section may be of assistance for all types of audits covered by GAGAS. Subsequent sections provide supplemental guidance for specific chapters of GAGAS, as indicated.

Overall Supplemental Guidance

A.02 Chapters 4 through 7 discuss the standards for financial audits, attestation engagements, and performance audits. The identification and communication of significant deficiencies and material weaknesses in internal control, fraud, noncompliance with provisions of laws, regulations, contracts or grant agreements, or abuse are important aspects of government auditing. The following discussion is provided to assist auditors in identifying significant deficiencies in internal control, abuse, and indicators of fraud risk and to assist auditors in determining whether noncompliance with provisions of laws, regulations, contracts or grant agreements are significant within the context of the audit objectives.

Internal Control

A.03 The *Internal Control—Integrated Framework*[173] published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) provides guidance on internal control. As discussed in the COSO framework, internal control consists of five interrelated components, which are (1) control

[173]*Internal Control—Integrated Framework,* Committee of Sponsoring Organizations of the Treadway Commission, 1992.

environment, (2) risk assessment, (3) control activities, (4) information and communication, and (5) monitoring. The objectives of internal control relate to (1) financial reporting, (2) operations, and (3) compliance. Safeguarding of assets is a subset of these objectives. Management designs internal control to provide reasonable assurance that unauthorized acquisition, use, or disposition of assets will be prevented or timely detected and corrected.

A.04 In addition to the COSO framework, the publication, *Standards for Internal Control in the Federal Government*,[174] which incorporates the concepts developed by COSO, provides definitions and fundamental concepts pertaining to internal control at the federal level and may also be useful to auditors at other levels of government. The related *Internal Control Management and Evaluation Tool*,[175] based on the federal internal control standards, provides a systematic, organized, and structured approach to assessing the internal control structure.

Examples of Deficiencies in Internal Control

A.05 GAGAS contains requirements for reporting identified deficiencies in internal control.

a. For financial audits, see paragraphs 4.19 through 4.24.

b. For attestation engagements, see paragraphs 5.20 through 5.23.

[174] *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

[175] *Internal Control Management and Evaluation Tool*, GAO-01-1008G (Washington, D.C.: August 2001).

c. For performance audits, see paragraphs 7.19 through 7.20.

A.06 The following are examples of control deficiencies:

a. Insufficient control consciousness within the organization. For example, the tone at the top and the control environment. Control deficiencies in other components of internal control could lead the auditor to conclude that weaknesses exist in the control environment.

b. Ineffective oversight by those charged with governance of the entity's financial reporting, performance reporting, or internal control, or an ineffective overall governance structure.

c. Control systems that did not prevent, or detect and correct material misstatements so that it was necessary to restate previously issued financial statements or operational results. Control systems that did not prevent or detect material misstatements in performance or operational results so that it was later necessary to make significant corrections to those results.

d. Control systems that did not prevent, or detect and correct material misstatements identified by the auditor. This includes misstatements involving estimation and judgment for which the auditor identifies potential material adjustments and corrections of the recorded amounts.

e. An ineffective internal audit function or risk assessment function at an entity for which such functions are important to the monitoring or risk assessment component of internal control, such as for a large or complex entity.

f. Identification of fraud of any magnitude on the part of senior management.

g. Failure by management or those charged with governance to assess the effect of a significant deficiency previously communicated to them and either to correct it or to conclude that it does not need to be corrected.

h. Inadequate controls for the safeguarding of assets.

i. Evidence of intentional override of internal control by those in authority to the detriment of the overall objectives of the system.

j. Deficiencies in the design or operation of internal control that could fail to prevent, or detect and correct, fraud, noncompliance with provisions of laws, regulations, contracts or grant agreements, or abuse having a material effect on the financial statements or the audit objective.

k. Inadequate design of information systems general, application, and user controls that prevent the information system from providing complete and accurate information consistent with financial, compliance, or performance reporting objectives or other current needs.

l. Failure of an application control caused by a deficiency in the design or operation of an information systems general control.

m. Employees or management who lack the qualifications and training to fulfill their assigned functions.

Examples of Abuse

A.07 GAGAS contains requirements for responding to indications of material abuse and reporting abuse that is material to the audit objectives.

a. For financial audits, see paragraphs 4.07 and 4.08 and 4.25 through 4.27.

b. For attestation engagements, see paragraphs 5.08 through 5.09 and 5.24 through 5.26.

c. For performance audits, see paragraphs 6.33 and 6.34 and 7.21 through 7.23.

A.08 The following are examples of abuse, depending on the facts and circumstances:

a. Creating unneeded overtime.

b. Requesting staff to perform personal errands or work tasks for a supervisor or manager.

c. Misusing the official's position for personal gain (including actions that could be perceived by an objective third party with knowledge of the relevant information as improperly benefiting an official's personal financial interests or those of an immediate or close family member; a general partner; an organization for which the official serves as an officer, director, trustee, or employee; or an organization with which the official is negotiating concerning future employment).

d. Making travel choices that are contrary to existing travel policies or are unnecessarily extravagant or expensive.

e. Making procurement or vendor selections that are contrary to existing policies or are unnecessarily extravagant or expensive.

Examples of Indicators of Fraud Risk

A.09 GAGAS contains requirements relating to evaluating fraud risk.

a. For financial audits, see paragraphs 4.06 and 4.25 through 4.27.

b. For attestation engagements, see paragraphs 5.07, 5.20, and 5.24 through 5.26.

c. For performance audits, see paragraphs 6.30 through 6.32 and 7.21 through 7.23.

A.10 In some circumstances, conditions such as the following might indicate a heightened risk of fraud:

a. economic, programmatic, or entity operating conditions threaten the entity's financial stability, viability, or budget;

b. the nature of the entity's operations provide opportunities to engage in fraud;

c. management's monitoring of compliance with policies, laws, and regulations is inadequate;

d. the organizational structure is unstable or unnecessarily complex;

e. communication and/or support for ethical standards by management is lacking;

f. management is willing to accept unusually high levels of risk in making significant decisions;

g. the entity has a history of impropriety, such as previous issues with fraud, waste, abuse, or questionable practices, or past audits or investigations with findings of questionable or criminal activity;

h. operating policies and procedures have not been developed or are outdated;

i. key documentation is lacking or does not exist;

j. asset accountability or safeguarding procedures is lacking;

k. improper payments;

l. false or misleading information;

m. a pattern of large procurements in any budget line with remaining funds at year end, in order to "use up all of the funds available;" and

n. unusual patterns and trends in contracting, procurement, acquisition, and other activities of the entity or program.

Determining Whether Provisions of Laws, Regulations, Contracts and Grant Agreements Are Significant within the Context of the Audit Objectives

A.11 GAGAS contains requirements for determining whether provisions of laws, regulations, contracts or grant agreements are significant within the context of the audit objectives.

a. For financial audits, see paragraphs 4.19 through 4.22.

b. For attestation engagements, see paragraphs 5.07 and 5.08.

c. For performance audits, see paragraphs 6.28 and 6.29.

A.12 Government programs are subject to many provisions of laws, regulations, contracts or grant agreements. At the same time, their significance within the context of the audit objectives varies widely,

depending on the objectives of the audit. Auditors may find the following approach helpful in assessing whether provisions of laws, regulations, contracts or grant agreements are significant within the context of the audit objectives:

a. Express each audit objective in terms of questions about specific aspects of the program being audited (that is, purpose and goals, internal control, inputs, program operations, outputs, and outcomes).

b. Identify provisions of laws, regulations, contracts or grant agreements that directly relate to specific aspects of the program within the context of the audit objectives.

c. Determine if the audit objectives or the auditors' conclusions could be significantly affected if noncompliance with those provisions of laws, regulations, contracts or grant agreements occurred. If the audit objectives or audit conclusions could be significantly affected, then those provisions of laws, regulations, contracts or grant agreements are likely to be significant to the audit objectives.

A.13 Auditors may consult with their own legal counsel to (1) determine those laws and regulations that are significant to the audit objectives, (2) design tests of compliance with laws and regulations, or (3) evaluate the results of those tests. Auditors also may consult with their own legal counsel when audit objectives require testing compliance with provisions of contracts or grant agreements. Depending on the circumstances of the audit, auditors may consult with others, such as investigative staff, other audit organizations or government entities that provided professional services to the audited entity, or applicable law enforcement authorities, to obtain information on compliance matters.

Information to Accompany Chapter 1

A1.01 Chapter 1 discusses the use and application of GAGAS and the role of auditing in government accountability. Those charged with governance and management of audited organizations also have roles in government accountability. The discussion that follows is provided to assist auditors in understanding the roles of others in accountability. The following section also contains background information on the laws, regulations, or other authoritative sources that require the use of GAGAS. This information is provided to place GAGAS within the context of overall government accountability.

Laws, Regulations, and Other Authoritative Sources That Require Use of GAGAS

A1.02 Laws, regulations, contracts, grant agreements, or policies frequently require the use of GAGAS.[176] The following are some of the laws, regulations, and or other authoritative sources that require the use of GAGAS:

a. The Inspector General Act of 1978, as amended, 5 U.S.C. App. requires that the statutorily appointed federal inspectors general comply with GAGAS for audits of federal establishments, organizations, programs, activities, and functions. The act further states that the inspectors general shall take appropriate steps to assure that any work performed by nonfederal auditors complies with GAGAS.

b. The Chief Financial Officers Act of 1990 (Public Law 101-576), as expanded by the Government Management Reform Act of 1994 (Public Law 103-356), requires that GAGAS be followed in audits of executive branch departments' and agencies' financial statements. The Accountability of Tax Dollars Act of 2002 (Public Law 107-289) generally extends this

[176]See paragraph 1.06 for additional discussion on the use of GAGAS.

requirement to most executive agencies not subject to the Chief Financial Officers Act unless they are exempted for a given year by the Office of Management and Budget (OMB).

c. The Single Audit Act Amendments of 1996 (Public Law 104-156) require that GAGAS be followed in audits of state and local governments and nonprofit entities that receive federal awards. OMB Circular No. A-133, *Audits of States, Local Governments, and Non-Profit Organizations*, which provides the governmentwide guidelines and policies on performing audits to comply with the Single Audit Act, also requires the use of GAGAS.

A1.03 Other laws, regulations, or authoritative sources may require the use of GAGAS. For example, auditors at the state and local levels of government may be required by state and local laws and regulations to follow GAGAS. Also, auditors may be required by the terms of an agreement or contract to follow GAGAS. Auditors may also be required to follow GAGAS by federal audit guidelines pertaining to program requirements, such as those issued for Housing and Urban Development programs and Student Financial Aid programs. Being alert to such other laws, regulations, or authoritative sources may assist auditors in performing their work in accordance with the required standards.

A1.04 Even if not required to do so, auditors may find it useful to follow GAGAS in performing audits of federal, state, and local government programs as well as audits of government awards administered by contractors, nonprofit entities, and other nongovernmental entities. Many audit organizations not formally required to do so, both in the United States of America and in other countries, voluntarily follow GAGAS.

The Role of Those Charged with Governance

A1.05 During the course of GAGAS audits, auditors communicate with those charged with governance.[177]

a. For financial audits, see paragraphs 4.03 and 4.04.

b. For attestation engagements, see paragraphs 5.04 and 5.05.

c. For performance audits, see paragraphs 6.47 through 6.50.

A1.06 Those charged with governance are responsible for overseeing the strategic direction of the entity and obligations related to the accountability of the entity. This includes overseeing the financial reporting process, subject matter, or program under audit including related internal controls. In certain entities covered by GAGAS, those charged with governance may also be part of the entity's management. In some audit entities, multiple parties may be charged with governance, including oversight bodies, members or staff of legislative committees, boards of directors, audit committees, or parties contracting for the audit.

A1.07 Because the governance structures of government entities and organizations can vary widely, it may not always be clearly evident who is charged with key governance functions. In these situations, auditors evaluate the organizational structure for directing and controlling operations to achieve the audited entity's objectives. This evaluation also includes how the audited entity delegates authority and establishes accountability for its management personnel.

[177]See paragraph 1.02 for additional discussion of those charged with governance.

Management's Role

A1.08 Managers have fundamental responsibilities for carrying out government functions.[178] Management of the audited entity is responsible for

a. using its financial, physical, and informational resources legally, effectively, efficiently, economically, ethically, and equitably to achieve the purposes for which the resources were furnished or the program was established;

b. complying with applicable laws and regulations (including identifying the requirements with which the entity and the official are responsible for compliance);

c. implementing systems designed to achieve compliance with applicable laws and regulations;

d. establishing and maintaining effective internal control to help ensure that appropriate goals and objectives are met; following laws and regulations; and ensuring that management and financial information is reliable and properly reported;

e. providing appropriate reports to those who oversee their actions and to the public in order to demonstrate accountability for the resources and authority used to carry out government programs and the results of these programs;

f. addressing the findings and recommendations of auditors, and for establishing and maintaining a process to track the status of such findings and recommendations;

[178]See paragraphs 1.01 and 1.02 for additional discussion of management and officials of government programs.

g. following sound procurement practices when contracting for audits, including ensuring procedures are in place for monitoring contract performance; and

h. taking timely and appropriate steps to remedy fraud, noncompliance with provisions of laws, regulations, contracts or grant agreements, or abuse that auditors report.

Information to Accompany Chapter 2

Attestation Engagements

A2.01 Examples of attestation engagements objectives[179] include

a. prospective financial or performance information;

b. management's discussion and analysis (MD&A) presentation;

c. an entity's internal control over financial reporting;

d. the effectiveness of an entity's internal control over compliance with specified requirements, such as those governing the bidding for, accounting for, and reporting on grants and contracts;

e. an entity's compliance with requirements of specified laws, regulations, policies, contracts, or grants;

f. the accuracy and reliability of reported performance measures;

[179]See paragraph 2.09 for additional discussion of attestation engagements.

g. whether incurred final contract costs are supported with required evidence and in compliance with the contract terms;

h. the allowability and reasonableness of proposed contract amounts that are based on detailed costs; and

i. the quantity, condition, or valuation of inventory or assets.

Performance Audit Objectives

A2.02 Examples of program effectiveness and results audit objectives[180] include:

a. assessing the extent to which legislative, regulatory, or organizational goals and objectives are being achieved;

b. assessing the relative ability of alternative approaches to yield better program performance or eliminate factors that inhibit program effectiveness;

c. analyzing the relative cost-effectiveness of a program or activity, focusing on combining cost information or other inputs with information about outputs or the benefit provided or with outcomes or the results achieved;

d. determining whether a program produced intended results or produced results that were not consistent with the program's objectives;

e. determining the current status or condition of program operations or progress in implementing legislative requirements;

[180]See paragraph 2.11a for additional discussion of program effectiveness and results audit objectives.

f. determining whether a program provides equitable access to or distribution of public resources within the context of statutory parameters;

g. assessing the extent to which programs duplicate, overlap, or conflict with other related programs;

h. evaluating whether the entity is following sound procurement practices;

i. assessing the reliability, validity, or relevance of performance measures concerning program effectiveness and results, or economy and efficiency;

j. assessing the reliability, validity, or relevance of financial information related to the performance of a program;

k. determining whether government resources (inputs) are obtained at reasonable costs while meeting timeliness and quality considerations;

l. determining whether appropriate value was obtained based on the cost or amount paid or based on the amount of revenue received;

m. determining whether government services and benefits are accessible to those individuals who have a right to access those services and benefits;

n. determining whether fees assessed cover costs;

o. determining whether and how the program's unit costs can be decreased or its productivity increased; and

p. assessing the reliability, validity, or relevance of budget proposals or budget requests to assist legislatures in the budget process.

A2.03 Examples of audit objectives related to internal control[181] include an assessment of the extent to which internal control provides reasonable assurance about whether

a. organizational missions, goals, and objectives are achieved effectively and efficiently;

b. resources are used in compliance with laws, regulations, or other requirements;

c. resources, including sensitive information accessed or stored outside the organization's physical perimeter, are safeguarded against unauthorized acquisition, use, or disposition;

d. management information, such as performance measures, and public reports are complete, accurate, and consistent to support performance and decision making;

e. the integrity of information from computerized systems is achieved; and

f. contingency planning for information systems provides essential back-up to prevent unwarranted disruption of the activities and functions that the systems support.

A2.04 Compliance objectives[182] include determining whether

[181]See paragraph 2.11b for additional discussion of internal control audit objectives.

[182]See paragraph 2.11c for additional discussion of compliance audit objectives.

a. the purpose of the program, the manner in which it is to be conducted, the services delivered, the outcomes, or the population it serves is in compliance with provisions of laws, regulations, contracts or grant agreements, or other requirements;

b. government services and benefits are distributed or delivered to citizens based on the individual's eligibility to obtain those services and benefits;

c. incurred or proposed costs are in compliance with applicable laws, regulations, contracts, or grant agreements; and

d. revenues received are in compliance with applicable laws, regulations, contracts or grant agreements.

A2.05 Examples of objectives pertaining to prospective analysis[183] include providing conclusions based on

a. current and projected trends and future potential impact on government programs and services;

b. program or policy alternatives, including forecasting program outcomes under various assumptions;

c. policy or legislative proposals, including advantages, disadvantages, and analysis of stakeholder views;

d. prospective information prepared by management;

e. budgets and forecasts that are based on (1) assumptions about expected future events and (2) management's expected reaction to those future events; and

[183]See paragraph 2.11d for additional discussion of prospective analysis audit objectives.

f. management's assumptions on which prospective information is based.

GAGAS Compliance Statements

A2.06 The determination of whether an unmodified or modified GAGAS compliance statement is appropriate is based on the consideration of the individual and aggregate effect of exceptions to GAGAS requirements.[184] Quantitative and qualitative factors that the auditor may consider include:

a. the likelihood that the exception(s) will affect the perceptions of report users about the audit findings, conclusions, and recommendations;

b. the magnitude of the effect of the exception(s) on the perceptions of report users about the audit findings, conclusions, and recommendations;

c. the pervasiveness of the exception(s);

d. the potential effect of the exception(s) on the sufficiency and appropriateness of evidence supporting the audit findings, conclusions, and recommendations; and

e. whether report users could be misled if the GAGAS compliance statement were not modified.

Information to Accompany Chapter 3

A3.01 Chapter 3 discusses the general standards applicable to financial audits, attestation engagements, and performance audits in accordance with GAGAS. The following supplemental guidance is provided to assist auditors and audited entities in avoiding

[184]See paragraphs 2.24 and 2.25 for additional discussion on citing compliance with GAGAS.

impairments to independence, establishing a system of quality control, and identifying peer review risk factors.

Threats to Independence

A3.02 This list is intended to illustrate by example the types of circumstances that create threats to independence that an auditor might identify when applying the conceptual framework.[185] It does not include all circumstances that create threats to independence; these circumstances will be unique to the conditions under which each evaluation takes place.

A3.03 Examples of circumstances that create self-interest threats for an auditor include:

a. A member of the audit team having a direct financial interest in the audited entity. This would not preclude auditors from auditing pension plans that they participate in if (1) the auditor has no control over the investment strategy, benefits, or other management issues associated with the pension plan and (2) the auditor belongs to such pension plan as part of his/her employment with the audit organization, provided that the plan is normally offered to all employees in equivalent employment positions.

b. An audit organization having undue dependence on income from a particular audited entity.

c. A member of the audit team entering into employment negotiations with an audited entity.

d. An auditor discovering a significant error when evaluating the results of a previous professional service performed by a member of the auditor's audit organization.

[185]See paragraphs 3.07 through 3.26.

A3.04 Examples of circumstances that create self-review threats for an auditor include:

a. An audit organization issuing a report on the effectiveness of the operation of financial or performance management systems after designing or implementing the systems.

b. An audit organization having prepared the original data used to generate records that are the subject matter of the audit.

c. An audit organization performing a service for an audited entity that directly affects the subject matter information of the audit.

d. A member of the audit team being, or having recently been, employed by the audited entity in a position to exert significant influence over the subject matter of the audit.

A3.05 Examples of circumstances that create bias threats for an auditor include:

a. An auditor's having preconceptions about the objectives of a program under audit that are sufficiently strong to impact the auditor's objectivity.

b. An auditor's having biases associated with political, ideological, or social convictions that result from membership or employment in, or loyalty to, a particular type of policy, group, organization, or level of government that could impact the auditor's objectivity.

A3.06 Examples of circumstances that create familiarity threats for an auditor include:

a. A member of the audit team having a close or immediate family member who is a principal or senior manager of the audited entity.

b. A member of the audit team having a close or immediate family member who is an employee of the audited entity and is in a position to exert significant influence over the subject matter of the audit.

c. A principal or employee of the audited entity in a position to exert significant influence over the subject matter of the audit having recently served on the audit team.

d. An auditor accepting gifts or preferential treatment from an audited entity, unless the value is trivial or inconsequential.

e. Senior audit personnel having a long association with the audited entity.

A3.07 Examples of circumstances that create undue influence threats for an auditor or audit organization include existence of:

a. External interference or influence that could improperly limit or modify the scope of an audit or threaten to do so, including exerting pressure to inappropriately reduce the extent of work performed in order to reduce costs or fees.

b. External interference with the selection or application of audit procedures or in the selection of transactions to be examined.

c. Unreasonable restrictions on the time allowed to complete an audit or issue the report.

d. External interference over the assignment, appointment, compensation, and promotion of audit personnel.

e. Restrictions on funds or other resources provided to the audit organization that adversely affect the audit organization's ability to carry out its responsibilities.

f. Authority to overrule or to inappropriately influence the auditors' judgment as to the appropriate content of the report.

g. Threat of replacing the auditors over a disagreement with the contents of an auditors' report, the auditors' conclusions, or the application of an accounting principle or other criteria.

h. Influences that jeopardize the auditors' continued employment for reasons other than incompetence, misconduct, or the need for audits or attestation engagements.

A3.08 Examples of circumstances that create management participation threats for an auditor include:

a. A member of the audit team being, or having recently been, a principal or senior manager of the audited entity.

b. An audit organization principal or employee serving as a voting member of an entity's management committee or board of directors, making policy decisions that affect future direction and operation of an entity's programs, supervising entity employees, developing or approving programmatic policy, authorizing an entity's transactions, or maintaining custody of an entity's assets.

c. An audit organization principal or employee recommending a single individual for a specific position that is key to the entity or program under audit, or otherwise ranking or influencing management's selection of the candidate.

d. An auditor preparing management's corrective action plan to deal with deficiencies detected in the audit.

A3.09 Examples of circumstances that create structural threats for an auditor include:

a. For both external and internal audit organizations, structural placement of the audit function within the reporting line of the areas under audit.

b. For internal audit organizations, administrative direction from the audited entity's management.

System of Quality Control

A3.10 Chapter 3 discusses the elements of an audit organization's system of quality control.[186] The following supplemental guidance is provided to assist auditors and audit organizations in establishing policies and procedures in its system of quality control to address the following elements: initiation, acceptance, and continuance of audits; audit performance, documentation, and reporting; and monitoring.

a. Government audit organizations initiate audits as a result of (1) legal mandates, (2) requests from legislative bodies or oversight bodies, and (3) the audit organization's discretion. In the case of legal mandates and requests, a government audit organization may be required to perform the audit and may not be permitted

[186]See paragraphs 3.82 through 3.95 for additional discussion of the system of quality control.

to make decisions about acceptance or continuance and may not be permitted to resign or withdraw from the audit.

b. GAGAS standards for audit performance, documentation, and reporting are in chapter 4 for financial audits, chapter 5 for attestation engagements, and chapters 6 and 7 for performance audits. Chapter 3 specifies that an audit organization's quality control system include policies and procedures designed to provide the audit organization with reasonable assurance that audits are performed and reports are issued in accordance with professional standards and legal and regulatory requirements.[187] Examples of such policies and procedures include the following:

(1) communication provided to team members so that they sufficiently understand the objectives of their work and the applicable professional standards;

(2) audit planning and supervision;

(3) appropriate documentation of the work performed;

(4) review of the work performed, the significant judgments made, and the resulting audit documentation and report;

(5) review of the independence and qualifications of any external specialists or contractors used, as well as a review of the scope and quality of their work;

(6) procedures for resolving difficult or contentious issues or disagreements among team members, including specialists;

[187]See paragraphs 3.82 through 3.95 for additional discussion of quality control policies and procedures.

(7) obtaining and addressing comments from the audited entity on draft reports; and

(8) reporting supported by the evidence obtained, and in accordance with applicable professional standards and legal or regulatory requirements.

c. Monitoring is an ongoing, periodic assessment of audits designed to provide management of the audit organization with reasonable assurance that the policies and procedures related to the system of quality control are suitably designed and operating effectively in practice.[188] The following guidance is provided to assist audit organizations with implementing and continuing its monitoring of quality:

(1) Who: Monitoring is most effective when performed by persons who do not have responsibility for the specific activity being monitored (e.g., for specific audits or specific centralized processes). The staff member or team of staff members assigned with responsibility for the monitoring process collectively need sufficient and appropriate competence and authority in the audit organization to assume that responsibility. Generally the staff member or the team of staff members performing the monitoring are apart from the normal audit supervision associated with individual audits.

(2) How much: The extent of monitoring procedures varies based on the audit organization's circumstances to enable the audit organization to assess compliance with applicable professional standards and the audit organization's quality control policies and procedures. Examples of specific monitoring procedures include

[188]See paragraphs 3.93 through 3.95 for additional discussion of monitoring.

(a) examination of selected administrative and personnel records pertaining to quality control;

(b) review of selected audit documentation and reports;

(c) discussions with the audit organization's personnel (as applicable and appropriate);

(d) periodic summarization of the findings from the monitoring procedures in writing (at least annually), and consideration of the systematic causes of findings that indicate improvements are needed;

(e) determination of any corrective actions to be taken or improvements to be made with respect to the specific audits reviewed or the audit organization's quality control policies and procedures;

(f) communication of the identified findings to appropriate audit organization management with subsequent follow-up; and

(g) consideration of findings by appropriate audit organization management personnel who also determine whether actions necessary, including necessary modifications to the quality control system, are performed on a timely basis.

(3) Review of selected administrative and personnel records: The review of selected administrative and personnel records pertaining to quality control may include tests of

(a) compliance with policies and procedures on independence;

(b) compliance with continuing professional development policies, including training;

(c) procedures related to recruitment and hiring of qualified personnel, including hiring of specialists or consultants when needed;

(d) procedures related to performance evaluation and advancement of personnel;

(e) procedures related to initiation, acceptance, and continuance of audits;

(f) audit organization personnel's understanding of the quality control policies and procedures, and implementation of these policies and procedures; and

(g) audit organization's process for updating its policies and procedures.

(4) Follow-up on previous findings: Monitoring procedures include an evaluation of whether the audit organization has taken appropriate corrective action to address findings and recommendations from previous monitoring and peer reviews. Personnel involved in monitoring use this information as part of the assessment of risk associated with the design and implementation of the audit organization's quality control system and in determining the nature, timing, and extent of monitoring procedures.

(5) Communication: The audit organization communicates internally the results of the monitoring of its quality control systems that allows the audit organization to take prompt and appropriate action where necessary. Information included in this communication includes:

(a) a description of the monitoring procedures performed;

(b) the conclusions drawn from the monitoring procedures; and

(c) where relevant, a description of the systemic, repetitive, or other significant deficiencies and of the actions taken to resolve those deficiencies.

Peer Review

A3.11 Examples of the factors to consider when performing an assessment of peer review risk for selecting audits for peer review[189] include:

a. scope of the audits including size of the audited entity or audits covering multiple locations;

b. functional area or type of government program;

c. types of audits provided, including the extent of nonaudit services provided to audited entities;

d. personnel (including use of new personnel or personnel not routinely assigned the types of audits provided);

e. initial audits;

f. familiarity resulting from a longstanding relationship with the audited entity;

g. political sensitivity of the audits;

h. budget constraints for the audit organization;

i. results of the peer review team's review of the design of system of quality control;

[189]See paragraph 3.99 for additional discussion of the assessment of peer review risk.

j. results of the audit organization's monitoring process; and

k. risk sensitivity of the audit organization.

A3.12 As discussed in paragraph 3.105, an external audit organization should make its most recent peer review report publicly available. Examples of how to achieve this transparency requirement include posting the peer review report on an external Web site or to a publicly available file. To help the public understand the peer review reports, an audit organization may also include a description of the peer review process and how it applies to its organization. The following provides examples of additional information that audit organizations may include to help users understand the meaning of the peer review report.

a. Explanation of the peer review process.

b. Description of the audit organization's system of quality control.

c. Explanation of the relationship of the peer review results to the audited organization's work.

d. If the peer review report that includes deficiencies or significant deficiencies is modified, explanation of the reviewed audit organization's plan for improving quality controls and the status of the improvements.

Information to Accompany Chapter 6

A6.01 Chapter 6 discusses the field work standards for performance audits. An integral concept for performance auditing is the use of sufficient, appropriate evidence based on the audit objectives to support a sound basis for audit findings, conclusions, and recommendations. The following discussion is provided to assist auditors in identifying criteria and the

various types of evidence, including assessing the appropriateness of evidence in relation to the audit objectives.

Types of Criteria

A6.02 The following are some examples of criteria:[190]

a. purpose or goals prescribed by law or regulation or set by officials of the audited entity,

b. policies and procedures established by officials of the audited entity,

c. technically developed standards or norms,

d. expert opinions,

e. prior periods' performance,

f. defined business practices,

g. contract or grant terms, and

h. performance of other entities or sectors used as defined benchmarks.

A6.03 Audit objectives may pertain to describing the current status or condition of a program or process. For this type of audit objective, criteria may also be represented by the assurance added by the auditor's (1) description of the status or condition, (2) evaluation of whether the status or condition meets certain characteristics, or (3) evaluation of whether management's description is verifiable, accurate, or supported.

[190]See paragraph 6.37 for additional discussion on identifying audit criteria.

Types of Evidence

A6.04 In terms of its form and how it is collected, evidence may be categorized as physical, documentary, or testimonial. Physical evidence is obtained by auditors' direct inspection or observation of people, property, or events. Such evidence may be documented in summary memos, photographs, videos, drawings, charts, maps, or physical samples. Documentary evidence is obtained in the form of already existing information such as letters, contracts, accounting records, invoices, spreadsheets, database extracts, electronically stored information, and management information on performance. Testimonial evidence is obtained through inquiries, interviews, focus groups, public forums, or questionnaires. Auditors frequently use analytical processes including computations, comparisons, separation of information into components, and rational arguments to analyze any evidence gathered to determine whether it is sufficient and appropriate.[191] The strength and weakness of each form of evidence depends on the facts and circumstances associated with the evidence and professional judgment in the context of the audit objectives.

Appropriateness of Evidence in Relation to the Audit Objectives

A6.05 One of the primary factors influencing the assurance associated with a performance audit is the appropriateness of the evidence in relation to the audit objectives.[192] For example:

a. The audit objectives might focus on verifying specific quantitative results presented by the audited entity. In these situations, the audit procedures would likely focus

[191]See paragraphs 6.67 and 6.60 for definitions of sufficient and appropriate.

[192]See paragraphs 6.60 through 6.66 for additional discussion on the appropriateness of evidence.

on obtaining evidence about the accuracy of the specific amounts in question. This work may include the use of statistical sampling.

b. The audit objectives might focus on the performance of a specific program or activity in the agency being audited. In these situations, the auditor may be provided with information compiled by the agency being audited in order to answer the audit objectives. The auditor may find it necessary to test the quality of the information, which includes both its validity and reliability.

c. The audit objectives might focus on information that is used for widely accepted purposes and obtained from sources generally recognized as appropriate. For example, economic statistics issued by government agencies for purposes such as adjusting for inflation, or other such information issued by authoritative organizations, may be the best information available. In such cases, it may not be practical or necessary for auditors to conduct procedures to verify the information. These decisions call for professional judgment based on the nature of the information, its common usage or acceptance, and how it is being used in the audit.

d. The audit objectives might focus on comparisons or benchmarking between various government functions or agencies. These types of audits are especially useful for analyzing the outcomes of various public policy decisions. In these cases, auditors may perform analyses, such as comparative statistics of different jurisdictions or changes in performance over time, where it would be impractical to verify the detailed data underlying the statistics. Clear disclosure as to what extent the comparative information or statistics were evaluated or corroborated will likely be necessary to place the evidence in context for report users.

e. The audit objectives might focus on trend information based on data provided by the audited entity. In this situation, auditors may assess the evidence by using overall analytical tests of underlying data, combined with a knowledge and understanding of the systems or processes used for compiling information.

f. The audit objectives might focus on the auditor identifying emerging and cross-cutting issues using information compiled or self-reported by agencies. In such cases, it may be helpful for the auditor to consider the overall appropriateness of the compiled information along with other information available about the program. Other sources of information, such as inspector general reports or other external audits, may provide the auditors with information regarding whether any unverified or self-reported information is consistent with or can be corroborated by these other external sources of information.

Findings

A6.06 When the audit objectives include explaining why a particular type of positive or negative program performance, output, or outcome identified in the audit occurred, they are referred to as "cause."[193] Identifying the cause of problems may assist auditors in making constructive recommendations for correction. Because deficiencies can result from a number of plausible factors or multiple causes, the recommendation can be more persuasive if auditors can clearly demonstrate and explain with evidence and reasoning the link between the deficiencies and the factor or factors they have identified as the cause or causes. Auditors may also identify deficiencies in program design or structure as the cause of deficient performance. Auditors may also identify deficiencies in internal control that are

[193]See paragraph 6.76 for additional discussion of "cause."

significant to the subject matter of the performance audit as the cause of deficient performance. In developing these types of findings, the deficiencies in program design or internal control would be described as the "cause." Often the causes of deficient program performance are complex and involve multiple factors, including fundamental, systemic root causes. Alternatively, when the audit objectives include estimating the program's effect on changes in physical, social, or economic conditions, auditors seek evidence of the extent to which the program itself is the "cause" of those changes.

A6.07 When the audit objectives include estimating the extent to which a program has caused changes in physical, social, or economic conditions, "effect" is a measure of the impact achieved by the program. In this case, "effect" is the extent to which positive or negative changes in actual physical, social, or economic conditions can be identified and attributed to the program.

Information to Accompany Chapter 7

A7.01 Chapter 7 discusses the reporting standards for performance audits. The following discussion is provided to assist auditors in developing and writing their audit report for performance audits.

Report Quality Elements

A7.02 The auditor may use the report quality elements of timely, complete, accurate, objective, convincing, clear, and concise when developing and writing the audit report as the subject permits.[194]

a. Accurate: An accurate report is supported by sufficient, appropriate evidence with key facts, figures,

[194]See paragraph 7.08 for additional discussion of report contents.

and findings being traceable to the audit evidence. Reports that are fact-based, with a clear statement of sources, methods, and assumptions so that report users can judge how much weight to give the evidence reported, assist in achieving accuracy. Disclosing data limitations and other disclosures also contribute to producing more accurate audit reports. Reports also are more accurate when the findings are presented in the broader context of the issue. One way to help audit organizations prepare accurate audit reports is to use a quality control process such as referencing. Referencing is a process in which an experienced auditor who is independent of the audit checks that statements of facts, figures, and dates are correctly reported, that the findings are adequately supported by the evidence in the audit documentation, and that the conclusions and recommendations flow logically from the evidence.

b. Objective: Objective means that the presentation of the report is balanced in content and tone. A report's credibility is significantly enhanced when it presents evidence in an unbiased manner and in the proper context. This means presenting the audit results impartially and fairly. The tone of reports may encourage decision makers to act on the auditors' findings and recommendations. This balanced tone can be achieved when reports present sufficient, appropriate evidence to support conclusions while refraining from using adjectives or adverbs that characterize evidence in a way that implies criticism or unsupported conclusions. The objectivity of audit reports is enhanced when the report explicitly states the source of the evidence and the assumptions used in the analysis. The report may recognize the positive aspects of the program reviewed if applicable to the audit objectives. Inclusion of positive program aspects may lead to improved performance by other government organizations that read the report. Audit reports are more objective when they demonstrate that the work

has been performed by professional, unbiased, independent, and knowledgeable staff.

c. Complete: Being complete means that the report contains sufficient, appropriate evidence needed to satisfy the audit objectives and promote an understanding of the matters reported. It also means the report states evidence and findings without omission of significant relevant information related to the audit objectives. Providing report users with an understanding means providing perspective on the extent and significance of reported findings, such as the frequency of occurrence relative to the number of cases or transactions tested and the relationship of the findings to the entity's operations. Being complete also means clearly stating what was and was not done and explicitly describing data limitations, constraints imposed by restrictions on access to records, or other issues.

d. Convincing: Being convincing means that the audit results are responsive to the audit objectives, that the findings are presented persuasively, and that the conclusions and recommendations flow logically from the facts presented. The validity of the findings, the reasonableness of the conclusions, and the benefit of implementing the recommendations are more convincing when supported by sufficient, appropriate evidence. Reports designed in this way can help focus the attention of responsible officials on the matters that warrant attention and can provide an incentive for taking corrective action.

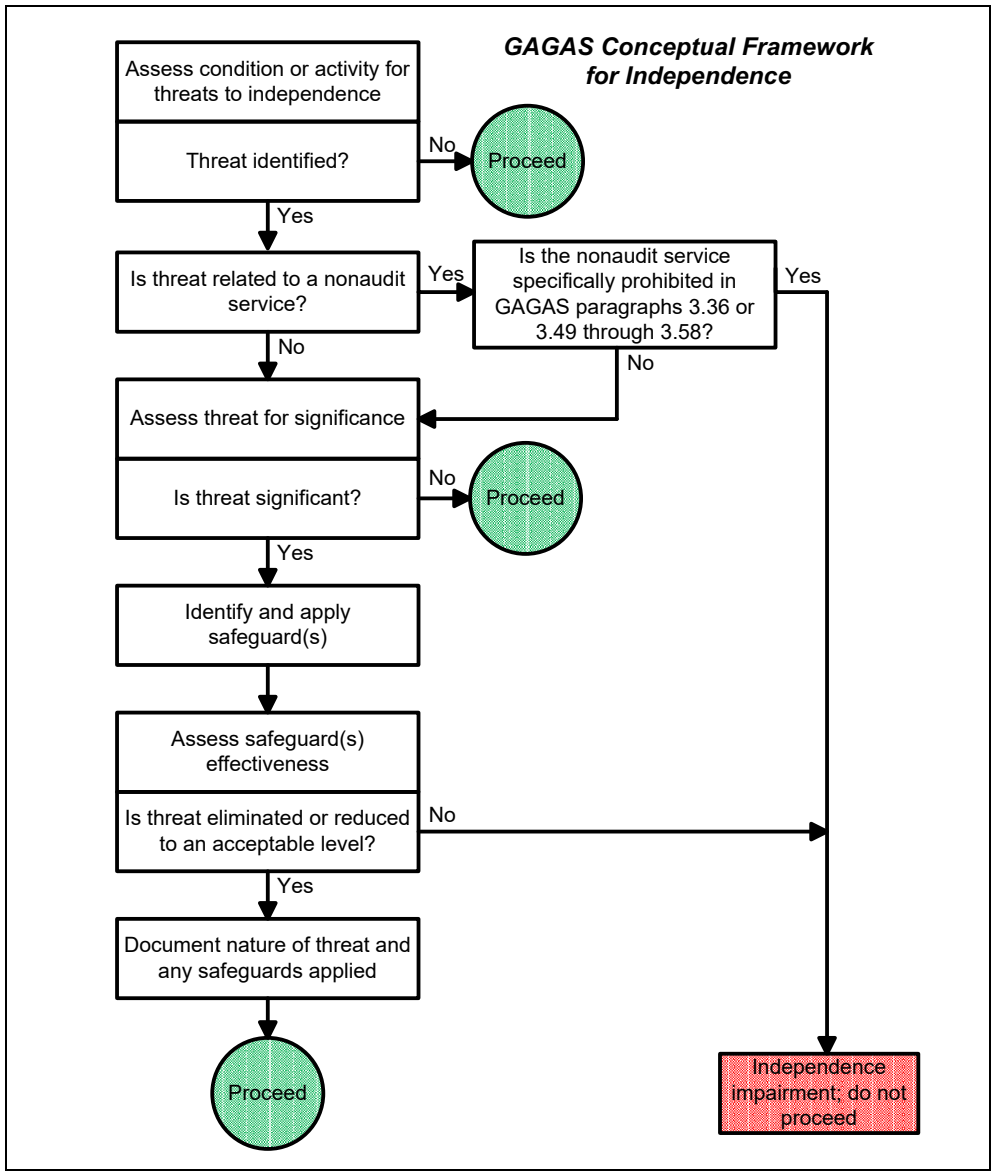
e. Clear: Clarity means the report is easy for the intended user to read and understand. Preparing the report in language as clear and simple as the subject permits assists auditors in achieving this goal. Use of straightforward, nontechnical language is helpful to simplify presentation. Defining technical terms,

abbreviations, and acronyms that are used in the report is also helpful. Auditors may use a highlights page or summary within the report to capture the report user's attention and highlight the overall message. If a summary is used, it is helpful if it focuses on the specific answers to the questions in the audit objectives, summarizes the audit's most significant findings and the report's principal conclusions, and prepares users to anticipate the major recommendations. Logical organization of material, and accuracy and precision in stating facts and in drawing conclusions assist in the report's clarity and understanding. Effective use of titles and captions and topic sentences makes the report easier to read and understand. Visual aids (such as pictures, charts, graphs, and maps) may clarify and summarize complex material.

f. Concise: Being concise means that the report is not longer than necessary to convey and support the message. Extraneous detail detracts from a report, may even conceal the real message, and may confuse or distract the users. Although room exists for considerable judgment in determining the content of reports, those that are fact-based but concise are likely to achieve results.

g. Timely: To be of maximum use, providing relevant evidence in time to respond to officials of the audited entity, legislative officials, and other users' legitimate needs is the auditors' goal. Likewise, the evidence provided in the report is more helpful if it is current. Therefore, the timely issuance of the report is an important reporting goal for auditors. During the audit, the auditors may provide interim reports of significant matters to appropriate entity officials. Such communication alerts officials to matters needing immediate attention and allows them to take corrective action before the final report is completed.

GAGAS Conceptual Framework for Independence



Source: GAO.

Comptroller General's Advisory Council on Government Auditing Standards

Advisory Council Members

Auston Johnson, Chair
State of Utah
(2009-2011)

The Honorable Ernest A. Almonte
State of Rhode Island
(member 2005-2008)

Christine C. Boesz
Consultant
(member 2007-2011)

Kathy A. Buller
Peace Corps
(member 2009-2011)

Dr. Paul A. Copley
James Madison University
(member 2005-2008)

David Cotton
Cotton & Co. LLP
(member 2006-2009)

Beryl H. Davis
Institute of Internal Auditors
(member 2007-2011)

Kristine Devine
Deloitte & Touche, LLP
(member 2005-2011)

Dr. Ehsan Feroz
University of Minnesota Duluth
(member 2002-2009)

Alex Fraser
Standard & Poor's
(member 2006-2008)

Mark Funkhouser
Kansas City, Missouri
(member 2005-2008)

Dr. Michael H. Granof
University of Texas at Austin
(member 2005-2008)

Jerome Heer
County of Milwaukee, Wisconsin
(member 2004-2011)

Michael Hendricks
Consultant
(member 2010-2012)

Marion Higa
State of Hawaii
(member 2006-2009)

The Honorable John P. Higgins, Jr.
U.S. Department of Education
(member 2005-2008)

Julia Higgs
Florida Atlantic University
(member 2009-2011)

Russell Hinton
State of Georgia
(member 2004-2011)

Drummond Kahn
City of Portland, Oregon
(member 2009-2011)

Richard A. Leach
United States Navy
(member 2005-2011)

David W. Martin
State of Florida
(member 2010-2012)

Patrick L. McNamee
PricewaterhouseCoopers, LLP
(member 2005-2008)

John R. Miller
KPMG LLP (Retired)
(chair 2001-2008)

Nancy A. Miller
Miller Foley Group
(member 2010-2012)

Rakesh Mohan
State of Idaho
(member 2004-2011)

The Honorable Samuel Mok
Consultant
(member 2006-2009)

Harold L. Monk, Jr.
Davis, Monk & Company
(member 2002-2012)

Stephen L. Morgan
City of Austin, Texas
(member 2001-2008)

Janice Mueller
State of Wisconsin
(member 2009-2011)

George A. Rippey
U.S. Department of Education
(member 2010-2012)

The Honorable Jon T. Rymer
Federal Deposit Insurance Corporation
(member 2009-2011)

Brian A. Schebler
McGladrey & Pullen, LLP
(member 2005-2011)

Barry R. Snyder
Federal Reserve Board
(member 2001-2008)

Dr. Daniel L. Stufflebeam
Western Michigan University
(member 2002-2009)

F. Michael Taylor
City of Stockton, California
(member 2010-2012)

Roland L. Unger
State of Maryland
(member 2010)

Edward J. Valenzuela
State of Florida
(member 2007-2009)

Thomas E. Vermeer
Alfred Lerner College of Business & Economics
(member 2010-2012)

Sandra H. Vice
State of Texas
(member 2010-2012)

John C. Weber
Crowe Horwath LLP
(member 2010-2012)

George Willie
Bert Smith & Co.
(member 2004-2011)

GAO Project Team

Jeanette M. Franzel, Managing Director
James R. Dalkin, Project Director
Robert F. Dacey, Chief Accountant
Marcia B. Buchanan, Assistant Director
Cheryl E. Clark, Assistant Director
Heather I. Keister, Assistant Director
Kristen A. Kociolek, Assistant Director
Michael C. Hrapsky, Specialist, Auditing Standards
Eric H. Holbrook, Specialist, Auditing Standards
Maria Hasan, Auditor
Laura S. Pacheco, Auditor
Christie A. Pugnetti, Auditor
Margaret A. Mills, Senior Communications Analyst
Jennifer V. Allison, Council Administrator

Index

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order Printed Copies

The printed version of the December 2011 revision of *Government Auditing Standards* can be ordered through the Government Printing Office (GPO) online or by calling 202-512-1800 or 1-866-512-1800 toll free.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

United States Government Accountability Office

By the Comptroller General of the United States

September 2013

STANDARDS FOR INTERNAL CONTROL IN THE FEDERAL GOVERNMENT

2013 Exposure Draft

GAO-13-830SP

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

September 2013

To Federal Officials and Others Interested in *Standards for Internal Control in the Federal Government*

GAO invites your comments on the accompanying proposed changes to *Standards for Internal Control in the Federal Government*, commonly known as the "Green Book." This letter describes the process used by GAO for revising the Green Book, summarizes the proposed major changes, discusses proposed effective dates, and provides instructions for submitting comments on the proposed standards.

Process for Revising the Green Book

To help ensure that the standards continue to meet the needs of the federal community and the public it serves, the Comptroller General of the United States established the Advisory Council on Standards for Internal Control in the Federal Government (Green Book Advisory Council) to review GAO's revision of the standards and consider any other necessary changes. The Green Book Advisory Council includes experts in financial management drawn from federal, state, and local government; the private sector; public accounting; and academia. This exposure draft includes the Green Book Advisory Council's input regarding the proposed changes. We are currently requesting public comments on the proposed revisions in the exposure draft.

Summary of Major Changes

The proposed revision to the Green Book will be the third since GAO first issued the standards in 1983. The proposed changes contained in the 2013 Exposure Draft update the Green Book to reflect major developments in the accountability and financial management profession and emphasize specific considerations applicable to the government environment.

Enclosure I to this letter contains a discussion of the major changes.

Effective Dates

When issued in final form, this revision will supersede the November 1999 revision of the standards. The effective date for this revision, as well as transition guidance to help officials implement the revised standards, will be included when the Green Book is issued in final form.

Instructions for Commenting

The draft of the proposed changes to *Standards for Internal Control in the Federal Government*, 2013 Exposure Draft, is only available in electronic format and can be downloaded from GAO's Green Book web page at: http://www.gao.gov/greenbook.

- - - - -

We are requesting comments on this draft from federal officials; managers and auditors at all levels of government; the public accounting profession; academia; professional organizations; public interest groups; and other interested parties. To assist you in developing your comments, specific issues are presented in enclosure II to this letter. We encourage you to comment on these issues and any additional issues that you note. Please associate your comments with specific references to question numbers in the enclosure and/or paragraph numbers in the proposed standards and provide your rationale for any suggested changes, along with suggested revised language. All comments received from the public will be considered a matter of public record and will ultimately be posted on the GAO website.

Please send your comment letters to our Green Book inbox: GreenBook@gao.gov no later than December 2, 2013.

If you need additional information please contact me at (202) 512-3133 or dalkinj@gao.gov.

James Dalkin
Director, Financial Management and Assurance

Enclosures - 2

Enclosure I: Summary of Major Changes

The 2013 revision of the *Standards for Internal Control in the Federal Government* represents a modernized version of the standards. These standards take into account the developments made in government in the area of internal control. These standards provide management criteria for designing, implementing, and operating an internal control system and reinforce management's accountability for internal control.

This revision does not change the previous standards on a conceptual level. The revised standards retain the five components of internal control, but introduce 17 principles to assist management in achieving an effective internal control system. These principles were adopted from the Committee of Sponsoring Organizations of the Treadway Commission's revision of its *Internal Control: Integrated Framework* and adapted for the government environment. The revised standards also introduce attributes that support these principles and further define the requirements for an effective internal control system.

Enclosure II: Questions for Commenters

The following questions are provided to guide users in commenting on the 2013 Exposure Draft of the *Standards for Internal Control in the Federal Government*. We encourage you to comment on these issues and any additional issues that you note. Please associate your comments with specific references to question numbers, paragraph numbers, or both in the proposed standards and provide your rationale for any proposed changes, along with suggested revised language.

1. Is the hierarchy of components, principles, and attributes clearly explained?

2. Are there any internal control concepts unique to the government environment that should be in the Green Book that are not currently included?

3. Does the framework provide the necessary information to allow program managers to evaluate the internal controls for their programs?

4. Does the Green Book provide adequate criteria for auditors?

5. Are the requirements for management to design, implement, and operate an internal control system clear, understandable, and adequate?

6. Is the evaluation of deficiencies discussion clear, understandable, and adequate?

7. Are the roles, divisions, and overlaps of responsibility for the oversight body, management, and personnel clear, understandable, and adequate?

8. Are the documentation requirements included in the Green Book clear, understandable, and adequate?

9. Is there a need for additional internal control implementation guidance? If so, what form should it take?

10. Is this Green Book written in such a way to allow state, local, and quasi-governmental entities, as well as not-for-profit organizations, to adapt it for their own use?

Contents

Overview

Foreword

Policymakers and program managers are continually seeking ways to improve accountability in achieving an entity's mission. A key factor in improving accountability in achieving an entity's mission is to implement an effective internal control system. An effective internal control system helps an entity adapt to shifting environments, evolving demands, and new priorities. As programs change and entities strive to improve operational processes and implement new technology, management continually evaluates its internal control system to ensure that it is effective and updated when necessary.

Section 3512 (c) and (d) of Title 31 of the United States Code (commonly known as the Federal Managers' Financial Integrity Act (FMFIA)) requires the Comptroller General to issue standards for internal control in government. These standards, known as the *Standards for Internal Control in the Federal Government* (Green Book), provide the overall framework for establishing and maintaining an effective internal control system. Office of Management and Budget (OMB) Circular No. A-123, *Management's Responsibility for Internal Control*, provides specific requirements for assessing and reporting on controls in the federal government. The term "internal control" in this document covers all aspects of an entity's objectives (operations, reporting, and compliance).

The Green Book may also be applied by state, local, and quasi-governmental entities, as well as not-for-profit organizations, as a framework for an internal control system. Management of these entities determines, based on applicable laws and regulations, how to appropriately adapt the framework presented in the Green Book for an entity.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) updated its internal control guidance in 2013 with the issuance of a revised *Internal Control - Integrated Framework*.[1] COSO has introduced the concept of principles related to the five components of internal control.

[1] See Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Internal Control – Integrated Framework* (May 2013)

We have adapted these principles in developing this update. When finalized, the updated Green Book will supersede those previously issued.[2]

[2] See GAO *Standards for Internal Control in the Federal Government,* GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999)

How to Use the Green Book

We are issuing the Green Book to provide managers with internal control criteria to help them design, implement, and operate an effective internal control system. Our goal is to define the standards of internal control through the components, principles, and relevant attributes of internal control and explain why they are integral to an entity's internal control system. We recognize that in discussing internal control, we are separating internal control from the operational processes in which it occurs. We have done so to clarify what processes management considers part of internal control. In a mature and highly effective internal control system, internal control may be indistinguishable from day-to-day activities personnel perform.

We have structured the Green Book as follows:

1. An overview, including:

- Section 1: an overview of the fundamental concepts of internal control
- Section 2: a discussion of internal control components, principles, and attributes; how these relate to an entity's objectives; and the three categories of objectives
- Section 3: a discussion of how management evaluates the internal control system's design, implementation, and operation
- Section 4: additional considerations that apply to all components in an internal control system

2. A discussion of the requirements for each of the five components, 17 principles, and related attributes as well as additional discussion of the requirements

We have clearly marked the requirements for the Green Book through the use of "must" and "should." For further discussion of the requirements, please refer to sections 2 and 3 of the Overview.

Section 1 - Fundamental Concepts of Internal Control

Definition of Internal Control

O1.01 Internal control is an integral component of an entity's management that provides reasonable assurance that the objectives of an entity are being achieved. These objectives and related risks can be broadly classified into one or more of the three following categories:

- Operations - Effectiveness and efficiency of operations
- Reporting - Reliability of reporting for internal and external use
- Compliance - Compliance with applicable laws and regulations

O1.02 These are distinct but overlapping categories. A particular objective can fall under more than one category, can address different needs, and may be the direct responsibility of different individuals.

O1.03 Internal control comprises the plans, methods, policies, and procedures used to fulfill the mission, strategic plan, goals, and objectives of the organization. Internal control serves as the first line of defense in safeguarding assets. In short, internal control helps federal managers achieve desired results through effective stewardship of public resources.

An Internal Control System

O1.04 An internal control system is a continuous built-in component of operations, effected by people, that provides reasonable assurance, not absolute assurance, that an organization's objectives will be achieved.

O1.05 Internal control is not one event, but a series of actions that occur throughout an entity's operations. Internal control is recognized as an integral part of the operational processes management uses to regulate and guide its operations rather than as a separate system within an entity. In this sense, internal control is built into the entity as a part of the organizational structure to help managers achieve the entity's objectives on an ongoing basis.

O1.06 People are what make internal control work. Management is responsible for an effective internal control system. As part of this responsibility, management sets the entity's objectives, implements

controls, and evaluates the internal control system. However, personnel throughout an organization play important roles in implementing and operating an effective internal control system.

O1.07 An effective internal control system increases the likelihood that an entity will achieve its objectives. However, no matter how well designed, implemented, or operated, an internal control system cannot provide absolute assurance that all of an organization's objectives will be met. Factors outside the control or influence of management can affect the entity's ability to achieve all of its objectives. For example, a natural disaster can affect an organization's ability to achieve its objectives. Therefore, once in place, effective internal control provides reasonable, not absolute, assurance that an organization will achieve its objectives.

Section 2 - Establishing an Effective Internal Control System

Presentation of Standards

O2.01 The Green Book defines the standards for internal control in the federal government. FMFIA requires federal executive branch entities to establish internal control in accordance with these standards. The standards provide criteria for assessing the design, implementation, and operating effectiveness of internal control in federal government entities to determine if an internal control system is effective. An entity must have an effective internal control system to comply with the standards.

O2.02 The Green Book applies to all aspects of an entity's objectives: operations, reporting, and compliance. However, these standards are not intended to limit or interfere with duly granted authority related to legislation, rule-making, or other discretionary policy-making in an organization. In implementing the Green Book, management is responsible for designing the policies and procedures to fit an entity's operations and building them in as an integral part of the entity's operations.

Components, Principles, and Attributes

O2.03 An entity determines its mission, sets a strategic plan, establishes entity objectives, and formulates plans to achieve its objectives. Management, with oversight from the entity's oversight body, may set objectives for an entity as a whole, or target activities within the entity.

Management uses internal control to help the organization achieve these objectives. While there are different ways to present internal control, the Green Book approaches internal control through a hierarchical structure of five components, 17 principles, and relevant attributes.

O2.04 The five components of internal control are:

- Control Environment - The foundation for an internal control system. It provides the discipline and structure to help an entity achieve its objectives.
- Risk Assessment - Assesses the risks facing the entity as it seeks to achieve its objectives. This assessment provides the basis for developing appropriate risk responses.
- Control Activities - The actions management establishes through policies and procedures to achieve objectives and respond to risks in the internal control system, which includes the entity's information system.
- Information and Communication - The quality information management uses to support the internal control system. Communicating quality information is vital for an entity to run and control its operations.
- Monitoring - Assesses the quality of performance over time and ensures that the findings of audits and other reviews are promptly resolved.

O2.05 These five components represent the highest level of the hierarchy of standards for internal control in the federal government. The principles and underlying attributes represent the requirements necessary to achieve the standards of internal control. In the Green Book, these requirements are identified through use of specific language. The Green Book uses the word "should" to denote a principle or attribute statement.

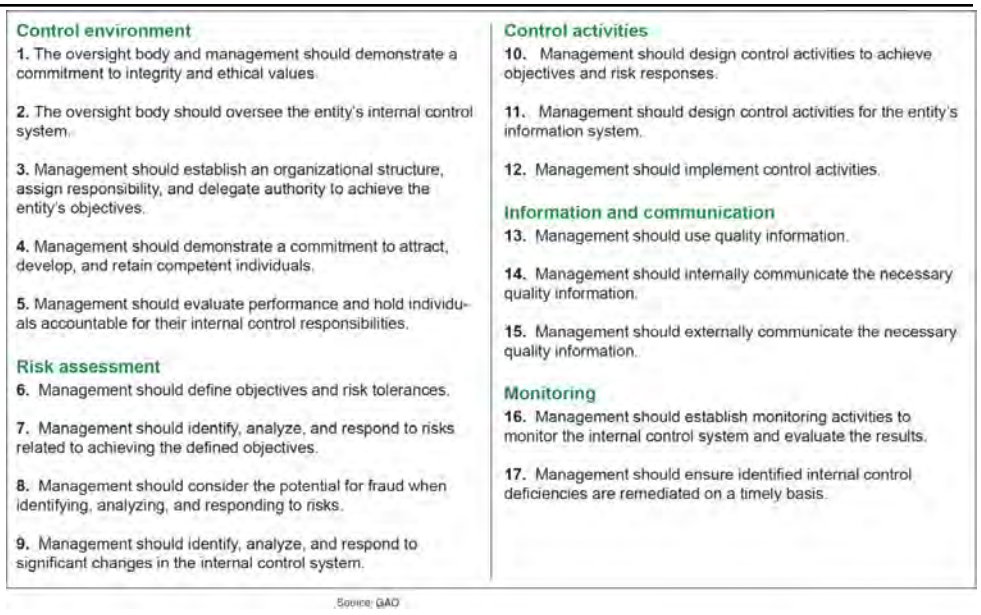
O2.06 In general, all components, principles, and attributes are relevant for an effective internal control system. However, there may be an operating or regulatory situation in which management has determined that a principle or attribute is not relevant for the entity to achieve its objectives and address related risks. Relevance refers to management's determination that each principle and attribute has a significant bearing on the design, implementation, and operation of its associated component. If management decides a principle or attribute is not relevant, management

supports that determination with documentation that includes the rationale of how, in the absence of that principle or attribute, the associated component could be designed, implemented, and operated effectively.

O2.07 In addition to principle and attribute requirements, the Green Book contains additional information in the form of application material. Application material provides further explanation of the principle and attribute requirements and may explain more precisely what a requirement means and what it is intended to cover, or include examples of procedures that may be appropriate for an entity. The words “may,” “might,” and “could” are used to describe these procedures. The application material may also provide background information on matters addressed in the Green Book. Although application material does not impose a requirement, it is relevant to the proper implementation of the requirements. Management has a responsibility to understand the application material and exercise judgment in fulfilling the requirements of the principles and attributes.

O2.08 Management has a responsibility to consider the entire text of the Green Book in designing, implementing, and operating an internal control system. The Green Book, however, does not prescribe the process for how management designs, implements, and operates its internal control system.

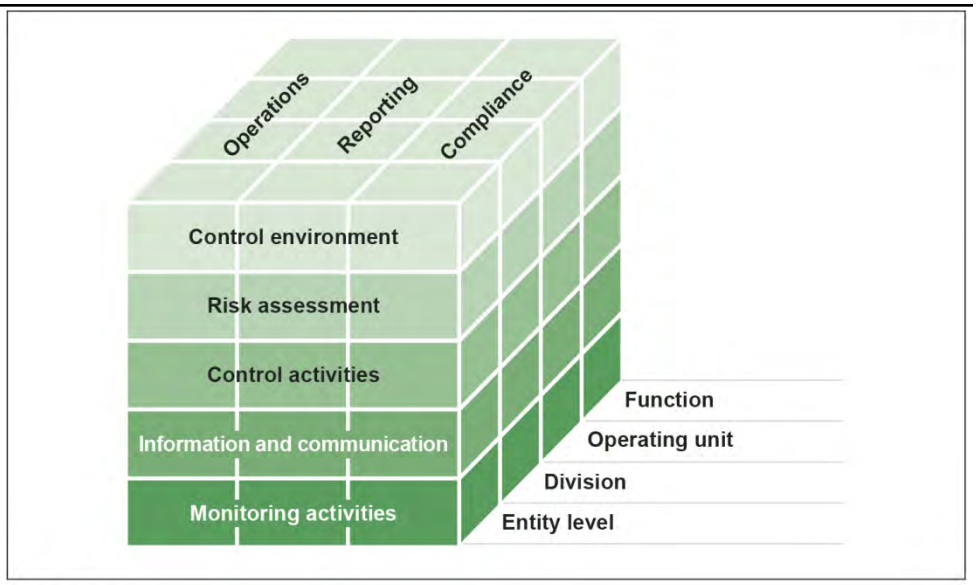
O2.09 Below are the five components of internal control and 17 related principles. The related attributes are covered in the respective component chapters.



Internal Control and the Entity

O2.10 A direct relationship exists among an entity's objectives, the five components of internal control, and the organizational structure of an entity. Objectives are what an entity wants to achieve. The five components of internal control are what is required of the entity to achieve the objectives. Organizational structure encompasses the operating units, operational processes, and other structures management uses to achieve the objectives. This relationship is depicted in the form of a cube developed by COSO.[3]

[3] See paras. 3.03 through 3.07 for further discussion of organizational structure.



Source: COSO.

O2.11 The three categories into which an entity's objectives can be classified are represented by the columns labelled on top of the cube. The five components of internal control are represented by the rows. The organizational structure is represented by the third dimension of the cube.

O2.12 Each component of internal control applies to all three categories of objectives and the organizational structure.

O2.13 Internal control is a dynamic, iterative, and integrated process in which components impact the design, implementation, and operating effectiveness of each other. No two entities will have an identical internal control system due to differences in factors such as mission, regulatory environment, strategic plan, entity size, risk tolerance, and information technology.

Roles in an Internal Control System

O2.14 Because internal control is a part of management's overall responsibility, the five components are discussed in the context of the management of the entity. However, everyone in the organization has a responsibility for internal control. In general, roles in an entity's internal control system can be categorized as follows:

- Oversight body - The oversight body is responsible for overseeing the strategic direction of the entity and obligations related to the

accountability of the entity. This includes overseeing management's design, implementation, and operation of an internal control system. For some entities, an oversight body might be one or a few members of senior management. For other entities, multiple parties may be members of the entity's oversight body. For the purpose of the Green Book, oversight by an oversight body is implicit in each principle and attribute.

- Management - Management is directly responsible for all activities of an organization, including the design, implementation, and operating effectiveness of an entity's internal control system. Managers' responsibilities vary depending on their functions in the organizational structure.
- Personnel - Personnel help management design, implement, and operate an internal control system and are responsible for reporting issues noted in the entity's operations, compliance, or reporting objectives.[4]

O2.15 External auditors and the Office of Inspector General (IG) are not considered a part of an entity's internal control system. While management may evaluate and incorporate recommendations by external auditors and the IG, responsibility for an entity's internal control system resides with management.

Objectives of an Entity

O2.16 Management, with oversight by an oversight body, sets objectives to meet the entity's mission, requirements of applicable laws and regulations, strategic plan, and goals. Management sets objectives before designing an entity's internal control system. Management may include setting objectives as part of the strategic planning process.

O2.17 Management, as part of designing an internal control system, defines the objectives in specific and measureable terms to enable management to identify, analyze, and respond to risks related to achieving those objectives.

Categories of Objectives

O2.18 Management groups objectives into one or more of the three categories of objectives:

[4] See paras. 16.01 through 17.10 for further discussion on identifying issues.

- Operations - Effectiveness and efficiency of operations
- Reporting - Reliability of reporting for internal and external use
- Compliance - Compliance with applicable laws and regulations

Operations Objectives

O2.19 Operations objectives relate to program operations that achieve an entity's mission. An entity's mission may be defined in a strategic plan. Such plans set the goals and objectives for an entity along with the effective and efficient operations necessary to fulfill those objectives. Effective operations produce the intended results from operational processes while efficient operations do so in a manner that minimizes the waste of resources.

O2.20 Management can set, from the objectives, related subobjectives for units within the organizational structure. Management, by linking objectives throughout the entity to the mission, improves the effectiveness and efficiency of program operations in achieving the mission.

Reporting Objectives

O2.21 Reporting objectives relate to the preparation of reports for use by the entity, its stakeholders, or other external parties. Reporting objectives may be grouped further into subcategories:

- External Financial Reporting Objectives - Objectives related to the release of the entity's financial performance in accordance with professional standards, applicable laws and regulations, as well as expectations of stakeholders.
- External Nonfinancial Reporting Objectives - Objectives related to the release of nonfinancial information in accordance with professional standards, applicable laws and regulations, as well as expectations of stakeholders.
- Internal Financial Reporting Objectives and Nonfinancial Reporting Objectives - Objectives related to gathering information needed by management to support decision making and evaluation of the entity's performance.

Compliance Objectives

O2.22 In the government sector, objectives related to compliance with applicable laws and regulations can be more significant than in the private sector. Laws and regulations often prescribe a government entity's objectives, structure, methods to achieve objectives, and reporting of performance relative to achieving objectives. Management considers objectives in the category of compliance comprehensively for the entity and determines what controls would be necessary to design, implement, and operate for the entity to achieve these objectives effectively.

O2.23 Management conducts activities in accordance with applicable laws and regulations. As part of specifying compliance objectives, the entity determines which laws and regulations apply to the entity. Management is expected to set objectives that incorporate these requirements. Some entities may set objectives to a higher level of performance than established by laws and regulations. In setting those objectives, management is able to exercise discretion relative to the performance of the entity.

Safeguarding of Assets

O2.24 A subset of the three categories of objectives is the safeguarding of assets. Management designs an internal control system to provide reasonable assurance regarding prevention or prompt detection of unauthorized acquisition, use, or disposition of an entity's assets.

Setting Subobjectives

O2.25 Management can develop from objectives more specific subobjectives throughout the organizational structure. Management needs to define subobjectives in specific and measurable terms that can be communicated to the personnel who are assigned responsibility to achieve these subobjectives. Both management and personnel require an understanding of an objective, its subobjectives, and defined levels of performance to ensure accountability in an internal control system.

Section 3 - Evaluation of an Effective Internal Control System

Requirements for Effective Internal Control

O3.01 An effective internal control system provides reasonable assurance that the organization will achieve its objectives. It requires that

- each of the five components, 17 principles, and relevant attributes of internal control are effectively designed, implemented, and operating and
- the five components are operating together in an integrated manner.

O3.02 To determine if an internal control system meets these requirements, management evaluates the effect of internal control deficiencies on the internal control system.

Evaluation of Deficiencies in Internal Control

O3.03 Management evaluates control deficiencies identified by management's ongoing monitoring of the internal control system as well as any separate evaluations performed by both internal and external sources. A deficiency in internal control exists when the design, implementation, or operation of a control does not allow management or personnel, in the normal course of performing their assigned functions, to achieve control objectives and address related risks.

O3.04 In the federal government FMFIA mandates that the head of each executive agency annually prepare a statement as to whether the agency's systems of internal accounting and administrative controls comply with the requirements of the act. If the systems do not comply, the head of the agency will include a report in which any material weaknesses in the agency's system of internal accounting and administrative control are identified and the plans and schedule for correcting any such weakness are described.

Design and Implementation

O3.05 When evaluating design of internal control, management determines if controls individually and in combination with other controls are capable of achieving an objective and addressing related risks. When evaluating implementation, management determines if the control exists

and if the entity has placed the control into operation. A control cannot be effectively implemented if it was not effectively designed. A deficiency in design exists when (a) a control necessary to meet a control objective is missing or (b) an existing control is not properly designed so that even if the control operates as designed, the control objective would not be met. A deficiency in implementation exists when a properly designed control is not implemented correctly in the internal control system.

Operation

O3.06 In evaluating operating effectiveness, management determines if controls were applied at relevant times during the period under evaluation, the consistency with which they were applied, and by whom or by what means they were applied. If substantially different controls were used at different times during the period under evaluation, management evaluates operating effectiveness separately for each unique control system. A control cannot be effectively operating if it was not effectively designed and implemented. A deficiency in operation exists when a properly designed control does not operate as designed, or when the person performing the control does not possess the necessary authority or competence to perform the control effectively.

Effect on the Internal Control System

O3.07 Management evaluates the significance of identified deficiencies. Significance refers to the relative importance of a deficiency in the entity achieving a defined objective. To evaluate the significance of the deficiency, management assesses its effect on achieving the defined objectives at both the entity and transaction level. Management evaluates the significance of a deficiency by considering the magnitude of impact, likelihood of occurrence, and nature of the deficiency. Magnitude of impact refers to the likely effect that the deficiency could have on the entity achieving its objectives and is affected by factors such as the size, pace, and duration of the deficiency's impact. A deficiency may be more significant to one objective than another. Likelihood of occurrence refers to the possibility of a deficiency impacting an entity's ability to achieve its objectives. The nature of the deficiency involves factors such as the degree of subjectivity involved with the deficiency and whether the deficiency arises from fraud or misconduct. The oversight body oversees management's evaluation of significance of deficiencies to ensure that deficiencies have been properly considered.

O3.08 Deficiencies are evaluated both on an individual basis and in the aggregate. Management considers the correlation among different deficiencies or groups of deficiencies when evaluating their significance. Deficiency evaluation varies by entity because of differences in entities' objectives.

O3.09 Generally, management first considers whether controls are designed, implemented, and operating effectively to achieve each relevant attribute. The Green Book describes each attribute in general terms. For each attribute, management considers the elements underlying the attribute and whether controls are properly designed, implemented, and operating effectively to achieve each element of the attribute. If one or more of the elements are not achieved, then a deficiency in internal control exists. In determining whether an attribute is achieved, management considers whether the design, implementation, and operation of the controls, in the aggregate, are sufficient to fully achieve the attribute. Such consideration includes an assessment of the impact of identified deficiencies on the achievement of the attribute.

O3.10 For each principle, management makes a summary determination as to whether the principle is designed, implemented, and operating effectively by considering whether the related attributes are achieved. If a principle is not designed, implemented, or operating effectively, then the respective component is not likely to be effective, and an internal control system is unlikely to be effective in helping the entity in achieving its objectives.

O3.11 Based on the results of this evaluation, management then evaluates the design, implementation, and operating effectiveness of each of the five components of internal control and whether they operate together effectively. If one or more of the five components are not effectively designed, implemented, or operating effectively, then an internal control system is ineffective. Judgment is used in making such determinations, which includes exercising reasonable care.

Section 4 - Additional Considerations

Service Organizations

O4.01 Management may engage external parties to perform certain operational processes for the entity, such as accounting and payroll

processing, security services, or healthcare claims processing. For the purpose of the Green Book, these external parties are referred to as "service organizations." Management, however, retains responsibility for the performance of processes assigned to service organizations. Therefore, management needs to understand the controls each service organization has designed, has implemented, and operates for the assigned operational process and how the service organization's internal control system impacts the entity's internal control system.

O4.02 Management also considers the complementary entity user controls identified by the service organization or its auditors. Management determines whether established internal controls are sufficient to ensure the entity achieves objectives and addresses risks related to the outsourced process or to incorporate the complementary user entity controls into the entity's internal control system.

O4.03 Management may consider the following when determining the extent of oversight controls for the service organization:

- The nature of services outsourced
- The service organization's standards of conduct
- Quality and frequency of the service organization's enforcement of adherence to standards of conduct by its personnel
- Magnitude and level of complexity of the entity's operations and organizational structure

Large versus Small Entities

O4.04 The 17 principles apply to both large and small entities. However, smaller entities may have different implementation approaches than larger entities. Smaller entities typically have unique advantages, which can contribute to an effective internal control system. These may include a higher level of involvement by management in operational processes and direct interaction with personnel. Smaller entities may find informal staff meetings effective for communicating quality information, where larger entities may need more formal mechanisms, such as written reports, intranet portals, or periodic formal meetings, to communicate with the organization.

O4.05 A smaller entity, however, faces greater challenges in segregating duties because of its concentration of responsibilities and authorities in the organizational structure.[5] Management, however, can respond to this increased risk through the design of the internal control system, such as by adding additional levels of review for key operational processes, reviewing randomly selected transactions and their supporting documentation, taking periodic asset counts, or checking supervisor reconciliations.

Benefits and Costs of Internal Control

O4.06 Internal control provides many benefits to an entity. It provides management with added confidence regarding the achievement of objectives, provides feedback on how effectively an entity is operating, and helps reduce risks related to achieving the entity's objectives. Management considers a variety of cost factors in relation to expected benefits when designing and implementing internal controls. The complexity of cost-benefit determination is compounded by the interrelationship of controls with operational processes. Where controls are integrated with operational processes, it is difficult to isolate either their costs or benefits.

O4.07 Management may decide how an entity evaluates the costs versus benefits of various approaches to implementing an effective internal control system. However, cost alone is not an acceptable reason to avoid implementing internal controls. Management is responsible for meeting internal control objectives. The cost versus benefits considerations support management's ability to design, implement, and operate effectively an internal control system that balances the allocation of human resources in relation to the areas of greatest risk, complexity, or other factors relevant to achieving the entity's objectives.

Documentation

O4.08 The Green Book has specified documentation requirements in five attributes in the framework, with discussion of these requirements in the accompanying application material. These are:

- Principle 3: Paragraph 3.12
- Principle 12: Paragraph 12.03

[5] See paras. 10.15 through 10.18 for further discussion of segregation of duties.

- Principle 16: Paragraph 16.12
- Principle 17: Paragraph 17.07
- Principle 17: Paragraph 17.09

O4.09 These attributes represent the minimum level of required documentation in an entity's internal control system. Management exercises judgment in determining what additional documentation may be required beyond these attributes for an effective internal control system.

Applicability to Other Entities

O4.10 The Green Book may be applied as a framework for an internal control system for state, local, and quasi-governmental entities, as well as not-for-profit organizations. Management of these entities determines, based on applicable laws and regulations, the applicable requirements for their entities. If management elects to use the Green Book as criteria, management follows all applicable requirements presented in these standards.

Control Environment

Overview

The control environment is the foundation for an internal control system. It provides the discipline and structure, which affect the overall quality of internal control. It influences how objectives are defined and how control activities are structured. The oversight body and management establish and maintain an environment throughout the organization that sets a positive attitude toward internal control.

Principles

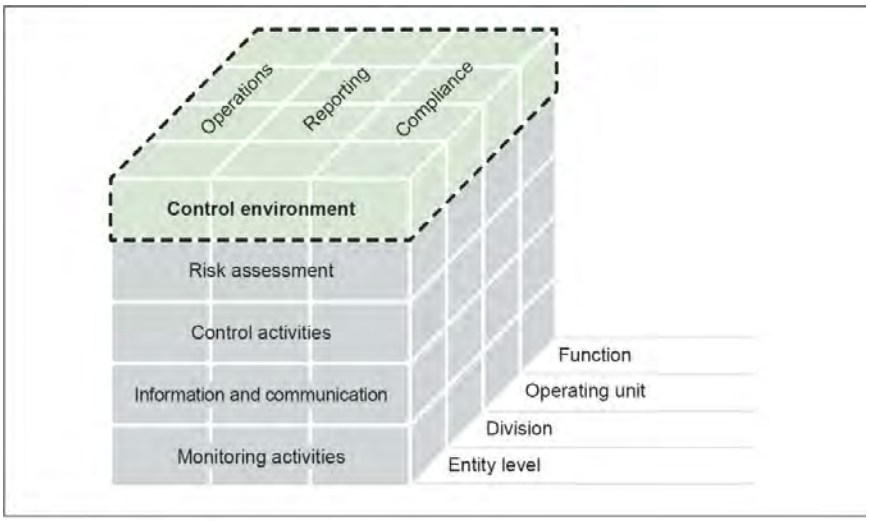
1. The oversight body and management should demonstrate a commitment to integrity and ethical values.

2. The oversight body should oversee the entity's internal control system.

3. Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.

4. Management should demonstrate a commitment to attract, develop, and retain competent individuals.

5. Management should evaluate performance and hold individuals accountable for their internal control responsibilities.



Source: COSO.

Principle 1 - Demonstrate Commitment to Integrity and Ethical Values

1.01 The oversight body and management should demonstrate a commitment to integrity and ethical values.

Attributes

1.02 The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

a. Set the Tone at the Top - The oversight body and management should demonstrate the importance of integrity and ethical values through their directives, attitudes, and behavior.

b. Establish Standards of Conduct - Management should define expectations concerning integrity and ethical values in the entity's standards of conduct.

c. Evaluate Adherence to Standards of Conduct - Management should establish processes to evaluate performance against the organization's expected standards of conduct and address any deviations in a timely manner.

Set Tone at the Top

1.03 The oversight body and management should demonstrate the importance of integrity and ethical values through their directives, attitudes, and behavior.

1.04 The oversight body and management lead by an example that demonstrates the organization's values, philosophy, and operating style. The oversight body and management set the tone at the top and throughout the organization by their example, which is fundamental to an effective internal control system. In larger organizations, the various layers of management in the organizational structure can also set "tone in the middle."

1.05 The oversight body and management's directives, attitudes, and behaviors reflect the integrity and ethical values expected throughout the organization. The oversight body and management reinforce the commitment to doing what is right, not just maintaining a minimum level of performance necessary to comply with applicable laws and

regulations, so that these priorities are understood by all stakeholders, such as regulators, employees, and the general public.

1.06 Tone at the top can be either a driver, as shown in the preceding paragraphs, or a barrier to internal control. Without a strong tone at the top to support an internal control system, the organization's risk identification may be incomplete, risk responses may be inappropriate, control activities may not be appropriately designed or implemented, information and communication may falter, and results of monitoring may not be understood or acted upon to remediate deficiencies.

Establish Standards of Conduct

1.07 Management should define expectations concerning integrity and ethical values in the entity's standards of conduct.

1.08 Management establishes standards of conduct to communicate expectations concerning integrity and ethical values. The organization uses ethical values to balance the needs and concerns of different stakeholders, such as regulators, employees, and the general public. The standards of conduct guide the directives, attitudes, and behaviors of the organization in achieving the entity's objectives.

1.09 Management, with oversight from the oversight body, defines the organization's expectations of ethical values in the standards of conduct. Management may consider using policies, operating principles, or guidelines to communicate the standards of conduct to the organization.

Evaluate Adherence to Standards of Conduct

1.10 Management should establish processes to evaluate performance against the organization's expected standards of conduct and address any deviations in a timely manner.

1.11 Management uses established standards of conduct as the basis for evaluating adherence to integrity and ethical values across the organization. Management evaluates the adherence to standards of conduct across all levels of the organization. To gain assurance that the entity's standards of conduct are implemented effectively, management

evaluates the directives, attitudes, and behaviors of individuals and teams. Evaluations may consist of ongoing monitoring or separate evaluations.[6] Individual personnel can also report issues through reporting lines, such as regular staff meetings, upward feedback processes, a whistle-blowing program, or an ethics hotline.[7] The oversight body evaluates management's adherence to the standards of conduct as well as the overall adherence by the organization.

1.12 Management determines the tolerance level for deviations. Management may determine that the entity will have zero tolerance for deviations from certain expected standards of conduct, while deviations from others may be addressed with warnings to personnel. Management establishes a process for evaluations of individual and team adherence to standards of conduct that escalates and remediates deviations. Management addresses deviations from expected standards of conduct in a timely and consistent manner. Depending on the severity of the deviation determined through the evaluation process, management, with oversight from the oversight body, takes appropriate actions and may also need to consider applicable laws and regulations. The standards of conduct to which management holds personnel, however, remain consistent.

Principle 2 - Exercise Oversight Responsibility

2.01 The oversight body should oversee the entity's internal control system.

Attributes

2.02 The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

a. Establish Oversight Structure - The entity should determine an appropriate oversight structure based on applicable laws and regulations, relevant government guidance, and feedback from key stakeholders.

[6] See paras. 16.06 through 16.11 for further discussion of ongoing monitoring and separate evaluations.

[7] See paras. 16.12 through 16.14 for further discussion of internal control issues.

b. Provide Oversight for the Internal Control System - The oversight body should oversee management's design, implementation, and operation of the internal control system.

c. Provide Input for Remediation of Deficiencies - The oversight body should provide input to management's plans for remediation of deficiencies in the internal control system as appropriate.

Establish Oversight Structure

2.03 The entity should determine an appropriate oversight structure based on applicable laws and regulations, relevant government guidance, and feedback from key stakeholders.

2.04 The entity determines an oversight structure to fulfill responsibilities set forth by applicable laws and regulations, relevant government guidance, and feedback from key stakeholders. The entity will select, or if mandated by law will have selected for it, an oversight body. When the oversight body is composed of entity management, activities referenced in the Green Book as performed by "management" exclude such management when in their role as the oversight body.

Responsibilities of an Oversight Body

2.05 When the oversight structure of an entity is led by senior management, senior management may distinguish itself from divisional or functional management through the establishment of an oversight body. An oversight body oversees the entity's operations, provides constructive criticism to management, and where appropriate, makes oversight decisions to ensure that the entity achieves its objectives in alignment with the entity's integrity and ethical values.

Qualifications for an Oversight Body

2.06 In selecting members for an oversight body, the entity or applicable body defines the entity knowledge, relevant expertise, number of members, and possible independence needed to fulfill the oversight responsibilities for the entity.

2.07 Members of an oversight body understand the entity's objectives, related risks, and expectations of its stakeholders. In addition to an oversight body, an organization within the federal government may have several bodies that are key stakeholders for the entity, such as the White House, Congress, OMB, and the Department of the Treasury. An oversight body works with key stakeholders to understand their expectations and help the entity fulfill these expectations if appropriate.

2.08 The entity or applicable body also considers the expertise needed by members to oversee, question, and evaluate management. Capabilities expected of all members of an oversight body include integrity and ethical values, leadership, critical thinking, and problem-solving.

2.09 Further, in determining the number of members of an oversight body, the entity or applicable body considers the need for more specialized skills to enable discussion, offer constructive criticism to management, and make appropriate oversight decisions. Some specialized skills may include:

- Internal control mindset (e.g., professional skepticism, perspectives on approaches for identifying and responding to risks, and assessing the effectiveness of the system of internal control)
- Programmatic expertise, including knowledge of the entity's mission, programs, and operational processes
- Financial expertise, including financial reporting (e.g., accounting standards, financial reporting requirements)
- Relevant systems and technology (e.g., understanding critical systems and technology risks and opportunities)

2.10 If authorized by applicable laws and regulations, the entity may also consider including independent members as part of an oversight body.[8] Members of an oversight body scrutinize and question management's activities, present alternative views, and act when faced with obvious or suspected wrongdoing. Independent members with relevant expertise provide value through their impartial evaluation of the entity and its operations in achieving objectives.

[8] See GAO, *Government Auditing Standards: 2011 Revision,* GAO-12-331G (Washington, D.C.: December 2011), paras. 3.02 through 3.59 for further discussion of independence.

Provide Oversight for the System of Internal Control

2.11 The oversight body should oversee management's design, implementation, and operation of the internal control system.

2.12 The oversight body oversees management's design, implementation, and operation of the entity's internal control system. The oversight body's responsibilities for the entity's internal control system include:

- Control Environment - Establish integrity and ethical values, establish oversight structure, develop expectations of competence, and maintain accountability to all members of the oversight body and key stakeholders.
- Risk Assessment - Oversee management's assessment of risks to the achievement of objectives, including the potential impact of significant changes, fraud, and management override of internal control.
- Control Activities - Provide oversight to management in the development and performance of control activities.
- Information and Communication - Analyze and discuss information relating to the entity's achievement of objectives.
- Monitoring - Scrutinize the nature and scope of management's monitoring activities as well as management's evaluation and remediation of identified deficiencies.

2.13 These responsibilities are supported by the organizational structure that management establishes.[9] The oversight body oversees management's design, implementation, and operation of the entity's organizational structure to ensure that the necessary processes to enable the oversight body to fulfill its responsibilities exist and are operating effectively.

Provide Input for Remediation of Deficiencies

2.14 The oversight body should provide input to management's plans for remediation of deficiencies in the internal control system as appropriate.

[9] See paras. 3.03 through 3.07 for further discussion of organizational structure.

2.15 Management reports deficiencies identified in the internal control system to the oversight body. The oversight body oversees and provides direction to management on the remediation of these deficiencies. The oversight body also provides direction when a deficiency crosses organizational boundaries or units, or when the interests of management may conflict with remediation efforts. When appropriate and authorized, the oversight body may direct the creation of teams to address or oversee specific matters critical to achieving the entity's objectives.

2.16 The oversight body is responsible for overseeing the remediation of deficiencies as appropriate and for providing direction to management on appropriate time frames for correcting these deficiencies.[10]

Principle 3 - Establish Structure, Responsibility, and Authority

3.01 Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.

Attributes

3.02 The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

a. Establish Organizational Structure - Management should establish an organizational structure.

b. Assign Responsibility and Delegate Authority - Management should assign responsibility and delegate authority to key roles throughout the organization.

c. Document Internal Control System - Management should develop and maintain documentation of its internal control system.

Establish Organizational Structure

3.03 Management should establish an organizational structure.

[10] See paras. 17.09 through 17.10 for further discussion of timely remediation of findings.

3.04 Management establishes an organizational structure necessary to enable the entity to plan, execute, control, and assess the organization in achieving its objectives. Management develops the overall responsibilities from the entity's objectives that enable the entity to achieve its objectives and address related risks.

3.05 Management develops an organizational structure with an understanding of the overall responsibilities, and assigns these responsibilities to discrete units to enable the organization to operate in an efficient and effective manner, comply with applicable laws and regulations, and reliably report quality information.[11] Based on the nature of the assigned responsibility, management chooses the type and number of discrete units, such as divisions, offices, or their related subunits.

3.06 As part of establishing an organizational structure, management considers how units interact in order to fulfill their overall responsibilities. Management establishes reporting lines within an organizational structure so that units can communicate the necessary quality information for each unit to fulfill its overall responsibilities.[12] Reporting lines are defined at all levels of the organization and provide methods of communication that can flow down, across, up, and around the structure.[13] Management also considers the entity's overall responsibilities to external sources and establishes reporting lines that allow the entity to both communicate and receive information from external sources.[14]

3.07 Management periodically evaluates the organizational structure to ensure that it meets the entity's objectives and has adapted to any new objectives for the entity, such as a new regulation.

Assign Responsibility and Delegate Authority

3.08 Management should assign responsibility and delegate authority to key roles throughout the organization.

[11] See paras. 13.08 through 13.10 for further discussion of quality information.

[12] See paras. 13.03 through 13.10 for further discussion of quality information.

[13] See paras. 14.03 through 14.08 for further discussion of internal reporting lines.

[14] See paras. 15.03 through 15.08 for further discussion of external reporting lines.

3.09 To achieve the entity's objectives, management assigns responsibility and delegates authority to key roles throughout the organization. A key role is a position in the organizational structure that is assigned an overall responsibility of the entity. Generally, key roles relate to senior management positions within an organization.

3.10 Management considers the overall responsibilities assigned to each unit, determines what key roles are needed to fulfill the assigned responsibilities, and establishes the key roles. Those in key roles can further assign responsibility for internal control to roles below them in the organizational structure, but retain ownership for fulfilling the overall responsibilities assigned to the unit.

3.11 Management determines what level of authority the key role needs to fulfill that responsibility. Management delegates authority only to the extent required to achieve the entity's objectives. As part of delegating authority, management evaluates the delegation to ensure proper segregation of duties within the unit and in the organizational structure. Segregation of duties helps prevent fraud, waste, and abuse in the entity by considering the need to separate authority, custody, and accounting in the organizational structure.[15] As with assigning responsibility, those in key roles can delegate their authority for internal control to roles below them in the organizational structure.

Document Internal Control System

3.12 Management should develop and maintain documentation of its internal control system.

3.13 Management develops and maintains documentation of its internal control system for a number of reasons. Effective documentation assists in management's design of internal control by establishing and communicating the who, what, when, where, and why of internal control execution to personnel. Documentation also provides a means to retain organizational knowledge and mitigate the risk of having that knowledge limited to a few personnel, as well as a means to communicate that knowledge as needed to external parties such as external auditors.

[15] See paras. 10.15 through 10.18 for further discussion of segregation of duties.

3.14 Management documents internal control to meet operational needs. Documentation of controls, including changes to controls, is evidence that controls are identified, capable of being communicated to those responsible for their performance, and capable of being monitored and evaluated by the entity. The extent of documentation supporting the design, implementation, and operating effectiveness of the five components of internal control is a matter of judgment for management. Management considers the cost-benefit of documentation requirements for the entity as well as the size, nature, and complexity of the entity and its objectives. Some level of documentation, however, is necessary to ensure that the components of internal control are designed, implemented, and operating effectively.

Principle 4 - Demonstrate Commitment to Competence

4.01 Management should demonstrate a commitment to attract, develop, and retain competent individuals.

Attributes

4.02 The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

a. Establish Expectations of Competence - Management should establish expectations of competence throughout the organization.

b. Attract, Develop, and Retain Individuals - Management should attract, develop, and retain competent personnel.

c. Plan and Prepare for Succession - Management should define succession and contingency plans for key roles in the organization.

Establish Expectations of Competence

4.03 Management should establish expectations of competence throughout the organization.

4.04 Management establishes expectations of competence for key roles, and other roles at management's discretion, to help the entity achieve its objectives. Competence is the qualification to carry out assigned responsibilities. It requires relevant knowledge, skills, and abilities, which are gained largely from professional experience, training, and

certifications. It is expressed in the attitude and behavior of individuals as they carry out their responsibilities.

4.05 Management considers standards of conduct, assigned responsibility, and delegated authority when establishing expectations. Management establishes expectations of competence for key roles. Management may also establish expectations of competence for all personnel through policies within the organization's internal control system.[16]

4.06 Personnel need to possess and maintain a level of competence that allows them to accomplish their assigned responsibilities, as well as understand the importance of effective internal control. Holding individuals accountable to established policies by evaluating personnel's competence is integral to attracting, developing, and retaining individuals. Management evaluates competence of personnel across the organization in relation to established policies. Management acts as necessary to address any deviations from the established policies. The oversight body evaluates the competence of management as well as the overall competence of the organization.

Attract, Develop, and Retain Individuals

4.07 Management should attract, develop, and retain competent personnel.

4.08 Management attracts, develops, and retains competent personnel to achieve the entity's objectives. Management may consider:

- Attract - Conduct procedures to determine whether a particular candidate fits the organizational needs and has the competence for the proposed role.
- Train - Enable individuals to develop competencies appropriate for key roles, reinforce standards of conduct, and tailor training based on the needs of the role.
- Mentor - Provide guidance on the individual's performance based on standards of conduct and expectations of competence, align the individual's skills and expertise with the entity's objectives, and help personnel adapt to an evolving environment.

[16] See paras. 12.03 through 12.05 for further discussion of policies.

- Retain – Provide incentives to motivate and reinforce expected levels of performance and desired conduct, including training and credentialing as appropriate.

Plan and Prepare for Succession

4.09 Management should define succession and contingency plans for key roles in the organization.

4.10 Management defines succession and contingency plans for key roles to help the organization continue achieving its objectives. Succession plans address the entity's need to replace competent personnel over the long term, whereas contingency plans address the organization's need to respond to sudden personnel changes impacting the organization that could compromise the internal control system.

4.11 Management defines succession plans for key roles, chooses succession candidates, and trains succession candidates to assume the key roles. If management relies on a service organization to fulfill the assigned responsibilities of key roles in the entity, management assesses whether the service organization can continue in these key roles, identifies other candidate organizations for the roles, and ensures that processes are in place to enable knowledge sharing with the succession candidate organization.

4.12 Management defines contingency plans for assigning responsibilities if a key role in the organization is vacated without advance notice. The importance of the key role in the internal control system and the impact to the organization of its vacancy dictates the formality and depth of the contingency plan.

Principle 5 - Enforce Accountability

5.01 Management should evaluate performance and hold individuals accountable for their internal control responsibilities.

Attributes

5.02 The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

a. Enforce Accountability - Management should enforce accountability for performance of internal control responsibilities.

b. Consider Excessive Pressures - Management should evaluate and adjust pressures on personnel related to achieving objectives as they assign responsibilities and evaluate performance.

Enforce Accountability

5.03 Management should enforce accountability for performance of internal control responsibilities.

5.04 Management enforces accountability of individuals performing their internal control responsibilities. Accountability is driven by the tone at the top and supported by the commitment to integrity and ethical values, organizational structure, and expectations of competence, which influence the control culture of the organization. Accountability for performance of internal control responsibility supports day-to-day decision making, attitudes, and behaviors. Management holds personnel accountable through mechanisms such as performance appraisals and disciplinary actions.

5.05 Management holds entity personnel accountable for performing their assigned internal control responsibilities. The oversight body, in turn, holds management accountable as well as the organization as a whole for its internal control responsibilities.

5.06 If management establishes incentives, management recognizes that actions can yield unintended consequences and evaluates incentives to ensure that they align with the entity's standards of conduct.

5.07 Management holds service organizations accountable for their assigned internal control responsibilities. Management may contract service organizations to perform roles in the organizational structure. Management communicates to the service organization the objectives of the entity and their related risks, the entity's standards of conduct, the role of the service organization in the organizational structure, the assigned

responsibilities and authorities of the role, and the expectations of competence for its role that will enable the service organization to perform its internal control responsibilities.

5.08 Management, with oversight from the oversight body, takes corrective action as necessary to enforce accountability for internal control in the organization. These actions can range from informal feedback provided by the direct supervisor to disciplinary action taken by the oversight body depending on the significance of the deficiency to the internal control system.[17]

Consider Excessive Pressures

5.09 Management should evaluate and adjust pressures on personnel related to achieving objectives as they assign responsibilities and evaluate performance.

5.10 Management adjusts excessive pressures on personnel in the organization. Pressure can appear in an organization due to goals established by management to meet objectives or cyclical demands of various processes performed by the organization, such as year-end financial statement preparation. Excessive pressure can result in personnel "cutting corners" to meet the established goals.

5.11 Management is responsible for evaluating pressure on personnel to help personnel fulfill their assigned responsibilities in accordance with the entity's standards of conduct. Management can adjust excessive pressures using many different tools, such as rebalancing workloads or increasing resource levels.

[17] See Overview: Effect on the Internal Control System for further discussion of significance of deficiencies.

Risk Assessment

Overview

Having established an effective control environment, management assesses the risks facing the entity as it seeks to achieve its objectives. This assessment provides the basis for developing appropriate risk responses. Management assesses the risks the entity faces from both external and internal sources.

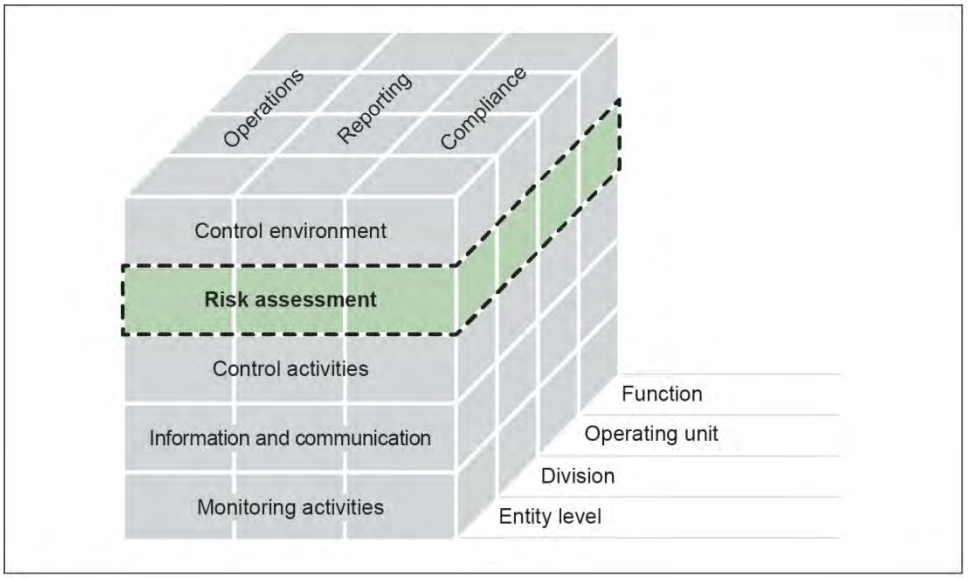
Principles

6. Management should define objectives and risk tolerances.

7. Management should identify, analyze, and respond to risks related to achieving the defined objectives.

8. Management should consider the potential for fraud when identifying, analyzing, and responding to risks.

9. Management should identify, analyze, and respond to significant changes in the internal control system.



Source: COSO.

Principle 6 - Define Objectives and Risk Tolerances

6.01 Management should define objectives and risk tolerances.

Attributes

6.02 The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

a. Define Objectives - Management should define objectives in specific and measurable terms to enable the design of internal control for related risks.

b. Define Risk Tolerances - Management should define the risk tolerances for the defined objectives.

Define Objectives

6.03 Management should define objectives in specific and measurable terms to enable the design of internal control for related risks.

6.04 Management defines objectives in specific and measurable terms to enable the design of internal control for related risks. Specific terms are fully and clearly set forth so they can be easily understood. Measurable terms allow for the assessment of performance toward achieving objectives. Objectives are initially set as part of the objective-setting process and then refined as they are incorporated into the internal control system when management uses them to establish the control environment.

6.05 Management defines objectives in specific terms so they are understood at all levels of the entity. This involves clearly defining what is to be achieved, who is to achieve it, how it will be achieved, and the time frames for achievement. All objectives can be broadly classified into one or more of three categories: operations, reporting, or compliance. Reporting objectives are further categorized as being either internal or external, and financial or nonfinancial. Management ensures that the defined objectives align with the organization’s mission, strategic plan and performance goals.

6.06 Management defines objectives in measurable terms so that performance toward achieving those objectives can be assessed. Measurable objectives are generally free of bias and do not require subjective judgments to dominate their measurement. Measurable objectives are also stated in a quantitative or qualitative form that permits reasonably consistent measurement.

6.07 Management considers external requirements and internal expectations when defining objectives to enable the design of internal control. Legislators, regulators, and standard-setting bodies set external requirements by establishing the laws, regulations, and standards with which the organization is required to comply. Management identifies, understands, and incorporates these requirements into the entity's objectives. Management sets internal expectations and requirements through the established standards of conduct,[18] oversight structure,[19] organizational structure,[20] and expectations of competence[21] as part of the control environment.

6.08 Management evaluates and, if necessary, revises defined objectives to ensure that they are consistent with these requirements and expectations. This consistency enables management to identify and analyze risks associated with achieving the defined objectives.

6.09 Management determines whether performance measures for the defined objectives are appropriate for evaluating the entity's performance in achieving those objectives. For quantitative objectives, performance measures may be a targeted percentage or numerical value. For qualitative objectives, management may need to design performance measures that indicate a level or degree of performance, such as milestones.

Define Risk Tolerances

6.10 Management should define the risk tolerances for the defined objectives.

[18] See paras. 1.07 through 1.09 for further discussion of standards of conduct.

[19] See paras. 2.03 through 2.10 for further discussion of oversight structure.

[20] See paras. 3.03 through 3.07 for further discussion of organizational structure.

[21] See paras. 4.03 through 4.06 for further discussion of expectations of competence.

6.11 Management defines risk tolerances for the defined objectives. Risk tolerance is the acceptable level of variation in performance relative to the achievement of objectives. Risk tolerances are initially set as part of the objective-setting process. Management defines the risk tolerances for defined objectives by ensuring that the set levels of variation for performance measures are appropriate for the design of an internal control system.

6.12 Management defines risk tolerances in specific and measurable terms so they are clearly stated and can be measured. Risk tolerance is often measured in the same unit as the performance measures for the defined objectives. Depending on the category of objectives, risk tolerances may be expressed as follows:

- Operations and Compliance Objectives - Acceptable level of variation in performance in relation to risk.
- Nonfinancial Reporting Objectives - Required level of precision and accuracy suitable for user needs.
- Financial Reporting Objectives - Material misstatements, including omissions, are those that, either individually or in the aggregate, could reasonably be expected to influence the decisions of financial statement users. Judgments about materiality are made in light of surrounding circumstances, involve both qualitative and quantitative considerations, and are affected by the needs of financial statement users and size or nature of a misstatement.

6.13 Management also evaluates whether risk tolerances enable the appropriate design of internal control by considering whether they are consistent with requirements and expectations for the defined objectives. As in defining objectives, management considers the risk tolerances in the context of the entity's applicable laws, regulations, and standards as well as the entity's standards of conduct, oversight structure, organizational structure, and expectations of competence. If risk tolerances for defined objectives are not consistent with these requirements and expectations, management revises the risk tolerances to achieve consistency.

Principle 7 – Identify, Analyze, and Respond to Risk

7.01 Management should identify, analyze, and respond to risks related to achieving the defined objectives.

Attributes

7.02 The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

a. Identify Risks - Management should identify risks throughout the entity.

b. Analyze Risks - Management should analyze the identified risks to estimate their significance.

c. Respond to Risks - Management should design responses to the analyzed risks.

Identify Risks

7.03 Management should identify risks throughout the entity.

7.04 Management identifies risks throughout the entity to provide a basis for analyzing risks. Risk assessment is the identification and analysis of risks related to achieving the defined objectives to form a basis for designing risk responses.

7.05 To identify risks, management considers the types of risks that impact the entity. This includes both inherent and residual risk. Inherent risk is the risk to an entity in the absence of management's response to the risk. Residual risk is the risk that remains after management's response to inherent risk. Both risks could cause deficiencies in the internal control system.

7.06 Management considers all significant interactions within the entity and with external parties, changes within the entity's internal and external environment,[22] and other internal and external factors to identify risks throughout the entity. Internal risk factors may include the complex nature of an entity's programs, its organizational structure, or the use of new technology in operational processes. External risk factors may include new or amended laws, regulations, or professional standards; economic instability; or potential natural disasters. Management considers these factors at both the entity and transaction level to comprehensively identify risks that affect defined objectives.[23] Risk identification methods may

[22] See paras. 9.03 through 9.05 for further discussion of changes in the internal control system.

[23] See paras. 10.10 through 10.14 for further discussion of level of controls.

include qualitative and quantitative ranking activities, management conferences, forecasting and strategic planning, and consideration of deficiencies identified through audits and other assessments.

Analyze Risks

7.07 Management should analyze the identified risks to estimate their significance.

7.08 Management analyzes the identified risks to estimate their significance, which provides a basis for responding to the risks. Significance refers to the effect on achieving a defined objective.

7.09 Management estimates the significance of the identified risks to assess their effect on achieving the defined objectives at both the entity and transaction level. Management estimates the significance of a risk by considering the magnitude of impact, likelihood of occurrence, and nature of the risk. Magnitude of impact refers to the likely magnitude of deficiency that could result from the risk and is affected by factors such as the size, pace, and duration of the risk's impact. Likelihood of occurrence refers to the possibility that a risk will occur. The nature of the risk involves factors such as the degree of subjectivity involved with the risk and whether the risk arises from fraud or from complex or unusual transactions. The oversight body may oversee management's estimates of significance to ensure that risk tolerances have been properly defined.

7.10 Risks may either be analyzed on an individual basis or grouped into categories with related risks and analyzed collectively. Regardless of whether risks are analyzed individually or collectively, management considers the correlation among different risks or groups of risks when estimating their significance. The specific risk analysis methodology used can vary by entity because of differences in entities' missions and the difficulty in qualitatively and quantitatively defining risk tolerances.

Respond to Risks

7.11 Management should design responses to the analyzed risks.

7.12 Management designs responses to the analyzed risks so that risks are within the defined risk tolerance for the defined objective. Management designs overall risk responses for the analyzed risks based on the significance of the risk and defined risk tolerance. These risk responses may include:

- Acceptance - No action is taken to respond to the risk.
- Avoidance - Action is taken to stop the operational process or the part of the operational process causing the risk.
- Reduction - Action is taken to reduce the likelihood or magnitude of the risk.
- Sharing - Action is taken to transfer or share risks across the entity or with external parties, such as insuring against losses.

7.13 Based on the selected risk response, management designs the specific actions to respond to the analyzed risks. The nature and extent of risk response actions depend on the defined risk tolerance. Operating within the defined risk tolerance provides greater assurance that the entity will achieve its objectives. Performance measures are used to assess whether risk response actions enable the entity to operate within the defined risk tolerances. When risk response actions do not enable the entity to operate within the defined risk tolerances, management may need to revise risk responses or reconsider defined risk tolerances.

Principle 8 - Assess Fraud Risk

8.01 Management should consider the potential for fraud when identifying, analyzing, and responding to risks.[24]

Attributes

8.02 The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

a. Consider Types of Fraud - Management should consider the types of fraud that can occur within the organization.

[24] Fraud involves obtaining something of value through willful misrepresentation. Whether an act is in fact fraud is a determination to be made through the judicial or other adjudicative system and is beyond management's professional responsibility for assessing risk.

b. Consider Fraud Risk Factors - Management should consider fraud risk factors.

c. Respond to Fraud Risks - Management should analyze and respond to identified fraud risks.

Consider Types of Fraud

8.03 Management should consider the types of fraud that can occur within the organization.

8.04 Management considers the types of fraud that can occur within the organization to provide a basis for identifying fraud risks. Fraud can occur in:

- Fraudulent Financial Reporting - Intentional misstatements or omissions of amounts or disclosures in financial statements to deceive financial statement users. This could include intentional alteration of accounting records, misrepresentation of transactions, intentional misapplication of accounting principles, or other means.
- Misappropriation of Assets - Theft of an entity's assets. This could include theft of property, embezzlement of receipts, fraudulent payments, or other means.
- Corruption - Bribery and other illegal acts.

8.05 In addition to fraud, management considers other forms of misconduct that can occur, such as waste and abuse. Waste is the act of using or expending resources carelessly, extravagantly, or to no purpose. Abuse involves behavior that is deficient or improper when compared with behavior that a prudent person would consider reasonable and necessary operational practice given the facts and circumstances. This includes the misuse of authority or position for personal gain or for the benefit of another. Waste and abuse do not necessarily involve fraud or illegal acts. However, they may be an indication of potential fraud or illegal acts and may still impact the achievement of defined objectives.

Consider Fraud Risk Factors

8.06 Management should consider fraud risk factors.

8.07 Management considers fraud risk factors. Fraud risk factors do not necessarily indicate that fraud exists but are often present when fraud occurs. Fraud risk factors include:

- Incentive/pressure - Management or other personnel have an incentive or are under pressure, which provides a motive to commit fraud.[25]
- Opportunity - Circumstances exist, such as the absence of controls, ineffective controls, or the ability of management to override controls, that provide an opportunity to commit fraud.
- Attitude/rationalization - Individuals involved are able to rationalize committing fraud. Some individuals possess an attitude, character, or ethical values that allow them to knowingly and intentionally commit a dishonest act.

8.08 Management uses the fraud risk factors to identify fraud risks. While fraud risk may be greatest when all three risk factors are present, one or more of these factors may indicate a fraud risk. Other information provided by internal and external parties can also be used to identify fraud risks. This may include allegations of fraud or suspected fraud reported by the OIG or internal auditors, personnel, or external parties that interact with the organization.

Respond to Fraud Risks

8.09 Management should analyze and respond to identified fraud risks.

8.10 Management analyzes and responds to identified fraud risks to ensure that they are effectively mitigated. Fraud risks are analyzed through the same risk analysis process performed for all identified risks.[26] Management analyzes the identified fraud risks by estimating their significance, both individually and in the aggregate, to assess their effect on achieving the defined objectives. As part of analyzing fraud risk, management also assesses the risk of management override of controls.[27] The oversight body oversees management's assessments of fraud risk and the risk of management override of controls to ensure that they are appropriate.

[25] See paras. 5.09 through 5.11 for further discussion of pressure.

[26] See paras. 7.07 through 7.10 for further discussion of analyzing risks.

[27] See para. 10.17 for further discussion of management override.

8.11 Management responds to fraud risks through the same risk response process performed for all analyzed risks.[28] Management designs an overall risk response and specific actions for responding to fraud risks. It may be possible to reduce or eliminate certain fraud risks by making changes to the entity's activities and processes. These changes may include stopping or reorganizing certain operations and reallocating roles among personnel to enhance segregation of duties. In addition to responding to fraud risks, management may need to develop further responses to address the risk of management override of controls. Further, when fraud has been detected, it may be necessary to revise the risk assessment process going forward.

Principle 9 – Identify, Analyze, and Respond to Change

9.01 Management should identify, analyze, and respond to significant changes in the internal control system.

Attributes

9.02 The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

a. Identify Change - Management should identify changes that could significantly impact the entity's internal control system.

b. Analyze and Respond to Change - Management should analyze and respond to identified changes that impact the entity's internal control system.

Identify Change

9.03 Management should identify changes that could significantly impact the entity's internal control system.

9.04 As part of risk assessment or a similar process, management identifies changes that could significantly impact the entity's internal control system. Identifying, analyzing, and responding to change is

[28] See paras. 7.11 through 7.13 for further discussion of responding to risks.

similar to, if not part of, the entity's regular risk assessment process. However, change is discussed separately because it is critical to an effective internal control system and can often be overlooked or inadequately addressed in the normal course of operations.

9.05 Conditions affecting the entity and its environment continually change. Management can anticipate and plan for significant changes by using a forward-looking process for identifying change. Management identifies, on a timely basis, significant changes to internal and external conditions that have already occurred or are expected to occur. Changes in internal conditions include changes to the entity's programs or activities, oversight structure, organizational structure, personnel, and technology. Changes in external conditions include changes in the governmental, economic, technological, legal, regulatory, and physical environments. Identified significant changes are communicated across the organization through established reporting lines to appropriate personnel.[29]

Analyze and Respond to Change

9.06 Management should analyze and respond to identified changes that impact the entity's internal control system.

9.07 As part of risk assessment or a similar process, management analyzes and responds to identified changes and related risks to ensure the effectiveness of the internal control system. Changes in conditions affecting the entity and its environment often require changes to the entity's internal control system, as existing controls may not be effective for meeting objectives or addressing risks under changed conditions. Management analyzes the effect of identified changes on the internal control system and responds by revising the internal control system on a timely basis, when necessary, to ensure its effectiveness.

9.08 Further, changing conditions often prompt new risks or changes to existing risks that need to be assessed. As part of analyzing and responding to change, management performs a risk assessment to identify, analyze, and respond to any new risks prompted by the changes. Additionally, existing risks may require further assessment to determine whether the defined risk tolerances and risk responses need to be revised.

[29] See paras. 14.03 through 14.08 for further discussion of internal reporting lines.

Control Activities

Overview

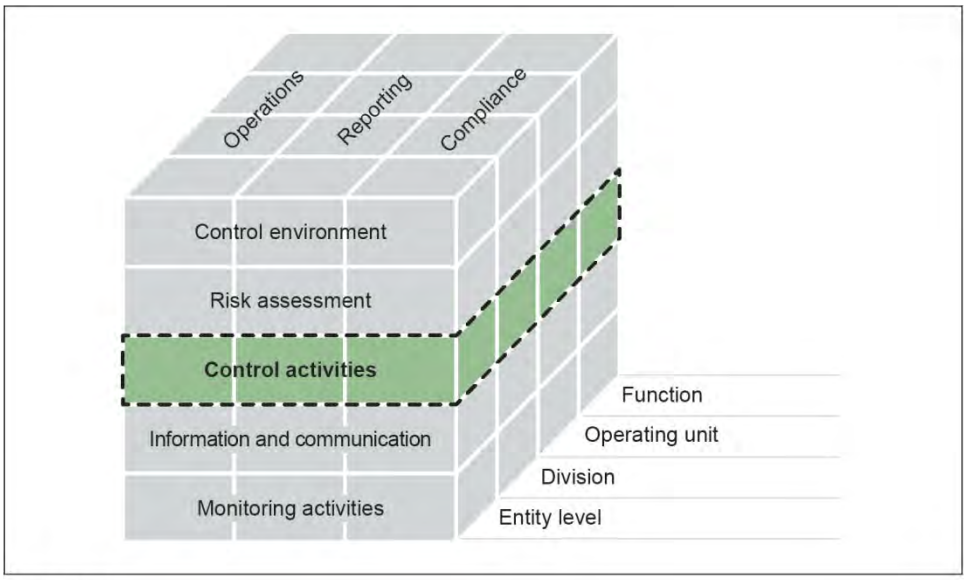
Control activities are the actions management establishes through policies and procedures to achieve objectives and respond to risks in the internal control system, which includes the entity's information system.

Principles

10. Management should design control activities to achieve objectives and risk responses.

11. Management should design control activities for the entity's information system.

12. Management should implement control activities.



Source: COSO.

Principle 10 - Design Control Activities

10.01 Management should design control activities to achieve objectives and risk responses.

Attributes

10.02 The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

a. Respond to Objectives and Risks - Management should design control activities that respond to the entity's objectives and risks.

b. Design the Types of Control Activities - Management should design appropriate types of control activities needed for the entity's internal control system.

c. Design Control Activities at Various Levels - Management should design control activities at appropriate levels in the organizational structure.

d. Consider Segregation of Duties - Management should consider segregation of duties in designing the assignment of control activity responsibilities.

Respond to Objectives and Risks

10.03 Management should design control activities that respond to the entity's objectives and risks.

10.04 Management designs control activities in response to the entity's objectives and risks to achieve an effective internal control system. Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives to achieve the entity's objectives and address related risks. As part of the control environment component, management defines responsibilities, assigns them to key roles, and delegates authority to achieve the entity's objectives. As part of the risk assessment component, management identifies the risks related to the entity and its objectives including its service organizations, the entity's risk tolerance, and risk responses. Management designs control activities to fulfill defined responsibilities and address identified risk responses.

Design Appropriate Types of Control Activities

10.05 Management should design appropriate types of control activities needed for the entity's internal control system.

10.06 Management designs appropriate types of control activities for the entity's internal control system. Control activities help management fulfill responsibilities and address identified risk responses in the internal control system.

Common Categories of Internal Control

Examples of common categories of control activities include the following:

- Top Level Reviews of Actual Performance
- Reviews by Management at the Functional or Activity Level
- Management of Human Capital
- Controls over Information Processing
- Physical control over vulnerable assets
- Establishment and Review of Performance Measures and Indicators
- Segregation of Duties
- Proper Execution of Transactions and Events
- Accurate and Timely Recording of Transactions and Events
- Access Restrictions to and Accountability for Resources and Records
- Appropriate Documentation of Transactions and Internal Control

Top Level Reviews of Actual Performance

Management tracks major entity achievements and compares these to the plans, goals, and objectives set by the entity.

Reviews by Management at the Functional or Activity Level

Management compares actual performance to planned or expected results throughout the organization and analyzes significant differences.

Management of Human Capital

Effective management of an organization's workforce, its human capital, is essential to achieving results and an important part of internal control. Only when the right personnel for the job are on board and are provided the right training, tools, structure, incentives, and responsibilities is operational success possible. Management ensures that the knowledge, skills, and ability needs are continually assessed and that the organization is able to obtain a workforce that has the required knowledge, skills, and

abilities necessary to achieve organizational goals. Training should be aimed at developing and retaining employee knowledge, skills, and abilities to meet changing organizational needs. Management provides qualified and continuous supervision to ensure that internal control objectives are achieved. Management designs performance evaluation and feedback, supplemented by an effective reward system, to help employees understand the connection between their performance and the entity's success. As a part of its human capital planning, management also considers how best to retain valuable employees, plan for their eventual succession, and ensure continuity of needed skills and abilities.

Controls over Information Processing

A variety of control activities are used in information processing. Examples include edit checks of data entered, accounting for transactions in numerical sequences, comparing file totals with control accounts, and controlling access to data, files, and programs. Further guidance on control activities for information processing is provided below under "Control Activities Specific for Information Systems" and in Principle 11.

Physical Control over Vulnerable Assets

Management establishes physical control to secure and safeguard vulnerable assets. Examples include security for and limited access to assets such as cash, securities, inventories, and equipment that might be vulnerable to risk of loss or unauthorized use. Management periodically counts and compares such assets to control records.

Establishment and Review of Performance Measures and Indicators

Management establishes activities to monitor performance measures and indicators. These may include comparisons and assessments relating different sets of data to one another so that analyses of the relationships can be made and appropriate actions taken. Management designs controls aimed at validating the propriety and integrity of both entity and individual performance measures and indicators.

Segregation of Duties

Management divides or segregates key duties and responsibilities among different people to reduce the risk of error, misuse, or fraud. This includes separating the responsibilities for authorizing transactions, processing and recording them, reviewing the transactions, and handling any related

assets. Management ensures that no one individual controls all key aspects of a transaction or event.

Proper Execution of Transactions and Events

Transactions and other significant events are authorized and executed only by persons acting within the scope of their authority. This is the principal means of assuring that only valid transactions to exchange, transfer, use, or commit resources and other events are initiated or entered into. Management clearly communicates authorizations to personnel.

Accurate and Timely Recording of Transactions and Events

Management ensures that transactions are promptly recorded to maintain their relevance and value to management in controlling operations and making decisions. This applies to the entire process or life cycle of a transaction or event from its initiation and authorization through its final classification in summary records. In addition, management designs control activities to help ensure that all transactions are completely and accurately recorded.

Access Restrictions to and Accountability for Resources and Records

Management limits access to resources and records to authorized individuals, and assigns and maintains accountability for their custody and use. Management may periodically compare resources with the recorded accountability to help reduce the risk of errors, fraud, misuse, or unauthorized alteration.

Appropriate Documentation of Transactions and Internal Control

Management clearly documents internal control and all transactions and other significant events, and ensures that the documentation is readily available for examination. The documentation may appear in management directives, administrative policies, or operating manuals, in either paper or electronic form. Documentation and records are properly managed and maintained.

10.07 Control activities can be either preventive or detective. The main difference between preventive and detective control activities is when the control activity occurs in an entity's operations. A preventive control

activity prevents an entity from failing to achieve an objective or addressing a risk. A detective control activity discovers when an entity is not achieving an objective or addressing a risk before the entity's operation has concluded and corrects the actions so that the entity achieves the objective or addresses the risk.

10.08 Management evaluates the purpose of the control activity as well as the effect a deficiency would have on the entity in achieving its objectives. If the control activity is for a significant purpose or the impact of a deficiency would be significant to achieving the entity's objectives, management may design both preventive and detective control activities.

10.09 Control activities can be implemented in either an automated or a manual manner. Automated control activities are either wholly or partially automated through the entity's information technology. Manual control activities are performed by individuals with minor use of the entity's information technology. Automated control activities tend to be more reliable because they are less susceptible to human error and are typically more efficient.[30] If the entity relies on information technology in its operations, management designs control activities to ensure that the information technology continues to operate properly.

Design Control Activities at Various Levels

10.10 Management should design control activities at the appropriate levels in the organizational structure.

10.11 Management designs control activities to ensure the appropriate coverage of objectives and risks in the operations. Operational processes transform inputs into outputs to achieve the organization's objectives. Management designs entity-level control activities, transaction control activities, or both depending on the level of precision needed to ensure that the entity meets its objectives and addresses related risks.

10.12 Entity-level controls are controls that have a pervasive effect on an organization's internal control system and may pertain to multiple components. Entity-level controls may include controls related to the entity's risk assessment process, control environment, service

[30] See paras. 11.07 through 11.10 for further discussion of control activities.

organizations, management override, monitoring, and year-end financial reporting.

10.13 Transaction control activities are actions built directly into operational processes to support the organization in achieving its objectives and addressing related risks. The term “transactions” tends to be associated with financial processes (e.g., payables transactions), while the term “activities” is more generally applied to operational or compliance processes. For the purposes of this standard, “transactions” covers both definitions. Management may design a variety of transaction control activities for operational processes, which may include verifications, reconciliations, authorizations and approvals, physical control activities, and supervisory control activities.

10.14 When choosing between entity-level and transaction control activities, management evaluates the level of precision needed for the operational processes to meet the organization’s objectives and address related risks. In determining the necessary level of precision for a control activity, management evaluates:

- Purpose of the control activity - A control activity that functions to prevent or detect generally is more precise than a control activity that merely identifies and explains differences.
- Level of aggregation - A control activity that is performed at a more granular level generally is more precise than one performed at a higher level. For example, an analysis of obligations by budget object class normally is more precise than an analysis of total obligations for the organization.
- Consistency of performance - A control activity that is performed routinely and consistently generally is more precise than one performed sporadically.
- Correlation to relevant operational processes - A control activity that is directly related to an operational process generally is more likely to prevent or detect than a control activity that is only indirectly related.

Consider Segregation of Duties

10.15 Management should consider segregation of duties in designing the assignment of control activity responsibilities.

10.16 Management considers segregation of duties in designing control activity responsibilities to ensure that incompatible duties are segregated and, where such segregation is not practical, designs alternative control activities to address the risk.

10.17 Segregation of duties helps prevent fraud, waste, and abuse in the internal control system.[31] Management considers the need to separate control activities related to authority, custody, and accounting of operations to achieve adequate segregation of duties. In particular, segregation of duties can address the risk of management override. Management override circumvents existing control activities and is a means of committing fraud. Management addresses this risk through segregation of duties, but cannot absolutely prevent it due to the risk of collusion, where two employees collude to commit fraud.

10.18 If segregation of duties is not practical within an operational process due to limited personnel or other factors, management designs alternative control activities to address the risk of fraud, waste, or abuse in the operational process.

Principle 11 – Design Activities for the Information System

11.01 Management should design control activities for the entity's information system.

Attributes

11.02 The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

a. Design the Entity's Information System - Management should design the entity's information system to respond to the entity's objectives and risks.

b. Design Appropriate Types of Control Activities - Management should design appropriate types of control activities in the entity's information system.

[31] See paras. 8.03 through 8.05 for further discussion of fraud, waste, and abuse.

c. Design the Information Technology Infrastructure - Management should design control activities over the information technology infrastructure.

d. Design Security Management - Management should design control activities for security management over the entity's information system.

e. Design Information Technology Acquisition, Development, and Maintenance - Management should design control activities over the acquisition, development, and maintenance of information technology.

Design the Entity's Information System

11.03 Management should design the entity's information system to respond to the entity's objectives and risks.

11.04 Management designs the entity's information system to obtain and process information to meet each operational process's information requirements and to respond to the entity's objectives and risks. An information system is the people, processes, data, and technology management organizes to obtain, communicate, or dispose of information. An information system represents the life cycle of information used for the entity's operational processes that enables the entity to obtain, store, and process quality information. An information system includes both manual and technology-enabled information processes. Technology-enabled information processes are commonly referred to as information technology. As part of the control environment component, management defines responsibilities, assigns them to key roles, and delegates authority to achieve the entity's objectives. As part of the risk assessment component, management identifies the risks related to the entity and its objectives including its service organizations, the entity's risk tolerance, and risk responses. Management designs control activities to fulfill defined responsibilities and address the identified risk responses for the entity's information system.

11.05 Management designs the entity's information system and the use of information technology by considering the defined information requirements for each of the entity's operational processes.[32] Information technology enables information related to operational processes to become more available to the entity on a timely basis. Additionally, information technology may enhance internal control over

[32] See paras. 13.03 through 13.05 for further discussion of defined information requirements.

security and confidentiality of information by appropriately restricting access. Although information technology implies specific types of control activities, information technology is not a “stand-alone” control consideration. It is an integral part of most control activities.

11.06 Management also evaluates information processing objectives to meet the defined information requirements. Information processing objectives may include:

- Completeness - Transactions that occur are recorded and not understated.
- Accuracy - Transactions are recorded at the correct amount in the right account (and on a timely basis) at each stage of processing.
- Validity - Recorded transactions represent economic events that actually occurred and were executed according to prescribed procedures.

Design Appropriate Types of Control Activities

11.07 Management should design appropriate types of control activities in the entity’s information system.

11.08 Management designs appropriate types of control activities in the entity’s information system to ensure coverage of information processing objectives for operational processes. For information systems, there are two main types of control activities: general and application control activities.

11.09 Information system general controls (entity-wide, system, and application levels) are the policies and procedures that apply to all or a large segment of an entity’s information systems. General controls help ensure the proper operation of information systems by creating the environment for proper operation of application controls. General controls include security management, logical and physical access, configuration management, segregation of duties, and contingency planning.

11.10 Application controls, sometimes referred to as business process controls, are those controls that are incorporated directly into computer applications to help ensure the validity, completeness, accuracy, and confidentiality of transactions and data during application processing.

Application controls include controls over input, processing, output, master file, interface, and data management system controls.

Design the Information Technology Infrastructure

11.11 Management should design control activities over the information technology infrastructure.

11.12 Management designs control activities over the information technology infrastructure to support the completeness, accuracy, and validity of information processing by information technology. Information technology requires an infrastructure in which to operate, including communication networks for linking information technologies, computing resources for applications to operate, and electricity to power the information technology. An entity's information technology infrastructure can be complex. It may be shared by different units within the entity or outsourced either to service organizations or to location-independent technology services (e.g., cloud computing). Management evaluates the objectives of the entity and related risks in designing control activities over the information technology infrastructure.

11.13 Management continues to evaluate changes in the use of information technology and designs new control activities when these changes are incorporated into the entity's information technology infrastructure. Management also designs control activities needed to maintain the information technology infrastructure. Maintaining technology often includes backup and recovery procedures, as well as continuity of operations plans, depending on the risks and consequences of a full or partial power systems outage.

Design Security Management

11.14 Management should design control activities for security management over the entity's information system.

11.15 Management designs control activities for security management over the entity's information system to ensure appropriate access by internal and external sources to protect the entity's information system. Objectives for security management include confidentiality, integrity

and availability. Confidentiality means that data, reports and other outputs are safeguarded against unauthorized access. Integrity means that information is guarded against improper modification or destruction, which includes ensuring information's nonrepudiation and authenticity. Availability means that data, reports, and other relevant information are readily available to users when needed.

11.16 Security management includes the information processes and control activities related to access rights in an entity's information technology, including who has the ability to execute transactions. Security management includes access rights across various levels of data, operating system (system software), network, application, and physical layers. Management designs control activities over access to protect an entity from inappropriate access and unauthorized use of the system. These control activities support appropriate segregation of duties. By preventing unauthorized use of and changes to the system, data and program integrity are protected from malicious intent (e.g., someone breaking into the technology to commit fraud, vandalism, or terrorism) or error.

11.17 Management evaluates security threats to information technology, which can be from both internal and external sources. External threats are particularly important for entities that depend on telecommunications networks and the Internet. External threats have become prevalent in today's highly interconnected business environments, and continual effort is required to address these risks. Internal threats may come from former or disgruntled employees. They pose unique risks because they may be both motivated to work against the entity and better equipped to succeed in carrying out a malicious act as they have greater access to and knowledge of the entity's security management systems and processes.

11.18 Management designs control activities to limit user access to information technology through authorization control activities where a unique user identification or token is authorized by an approved list. These control activities may restrict authorized users to the applications or functions commensurate with their assigned responsibilities, supporting an appropriate segregation of duties. Management designs other control activities to update access rights when employees change job functions or leave the entity. Management also designs control

activities for access rights when different information technology elements are connected to each other.

Design Information Technology Acquisition, Development, and Maintenance

11.19 Management should design control activities over the acquisition, development, and maintenance of information technology.

11.20 Management designs control activities over the acquisition, development, and maintenance of information technology. Management may use the Systems Development Life Cycle (SDLC) framework in designing control activities. An SDLC provides a structure for a new information technology design by outlining specific phases and documenting requirements, approvals, and checkpoints within control activities over the acquisition, development, and maintenance of technology. Through the SDLC, management designs control activities over changes to technology. This may involve requiring authorization of change requests, reviewing the changes, approvals, testing results, and designing protocols to determine whether changes are made properly. Depending on the size and complexity of the entity, development of information technology and changes to the information technology may be included in one SDLC or two separate methodologies. Management evaluates the objectives and risks of the new technology in designing control activities over its SDLC.

11.21 Management may also acquire information technology through packaged software from vendors. Management incorporates into its information technology development methodologies for the acquisition of vendor packages and designs control activities over their selection, ongoing development, and maintenance. Control activities on the development, maintenance, and change of application software prevent unauthorized programs or modifications to existing programs.

11.22 Another alternative is outsourcing the development of information technology to service organizations. As for an SDLC developed internally, management designs control activities to meet objectives and address related risks. Management also evaluates the unique risks that utilizing a service organization presents for the completeness, accuracy, and validity of information submitted to and received from the service organization.

Principle 12 – Implement Control Activities

12.01 Management should implement control activities.

Attributes

12.02 The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

a. Document Responsibilities through Policies - Management should document in policies the internal control responsibilities of the organization.

b. Perform Periodic Review - Management should periodically review the implementation of control activities to determine their continued relevance, redesign them when necessary, and communicate them as appropriate.

Document Responsibilities through Policies

12.03 Management should document in policies the internal control responsibilities of the organization.

12.04 Management documents in policies for each unit its responsibility for an operational process's objectives and related risks, control activity design, implementation, and operating effectiveness.[33] Each unit, with guidance from management, determines based on the objectives and related risks the number of policies necessary for the operational process. Each unit also documents policies in the appropriate level of detail to allow management to effectively monitor the control activity.

[33] See paras. 3.03 through 3.07 for further discussion of units.

Elements of a written policy may include:

- **Timeliness** – Management documents when a control activity and any follow-up corrective actions are performed.

- **Corrective actions** – Management documents the need for appropriate follow-up when matters are identified that require investigation, and establishes responsibility for any corrective actions taken.

- **Competence** – Management documents the level of competency required to perform a control activity. Requirements depend on factors such as the complexity of the control activity and the complexity and volume of the underlying transactions.

12.05 Those in key roles for the unit may further define policies through day-to-day procedures, depending on the rate of change in the operating environment and complexity of the operational process. Procedures may include the timing of when a control activity occurs, and any follow-up corrective actions to be performed by competent personnel if deficiencies are identified.[34] Management communicates to personnel the policies and procedures so that personnel can implement the control activities for their assigned responsibilities.

Perform Periodic Review

12.06 Management should periodically review the implementation of control activities to determine their continued relevance, redesign them when necessary, and communicate them as appropriate.

12.07 Management periodically reviews policies, procedures, and related control activities for continued relevance and effectiveness in achieving the entity's objectives or addressing related risks. If there is a significant change in an entity's process, management reviews this process in a timely manner after the change to ensure the control activities are designed and implemented appropriately. Changes may occur in personnel, operational processes, or information technology. Regulators, Congress, and OMB, may also change either an entity's objectives or how an entity is to achieve an objective. Management considers these changes in its periodic review.

[34] See paras. 17.09 through 17.10 for further discussion of corrective actions.

Information and Communication

Overview

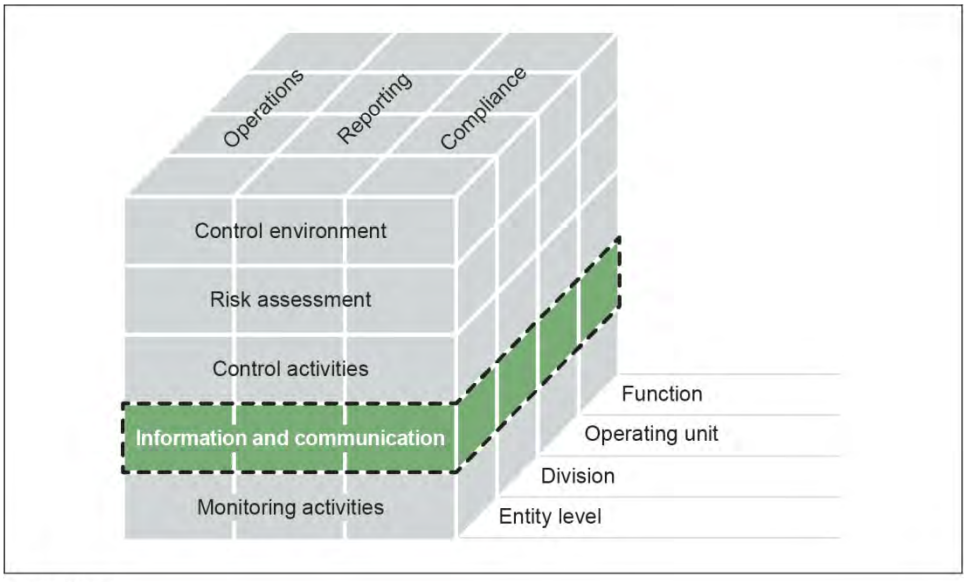
Management uses quality information to support the internal control system. Effective information and communication is vital for an entity to run and control its operations. Entity management needs access to relevant and reliable communication related to internal as well as external events.

Principles

13. Management should use quality information.

14. Management should internally communicate the necessary quality information.

15. Management should externally communicate the necessary quality information.



Source: COSO.

Principle 13 - Use Quality Information

13.01 Management should use quality information.

Attributes

13.02 The following attributes contribute to the design, implementation and operating effectiveness of this principle:

a. Identify Information Requirements - Management should design a process to identify information requirements.

b. Obtain Relevant Data from Reliable Sources - Management should obtain relevant data from reliable internal and external sources on a timely basis based on the identified information requirements.

c. Process Data into Quality Information - Management should process the obtained data into quality information.

Identify Information Requirements

13.03 Management should design a process to identify information requirements.

13.04 Management designs a process that uses the entity's objectives and related risks to identify the information requirements needed to achieve the objectives and address the risks. Information requirements consider the expectations of both internal and external users. Management defines the identified information requirements at the relevant level and requisite specificity for appropriate personnel.

13.05 Management identifies information requirements in an iterative and ongoing process that occurs throughout the performance of an effective internal control system. As change in the entity and its objectives and risks occur, management changes information requirements as needed to meet these modified objectives and address these modified risks.

Obtain Relevant Data from Reliable Sources

13.06 Management should obtain relevant data from reliable internal and external sources on a timely basis based on the identified information requirements.

13.07 Management obtains relevant data from reliable internal and external sources on a timely basis based on the identified information requirements. Relevant data has a logical connection with, or bearing upon, the identified information requirements. Reliable internal and external sources provide data that are reasonably free from error and bias and faithfully represent what they purport to represent. Management evaluates both internal and external sources of data to ensure that they are reliable. Sources of data can be operational, financial, or compliance related. Management obtains data on a timely basis to allow it to be used for effective monitoring.

Process Data into Quality Information

13.08 Management should process the obtained data into quality information.

13.09 Management processes the obtained data into quality information that supports the internal control system. This involves processing data into information and then evaluating the processed information to ensure that it is quality information. Quality information meets the identified information requirements by using relevant data from reliable sources. Quality information is appropriate, current, accurate, accessible, and provided on a timely basis. Management considers these characteristics as well as the information processing objectives in evaluating processed information and makes revisions when necessary to ensure that the information is quality information.[35] Management uses the quality information to make informed decisions and evaluate the entity's performance in achieving key objectives and addressing risks.

13.10 Management processes relevant data from reliable sources into quality information within the organization's information system. An information system is the people, processes, data, and technology

[35] See paras. 11.03 through 11.06 for further discussion of information processing objectives.

management organizes to obtain, communicate, or dispose of information.[36]

Principle 14 - Communicate Internally

14.01 Management should internally communicate the necessary quality information.

Attributes

14.02 The following attributes contribute to the design, implementation and operating effectiveness of this principle:

a. Communicate throughout the Entity - Management should communicate quality information throughout the entity utilizing established reporting lines.

b. Select Appropriate Method of Communication - Management should select appropriate methods to communicate internally.

Communicate throughout the Entity

14.03 Management should communicate quality information throughout the entity utilizing established reporting lines.

14.04 Management communicates quality information throughout the entity utilizing established reporting lines. Quality information is communicated down, across, up, and around reporting lines to all levels of the entity.

14.05 Management communicates quality information down and across reporting lines to enable personnel to perform key roles in achieving objectives, addressing risks, and supporting the internal control system. In these communications, management assigns the internal control responsibilities for key roles.

14.06 Management receives quality information about the entity's operational processes that flows up the reporting lines from personnel to help management achieve the entity's objectives.

[36] See paras. 11.03 through 11.06 for further discussion of information systems.

14.07 The oversight body receives quality information that flows up the reporting lines from management and personnel. Information relating to internal control communicated to the oversight body includes significant matters about the adherence to, changes in, or issues arising from the internal control system. This upward communication is necessary for the effective oversight of internal control.

14.08 Personnel utilize separate reporting lines to go around upward reporting lines when these lines are compromised. Laws and regulations may require entities to establish separate lines of communication, such as whistleblower and ethics hotlines, for communicating confidential information. Management informs employees of these separate reporting lines, how they operate, how they are to be used, and how the information will remain confidential.

Select Appropriate Methods of Communication

14.09 Management should select appropriate methods to communicate internally.

14.10 Management selects appropriate methods to communicate internally. Management considers a variety of factors in selecting an appropriate method of communication. Some factors to consider:

- Audience - The intended recipients of the communication
- Nature of Information - The purpose and type of information being communicated
- Availability - Information readily available to the audience when needed
- Cost - The resources used to communicate the information
- Legal or Regulatory requirements - Requirements by laws and regulations that may impact communication, such as retention requirements

14.11 Based on the consideration of the factors, management selects appropriate methods of communication, such as a written document, whether in hard copy or electronic format, or a face-to-face meeting. Management periodically evaluates the organization's methods of communication to ensure that the organization has the appropriate tools to communicate quality information throughout the entity on a timely basis.

Principle 15 - Communicate Externally

15.01 The organization should externally communicate the necessary quality information.

Attributes

15.02 The following attributes contribute to the design, implementation and operating effectiveness of this principle:

a. Communicate with External Parties - Management should communicate with, and obtain quality information from, external parties utilizing established reporting lines.

b. Select Appropriate Method of Communication - Management should select appropriate methods to communicate externally.

Communicate with External Parties

15.03 Management should communicate with, and obtain quality information from, external parties utilizing established reporting lines.

15.04 Management communicates with, and obtains quality information from, external parties utilizing established reporting lines. Open two-way external reporting lines allow for this communication. External parties include stakeholders,[37] suppliers, contractors, service organizations, regulators, external auditors, government entities, and the general public.

15.05 Management communicates quality information externally through reporting lines so that external parties can help the entity achieve its objectives and address related risks. Management includes in these communications information relating to the organization's events and activities that impact the internal control system.

15.06 Management receives information through reporting lines from external parties. Information communicated to management includes significant matters relating to risks, changes, or issues that impact the entity's internal control system. This communication is necessary for the effective operation of internal control. Management evaluates external

[37] See paras. 2.03 through 2.10 for further discussion of stakeholders.

information received against the characteristics of quality information and information processing objectives and takes any necessary actions to ensure that the information is quality information.[38]

15.07 The oversight body receives information through reporting lines from external parties. Information communicated to the oversight body includes significant matters relating to risks, changes, or issues that impact the entity's internal control system. This communication is necessary for the effective oversight of internal control.

15.08 External parties utilize separate reporting lines when external reporting lines are compromised. Laws and regulations may require entities to establish separate lines of communication, such as whistleblower and ethics hotlines, for communicating confidential information. Management informs external parties of these separate reporting lines, how they operate, how they are to be used, and how the information will remain confidential.

Select Appropriate Methods of Communication

15.09 Management should select appropriate methods to communicate externally.

15.10 Management selects appropriate methods to communicate externally. Management considers a variety of factors in selecting an appropriate method of communication. Some factors to consider:

- Audience - The intended recipients of the communication
- Nature of Information - The purpose and type of information being communicated
- Availability - Information readily available to the audience when needed
- Cost - The resources used to communicate the information
- Legal or Regulatory requirements - Requirements by laws and regulations that may impact communication

[38] See paras. 11.03 through 11.06 for further discussion of information processing objectives.

15.11 Based on the consideration of the factors, management selects appropriate methods of communication, such as a written document, whether in paper or electronic format, or a face-to-face meeting. Management periodically evaluates the organization's methods of communication to ensure that the organization has the appropriate tools to communicate quality information throughout and outside of the entity on a timely basis.

15.12 In the federal government, organizations not only report to Congress and the President but to the general public as well. Organizations need to consider appropriate methods when communicating with such a broad audience.

Monitoring

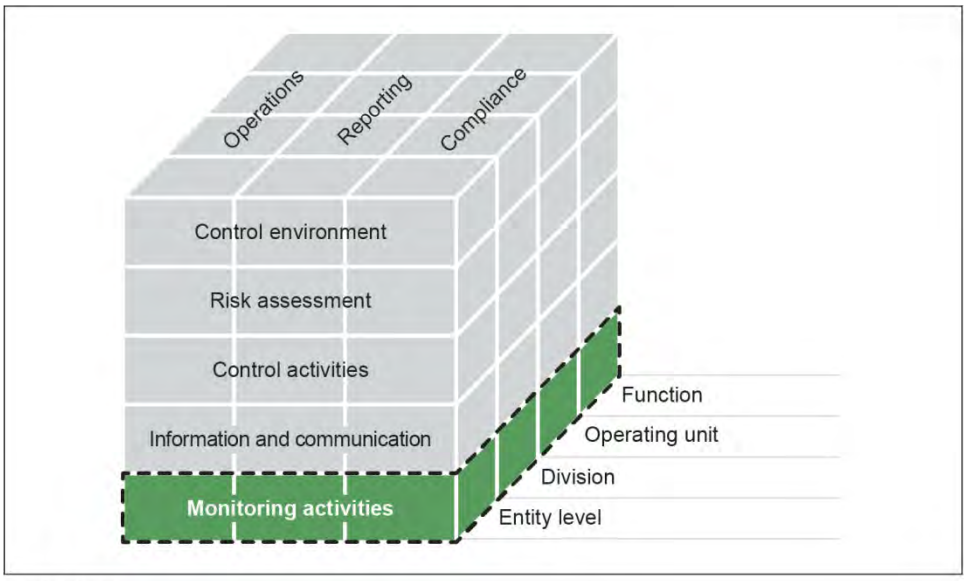
Overview

Finally, since internal control is a dynamic process that has to be adapted continuously to the risks and changes an organization faces, monitoring of the internal control system is essential to help ensure that internal control remains aligned with changing objectives, environment, laws, resources, and risks. Internal control monitoring assesses the quality of performance over time and ensures that the findings of audits and other reviews are promptly resolved. Corrective actions are a necessary complement to control activities in order to achieve objectives.

Principles

16. Management should establish monitoring activities to monitor the internal control system and evaluate the results.

17. Management should ensure identified internal control deficiencies are remediated on a timely basis.



Source: COSO.

Principle 16 - Perform Monitoring Activities

16.01 Management should establish monitoring activities to monitor the internal control system and evaluate the results.

Attributes

16.02 The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

a. Establish a Baseline - Management should establish a baseline for monitoring the internal control system.

b. Monitor Internal Control System - Management should monitor the internal control system through ongoing monitoring and separate evaluations.

c. Evaluate Results - Management should document and evaluate the results of ongoing monitoring and separate evaluations to identify internal control issues.

Establish a Baseline

16.03 Management should establish a baseline for monitoring the internal control system.

16.04 Management establishes a baseline to monitor the internal control system in supporting the entity in achieving its objectives. The baseline is the current state of the internal control system compared against management's design of the internal control system. The baseline represents the difference between the criteria of the design of the internal control system and condition of the internal control system at a specific point in time. In other words, the baseline consists of issues and deficiencies identified in an entity's internal control system.

16.05 Once established, management can use the baseline as criteria in evaluating the internal control system and make changes to reduce the difference between the criteria and condition. Management reduces this difference in one of two ways. Management either changes the design of the internal control system to better address the objectives and risks of the entity or improves the operating effectiveness of the internal control

system. As part of monitoring, management determines when to revise the baseline to reflect changes in the internal control system.

Monitor Internal Control System

16.06 Management should monitor the internal control system through ongoing monitoring and separate evaluations.

16.07 Management monitors the internal control system through the monitoring activities of ongoing monitoring and separate evaluations. Ongoing monitoring is built into the entity's operations, performed continually, and responsive to change. Separate evaluations are used periodically and may provide feedback on the effectiveness of ongoing monitoring.

16.08 Management performs ongoing monitoring of the design and operating effectiveness of the internal control system as part of the normal course of operations. Ongoing monitoring includes regular management and supervisory activities, comparisons, reconciliations, and other routine actions. Ongoing monitoring may include automated tools, which can increase objectivity and efficiency by electronically evaluating controls and transactions.

16.09 Management uses separate evaluations to monitor the design and operating effectiveness of the internal control system at a specific time or of a specific function or process. The scope and frequency of separate evaluations depend primarily on the assessment of risks, effectiveness of ongoing monitoring, and rate of change within the entity and its environment. Separate evaluations may take the form of self-assessments, which include cross operating unit or cross functional evaluations.

16.10 Separate evaluations also include audits and other evaluations that may involve the review of control design and direct testing of internal control. These audits and other evaluations may be mandated by law and are performed by internal auditors, external auditors, the Inspectors General, and other external reviewers. Separate evaluations provide greater objectivity when performed by reviewers who do not have responsibility for the activities being evaluated.

16.11 Management retains responsibility for monitoring the effectiveness of internal control over the assigned processes performed by service organizations. Management uses ongoing monitoring, separate evaluations, or a combination of the two to obtain reasonable assurance over the operating effectiveness of the service organization's internal controls over the assigned process.[39] These monitoring activities related to service organizations may either be performed by management or performed by external parties and reviewed by management.

Evaluate Results

16.12 Management should evaluate and document the results of ongoing monitoring and separate evaluations to identify internal control issues.

16.13 Management evaluates and documents the results of ongoing monitoring and separate evaluations to identify issues in the internal control system. Management utilizes this evaluation to determine the effectiveness of the internal control system. Differences between the results of monitoring activities and the previously established baseline may indicate internal control issues, including undocumented changes in the internal control system or potential internal control deficiencies.

16.14 Management may identify changes in the internal control system that either have occurred or are needed due to changes in the entity and its environment. External parties can also help management identify issues in the internal control system. For example, complaints from the general public and regulator comments may indicate areas in the internal control system that need improvement. Management considers whether current controls address the identified issues and modifies controls if necessary.

Principle 17 – Remediate Deficiencies

17.01 Management should ensure identified internal control deficiencies are remediated on a timely basis.

[39] See the Overview: Service Organizations for further discussion of service organizations.

Attributes

17.02 The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

a. Report Issues - Personnel should report internal control issues to appropriate internal and external parties on a timely basis.

b. Evaluate Issues - Management should evaluate and document internal control issues and determine appropriate corrective actions for internal control deficiencies on a timely basis.

c. Complete Corrective Actions - Management should complete and document corrective actions to remediate internal control deficiencies on a timely basis.

Report Issues

17.03 Personnel should report internal control issues to appropriate internal and external parties on a timely basis.

17.04 Personnel report internal control issues through established reporting lines to the appropriate internal and external parties on a timely basis to enable the entity to timely evaluate those issues.[40]

17.05 Personnel may identify internal control issues while performing their assigned internal control responsibilities. Personnel communicate these issues internally to the person in the key role responsible for the internal control or associated process and to at least one level of management above that individual. Depending on the nature of the issues, personnel may consider reporting certain issues to the oversight body. Such issues may include:

- Issues that cut across the organizational structure or extend outside the organization to service organizations, contractors, or suppliers.
- Issues that may not be remediated due to the interests of management, such as sensitive information regarding fraud or other illegal acts.[41]

[40] See paras. 14.03 through 14.08 for further discussion of internal reporting lines and paras. 15.03 through 15.08 for further discussion of external reporting lines.

[41] See paras. 8.03 through 8.05 for further discussion of fraud.

17.06 Depending on the entity's regulatory or compliance requirements, the entity may also be required to report issues externally to appropriate external parties, such as the legislators, regulators and standard-setting bodies that establish laws, rules, regulations, and standards to which the entity is subject.

Evaluate Issues

17.07 Management should evaluate and document internal control issues and determine appropriate corrective actions for internal control deficiencies on a timely basis.

17.08 Management evaluates and documents internal control issues and determines appropriate corrective actions for internal control deficiencies on a timely basis to ensure an effective internal control system. Management evaluates issues identified through monitoring activities or reported by personnel to determine whether any of the issues rise to the level of an internal control deficiency. Internal control deficiencies require further evaluation and remediation by management. An internal control deficiency can be in the design, implementation, or operating effectiveness of the internal control and its related process.[42] Management determines from the type of internal control deficiency the appropriate corrective actions to remediate the internal control deficiency on a timely basis. Management assigns responsibility and delegates authority to remediate the internal control deficiency.

Complete Corrective Actions

17.09 Management should complete and document corrective actions to remediate internal control deficiencies on a timely basis.

17.10 Management completes and documents corrective actions to remediate internal control deficiencies on a timely basis. Depending on the nature of the deficiency, either the oversight body or management oversees the prompt remediation of deficiencies by communicating the corrective actions to the appropriate level of the organizational structure and delegating authority for completing corrective actions to appropriate

[42] See the Overview: Evaluation of an Internal Control System for further discussion of evaluation of internal control deficiency.

personnel. Management, with oversight from the oversight body, tracks the status of remediation efforts to ensure that they are completed on a timely basis.

Glossary

The following terms are provided to assist in clarifying the *Standards for Internal Control in the Federal Government*. The most relevant paragraph numbers are provided for reference.

Terms

Application control activities - Controls that are incorporated directly into computer applications to help ensure the validity, completeness, accuracy, and confidentiality of transactions and data during application processing; application controls include controls over input, processing, output, master file, interface, and data management system controls (paragraph 11.10)

Application material - Additional information that provides further explanation of the principle and attribute requirements of internal control (Overview: Components, Principles and Attributes)

Baseline - The difference between the criteria of the design of the internal control system and condition of the internal control system at a specific point in time (paragraph 16.04)

Competence - The qualification to carry out assigned responsibilities (paragraph 4.04)

Complementary user entity controls - Controls that management of the service organization assumes, in the design of its service, will be implemented by user entities, and which, if necessary to achieve the control objectives stated in management's description of the service organization's system, are identified as such in that description (Overview: Service Organizations).

Contingency plans - The processes defined to address an organization’s need to respond to sudden personnel changes impacting the organization (paragraph 4.10)

Control activities - The policies, procedures, techniques, and mechanisms that enforce management’s directives to achieve the entity’s objectives and address related risks (paragraph 10.04)

Deficiency - When the design, implementation, or operation of a control does not allow management or personnel, in the normal course of performing their assigned functions, to achieve control objectives and address related risks (Overview: Evaluation of Deficiencies in Internal Control)

Detective control - An activity that is designed to discover when an entity is not achieving an objective or addressing a risk before the entity's operation has concluded and corrects the actions so that the entity achieves the objective or addresses the risk (paragraph 10.07)

Entity-level control - Controls that have a pervasive effect on an organization's internal control system; entity-level controls may include controls related to the entity's risk assessment process, control environment, service organizations, management override, monitoring, and year-end financial reporting (paragraph 10.12)

Fraud - Involves obtaining something of value through willful misrepresentation (paragraph 8.04)

General control activities - The policies and procedures that apply to all or a large segment of an entity's information systems; general controls include security management, logical and physical access, configuration management, segregation of duties, and contingency planning (paragraph 11.09)

Green Book - The commonly used name for the *Standards for Internal Control in the Federal Government* (Overview: Foreword)

Information system - The people, processes, data, and technology management organizes to obtain, communicate, or dispose of information (paragraph 11.04)

Information technology - Technology-enabled information processes (paragraph 11.04)

Inherent risk - The risk to an entity in the absence of management's response to the risk (paragraph 7.05)

Internal control - The plans, methods, policies, and procedures used to fulfill the mission, strategic plan, goals, and objectives of the organization (Overview: Definition of Internal Control)

Internal control system - A continuous built-in component of operations, effected by people, that provides reasonable assurance, not absolute assurance, that an organization's objectives will be achieved (Overview: An Internal Control System)

Key role - A position in an organizational structure that is assigned an overall responsibility of an entity (paragraph 3.09)

Likelihood of occurrence - The possibility that a risk will occur (paragraph 7.09)

Magnitude of impact - Magnitude of deficiency that could result from the risk and is affected by factors such as the size, pace, and duration of the risk's impact (paragraph 7.09)

Management - Entity personnel who are directly responsible for all activities of an organization, including the design, implementation, and operating effectiveness of an entity's internal control system (Overview: Roles in an Internal Control System)

Organizational structure - The operating units, operational processes, and other structures management uses to achieve objectives (Overview: Internal Control and the Entity)

Oversight body - Those responsible for overseeing management's design, implementation, and operation of an internal control system (Overview: Roles in an Internal Control System)

Performance measure - A means of evaluating the entity's performance in achieving objectives (paragraph 6.09)

Policies - Statements of responsibility for an operational process's objectives and related risks, control activity design, implementation, and operating effectiveness (paragraph 12.04)

Preventive control - An activity that is designed to prevent an entity from failing to achieve an objective or addressing a risk (paragraph 10.07)

Qualitative objectives - Subjective objectives where management may need to design performance measures that indicate a level or degree of performance, such as milestones (paragraph 6.09)

Quality information - Information from relevant and reliable data that is appropriate, current, accurate, accessible, provided on a timely basis, and meets the need of identified information requirements (paragraph 13.09)

Quantitative objectives - Calculable objectives where performance measures may be a targeted percentage or numerical value (paragraph 6.09)

Reasonable assurance - A high degree of confidence, but not absolute confidence (Overview: An Internal Control System)

Reporting lines - Communication lines at all levels of the organization that provide methods of communication that can flow down, across, up, and around the organizational structure (paragraph 3.06)

Residual risk - The risk that remains after management's response to inherent risk (paragraph 7.05)

Risk - The possibility that an event will occur and adversely affect the achievement of objectives (paragraph 7.03)

Risk tolerance - The acceptable level of variation in performance relative to the achievement of objectives (paragraph 6.11)

Security management - The information processes and control activities related to access rights in an entity's information technology (paragraph 11.16)

Segregation of duties - The separation of the authority, custody and accounting of an operation (paragraph 10.17)

Service organization - An external party that performs operational process(es) for an entity (Overview: Service Organizations)

Succession plans - The processes that address an organization's need to replace competent personnel over the long term (paragraph 4.10)

Transaction control activities - Actions built directly into operational processes to support the organization in achieving its objectives and addressing related risks (paragraph 10.13)

Appendix I – Comptroller General's Advisory Council on Standards for Internal Control in the Federal Government and GAO Project Team

Advisory Council Members (2013-2015)

Jon Rymer, Chair
Federal Deposit Insurance Corporation

Brett Baker
National Science Foundation

Lisa Casias
Department of Commerce

Carole Clay
State Department

Melinda DeCorte
Cotton & Company LLP

Stephen Eells
New Jersey, Office of the State Auditor

Carol M. Eyermann
National Science Foundation

William (Bill) Hughes
MorganFranklin

Scot Janssen
KPMG LLP

John Kaschak
Pennsylvania Office of the Budget, Bureau of Audits

David L. Landsittel
COSO

Samuel T. Mok
Condor International Advisors, LLC

Kenneth J. Mory
City of Austin, Texas

Dan Murrin
Ernst & Young

Annette K. Pridgen
Jackson State University

Sandra B. Richtermeyer
Xavier University

Neil Ryder
Department of Justice

Peggy Sherry
Department of Homeland Security

F. Michael Taylor
Hanover County Government

David A. Von Moll
Commonwealth of Virginia Office of the State Comptroller

David M. Zavada
Kearney & Company

GAO Project Team

Steven J. Sebastian, Managing Director
James R. Dalkin, Project Director
Robert F. Dacey, Chief Accountant
Heather I. Keister, Assistant Director
Kristen A. Kociolek, Assistant Director
Brian S. Harechmak, Senior Auditor
Bernice M. Lemaire, Senior Auditor
Mary O. Osorno, Senior Auditor
Christie A. Pugnetti, Senior Auditor
Grant L. Simmons, Senior Auditor
Doris G. Yanger, Senior Auditor
Lee Evans, Auditor
Marci L. Goasdone, Auditor
Debra L. Hoffman, Auditor
Alan S. MacMullin, Auditor
Andrew D. Seehusen, Auditor
Jacquelyn Hamilton, Deputy Assistant General Counsel
Francine M. DelVecchio, Supervisory Communications Analyst

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Federal Equal Opportunity Recruitment Program (FEORP) for Fiscal Year 2012

PSSC: PRG B.1

Purpose: (b) (5)

Source: OPM

Report to the Congress

Prepared by: Sopeany Keo, SR Auditor

Reviewed by: Kimberly Perteet, SR Auditor

A New Day for Federal Service

UNITED STATES OFFIC OF PERSONNEL MANAGEMENT
January 2014

A MESSAGE FROM THE DIRECTOR OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT (OPM)

I am pleased to submit the annual Federal Equal Opportunity Recruitment Program (FEORP) Report for Fiscal Year (FY) 2012 to Congress. Prepared in accordance with the requirements of title 5, United States Code, section 7201, this report provides statistical data on employment in the Federal workforce (FW) and highlights human capital practices Federal agencies are using to recruit, develop, and retain talent.

Findings for FY 2012

The number of minorities in the FW increased by 1.2 percent from 662,991 in FY 2011 to 670,853 in FY 2012. The FW is 17.9 percent Black, 8.2 percent Hispanic, 5.8 percent Asian/Pacific Islander, 1.7 percent American Indian/Alaska Native, 1.0 percent Non-Hispanic/Multi-Racial, and 65.4 percent White. Minorities as a whole constituted 34.6 percent of the FW. Men comprised 56.5 percent of all Federal permanent employees and women 43.5 percent. Notably, the Federal government still faces challenges with regard to the full employment of Hispanics, as they constitute 8.2 percent of the FW.

The Senior Executive Service (SES) is now more diverse than ever. The SES is 10.5 percent Black, 4.1 percent Hispanic, 3.3 percent Asian/Pacific Islander, 1.4 percent American Indian/Alaska Native, and 0.6 percent Non-Hispanic/Multi-Racial. In addition, women now make up 33.5 percent of the SES.

OPM Initiatives

Since 2009 President Obama has signed various Executive Orders aimed at promoting a diverse and inclusive Federal workforce. On August 19, 2011, the President signed and issued Executive Order 13583, *Establishing a Coordinated Government-Wide Initiative to Promote Diversity and Inclusion in the Federal Workforce*, in order to promote the Federal workplace as a model of equality, diversity, and inclusion. On November 17, 2011, OPM issued the Government-Wide Diversity and Inclusion Strategic Plan, which identified three goals for implementation by agencies to include Workforce Diversity, Workplace Inclusion, and Sustainability. Fifty-seven agencies submitted agency-specific Diversity and Inclusion Strategic Plans, and they continue to actively implement those plans with guidance from OPM.

On November 9, 2009, President Obama signed Executive Order 13518, Employment of Veterans in the Federal Government, which established the Veterans Employment Initiative. In the first full year, the Executive Branch of the Government hired the highest percentage of veterans in more than 20 years.

In addition, OPM is committed to assisting agencies in implementing Executive Order 13548, Increasing Federal Employment of Individuals with Disabilities. The goal under Executive Order 13548 is to hire 100,000 people with disabilities in all job series and at all

grade levels by 2015 in order to enable the Federal Government to tap into this rich source of diverse talent. Initial FY 2012 data indicates an increase in the hiring of people with disabilities as compared to 2011, and in FY 2011, Americans with disabilities, including veterans who are 30 percent or more disabled, made up 14.7 percent of new hires, a 20-year high.

To address difficulties recruiting and hiring students, recent graduates and Veterans, President Obama signed Executive Order 13562, Recruiting and Hiring Students and Recent Graduates, on December 27, 2010. This executive order establishes the Pathways Program, consisting of three excepted-service programs tailored to recruit, hire, develop, and retain students and recent graduates to include veterans. Under this program, OPM is conducting outreach to, among others, Historically Black Colleges and Universities, Hispanic Serving Institutions, Tribal Colleges and Universities, and Asian American and American Indian/Alaska Native Pacific Islander Serving Institutions. Additionally, through the creation of the *Governmentwide Veterans Recruitment and Employment Strategic Plan for FY 2010–FY 2012*, OPM is helping agencies to meet the overarching goal to increase the percentage of veterans hired in the Federal Executive Branch.

Due to the challenge of underrepresentation of Hispanics in the Federal workforce, OPM renewed the Hispanic Council on Federal Employment (Council) through 2014. This Council, which brings together leaders from the Hispanic community, Human Resources (HR), Equal Employment Opportunity (EEO), and Diversity and Inclusion (D&I), is actively advising the Director of OPM on specific practices and recommendations related to the recruitment, hiring, retention, and advancement of Hispanics in the Federal workplace.

Finally, the OPM is working with the Chief Human Capital Officers (CHCO) Council and agencies to assess current and emerging skills gaps and develop strategies to close these gaps in mission-critical occupations and skills areas that have the greatest impact on government-wide, and agency-specific, performance. The desired outcomes of this effort are: (1) increased proficiency levels in targeted skills areas through training, and (2) institutionalized processes for identifying and addressing skills gaps (government-wide and agency-specific).

These efforts are designed to provide agencies with the foundation and support they need to advance the Federal government's goals - to recruit, hire, retain, and develop qualified candidates for Federal service. OPM will continue to work with agencies to ensure that they have the tools required to succeed in creating and developing a diverse and inclusive Federal workforce that is a model for the 21st Century.

Katherine L. Archuleta
Director

TABLE OF CONTENTS

EXECUTIVE SUMMARY

On August 18, 2011, President Obama signed Executive Order 13583, Establishing a Coordinated Government-Wide Initiative to Promote Diversity and Inclusion in the Federal Workforce. As a result, OPM in consultation with the Office of Management and Budget (OMB) and the Equal Employment Opportunity Commission (EEOC) developed a Government-Wide Diversity and Inclusion Strategic Plan (Plan) that provides guidance to agencies on implementing the President's Executive Order (the Executive Order). The Plan provides a shared direction, encourages commitment, and creates alignment so agencies can approach their workplace diversity and inclusion efforts in a coordinated, collaborative, and integrated manner. Three key goals provide a path for successful agency diversity and inclusion efforts: workforce diversity, workplace inclusion, and sustainability.

On March 16, 2012, 120 days after the issuance of the Government-Wide Diversity and Inclusion Strategic Plan, agencies were required to submit agency-specific Diversity and Inclusion Strategic Plans, consistent with the government-wide plan. Fifty-seven departments and agencies submitted plans, and OPM continues to conduct Feedback Assistance Roundtables (FAR), a three phased review process, with each agency's Chief Human Capital Officer (CHCO), Equal Employment Opportunity (EEO) Director, and Diversity and Inclusion (D&I) Director, where one exists. During Phase I of the FAR review, which was completed in July 2012, agencies met in clusters of three (3) in the OPM Innovation Lab to share successful practices and address challenges. OPM is now conducting Phase II of the FAR review, which entails meeting with each agency individually and discussing progress on the agency-specific Diversity and Inclusion Strategic Plans. Phase III will begin approximately 18 months after the submission of the plans and will include metric analysis for each agency, related to the three goals of diversity, inclusion, and sustainability.

In addition, the Executive Order directed agencies to identify and adopt best practices to promote diversity and inclusion and to identify and remove any barriers to equal employment opportunity, consistent with merit system principles and applicable law. To this end, agencies were asked to submit their successful or promising practices from the agency-specific Diversity and Inclusion Strategic Plans. This report provides information about those successful practices that agencies discussed during the FAR process or submitted in their FEORP reports.

Against this backdrop, we present the data for the FY 2012 FEORP Report.

FEORP Composition of Federal Workforce at a Glance

	Representation of the Federal Workforce		Representation in the Senior Executive Service	
	FY 2012	FY 2011	FY 2012	FY 2011
Men	56.5	56.4	66.5	67.7
Women	43.5	43.6	33.5	32.3
Hispanic or Latino	8.2	8.1	4.1	4.1
White	65.4	65.9	80.6	81.2
Black or African American	17.9	17.8	10.5	10.1
Asian/Pacific Islander	5.8	5.6	3.3	3.2
American Indian/Alaska Native	1.7	1.7	1.4	1.1
Non-Hispanic/Multi-Racial	1.0	0.8	0.6	0.5

Major findings in the FY 2012 FEORP Report are:

- The number of minorities in the FW increased by 1.2 percent from 662,991 in FY 2011 to 670,853 in FY 2012. The FW is 17.9 percent Black, 8.2 percent Hispanic, 5.8 percent Asian/Pacific Islander, 1.7 percent American Indian/Alaska Native, 1.0 percent Non-Hispanic/Multi-Racial, and 65.4 percent White. Minorities as a whole constituted 34.6 percent of the FW.
- Black employees represented 17.9 percent (346,824) of the permanent FW as of September 30, 2012, compared to 17.8 percent in FY 2011.
- Hispanic employees represented 8.2 percent (159,639) of the permanent FW as of September 30, 2012, compared to 8.1 percent in FY 2011.
- Asian/Pacific Islander employees represented 5.8 percent (112,261) of the permanent FW as of September 30, 2012, compared to 5.6 percent in FY 2011.
- American Indian/Alaska Native employees represented 1.7 percent (33,171) of the permanent FW as of September 30, 2012, compared to 1.7 percent in FY 2011.
- White employees represented 65.4 percent (1,270,362) of the permanent FW as of September 30, 2012, compared to 65.9 percent in FY 2011.
- Non-Hispanic Multi-Racial employees represented 1.0 percent (18,958) of the permanent FW as of September 30, 2012, compared to 0.8 percent in FY 2011.
- Women comprised 43.5 percent (844,223) of all Federal permanent employees as of September 30, 2012, compared to 43.6 percent in FY 2011.
- Men comprised 56.5 percent (1,096,992) of all Federal permanent employees as of September 30, 2012, compared to 56.4 percent in FY 2011.
- The percentage of minorities in the Senior Executive Service (SES) increased by 0.9 percent from 19 percent in FY 2011 to 19.9 percent in FY 2012. The SES is 10.5 percent Black, 4.1 percent Hispanic, 3.3 percent Asian/Pacific Islander, 1.4 percent American Indian/Alaska Native, and 0.6 percent Non-Hispanic/Multi-racial.
- The percentage of women in the Senior Executive Service (SES) increased by 1.2 percent from 32.3 percent in FY 2011 to 33.5 percent in FY 2012.

Federal Agencies' FEORP Report Submissions

In an effort to consolidate reporting requirements that necessitate similar information and provide meaningful guidance to the agencies, the OPM once again requested that Federal agencies jointly submit their FEORP Report and their Hispanic Employment Report, as required by Executive Order 13171 of October 12, 2000. Agencies were provided with the opportunity to include successful practices and planned activities that have been shown to improve the recruitment, career development, and retention of Hispanics, as well as women and other minorities. OPM also requested data regarding mentoring programs, leadership development programs, D&I Councils, and D&I training.

Agency successful practices can be found in the section titled *Agency FEORP Current Practices* on page 72 of this report.

DATA COVERAGE AND DEFINITIONS

On-board Federal employment statistics used in this report are as of September 30, 2011. All data are produced from OPM's Central Personnel Data File (CPDF). The FW referred to in this report is not the entire FW, but rather only permanent employees in those non-postal Federal Executive Branch agencies participating in the CPDF. This report covers workers in all pay plans including General Schedule and Related (GSR) pay plans, non-GSR pay plans, blue-collar pay plans, and employees at Senior Pay levels.

All references made to the General Schedule pay plan in this report are to General Schedule and Related (GSR) pay plans.

Only those agencies with 500 or more permanent employees are displayed in this report.

Non-Hispanic/Multi-Racial is defined as Non-Hispanic and of more than one race.

Senior Pay level employment includes employees in the Senior Executive Service (SES), Senior Foreign Service, and other employees earning salaries above grade 15, step 10 of the General Schedule, but excludes those employees under the Executive Schedule (pay plan EX).

The **Civilian Labor Force** (**CLF)** percentages for each minority group presented in this report are derived from the Bureau of Labor Statistics' (BLS) Current Population Survey (CPS). The CPS data, which is a monthly survey of households that is conducted by the Bureau of the Census for BLS, cover non-institutionalized individuals 16 years of age or older, employed or unemployed, U.S. citizens and non-U.S. citizens. Regarding multi-racial persons, the BLS designation "Two or More Races, Both Sexes" provides the data source for the multi-racial CLF percent.

The **Relevant Civilian Labor Force (RCLF)** is the CLF data that are directly comparable (or relevant) to the occupational population being considered in the FW. The RCLF is the benchmark used to measure individual Federal agencies' minority representation relative to their representation in that occupational category. In this Report, the RCLF is presented for each occupational category in the sections titled "Employment by Occupational Category." For further info on the RCLF, please see the U.S. Census Bureau Equal Employment Opportunity (EEO) Tabulation at http://www.census.gov/people/eeotabulation/about/page_c.html

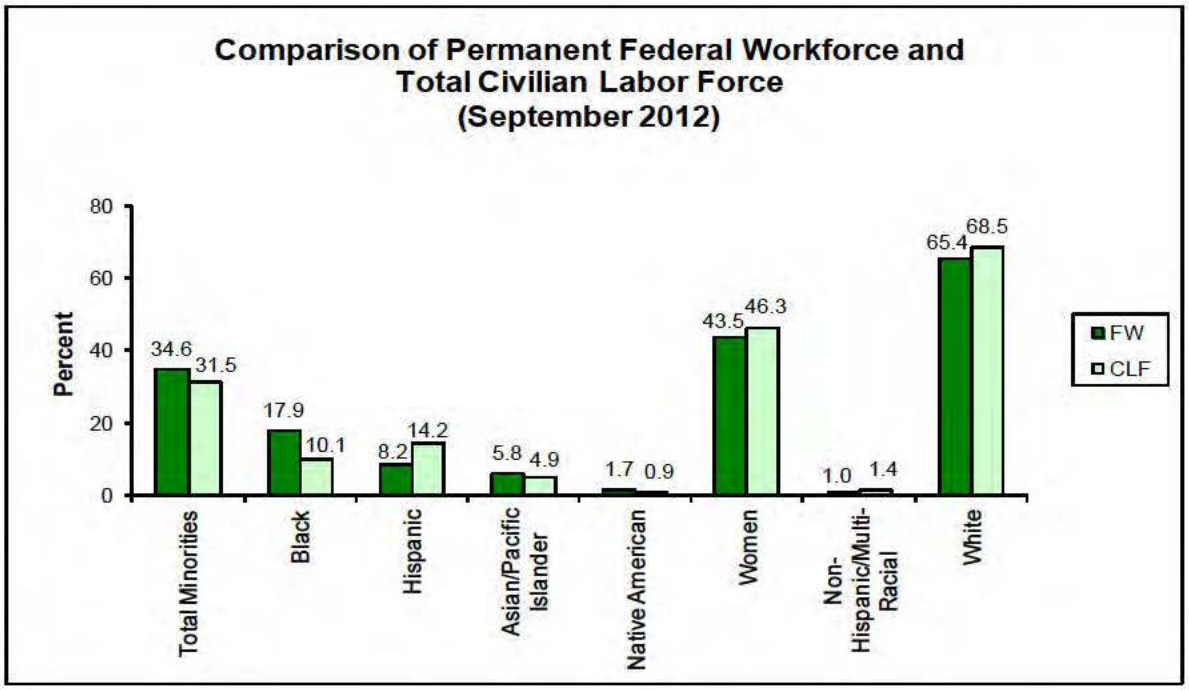
Underrepresentation, as defined in 5 CFR, section 720.202, means a situation in which the number of women or members of a minority group within a category of civil service employment constitutes a lower percentage of the total number of employees within the employment category than the percentage of women or the minority group constitutes within the CLF of the United States.

Occupational categories discussed in this report are white collar and blue collar. The white-collar category contains Professional, Administrative, Technical, Clerical or "Other" white-collar occupations. Professional occupations typically require a baccalaureate or professional degree and, along with Administrative occupations, are the usual sources for selections to senior management and executive positions. Positions in Technical, Clerical, Other, and blue-collar occupations usually are limited to lower grades, with limited opportunity for promotion to management levels. Advancement in these occupations often depends on individual attainment of further education or advanced skills. Employment data in this report are presented by occupational category and grade to provide a more informative profile.

NOTE: STATISTICS IN THIS REPORT MAY VARY FROM OTHER FEORP RELEASES BECAUSE OF DIFFERENCES IN COVERAGE (E.G., AGENCY, WORK SCHEDULE, TENURE, AND DATES). ALSO, PERCENTAGES SHOWN IN THIS REPORT MAY NOT ADD TO TOTALS OF 100 DUE TO INDEPENDENT ROUNDING.

FEDERAL WORKFORCE

TOTAL FEDERAL WORKFORCE EMPLOYMENT[1]



The number of minorities in the FW increased by 1.2percent from 662,991 to 670,853 in FY 2012.

- Blacks represented 17.9 percent (346,824) of the FW in 2012 and 17.8 percent (345,679) in FY 2011. The representation of Blacks in the CLF was 10.1 percent in 2012 and 2011.
- Hispanics represented 8.2 percent (159,639) of the FW in 2012, compared to 8.1 percent (157,648) in FY 2011. The representation of Hispanics in the CLF[2] was 14.2 percent in 2012, compared to 13.6 in 2011.
- Asian/Pacific Islanders represented 5.8 percent (112,261) of the FW in 2012, compared to 5.6 percent (109,871) in FY 2011. The representation of Asians/Pacific Islanders in the CLF[3] was 4.9 percent in 2012, compared to 4.4 in 2011.

---

[1] Detail percentages may not add to total due to rounding.

[2] Although Hispanics, taken as a whole, make up 14.2 percent of the Civilian Labor Force (CLF), that number drops to 10.8 percent of the CLF when only U.S. citizens (including those in Puerto Rico) are counted. (Citizenship is a requirement for most Federal positions.) Citizenship-based CLF calculations are based on the Equal Employment Opportunity (EEO) Tabulation of 5-year ACS data.

[3] Although Asian/Pacific Islanders make up 4.9 percent of the Civilian Labor Force (CLF), that number drops to 3.6 percent of the CLF, when only U.S. citizens are counted. As noted above, citizenship is a requirement for most Federal positions. Citizenship-based CLF calculations are based on the Equal Employment Opportunity (EEO) Tabulation of 5-year ACS data.

- American Indian/Alaska Natives represented 1.7 percent (33,171) of the FW in 2012 and 1.7 percent (33,761) in FY 2011. American Indian/Alaska Natives representation in the CLF was 0.9 percent in 2012, compared to 0.7 in 2011.
- Non-Hispanic Multi-Racial employees represented 1.0 percent (18,958) of the FW in 2012 compared to 0.8 (16,032) in FY 2011. The representation of Non-Hispanic Multi-Racial employees in the CLF was 1.7 percent in 2012, compared to 1.2 in 2011.
- White employees represented 65.4 percent (1,270,362) of the permanent FW as of September 30, 2012, compared to 65.9 (1,281,659). The representation of White employees in the CLF was 68.5 percent in 2012, compared to 70.0 percent in 2011.
- Women represented 43.5 percent (844,223) of the FW in 2012, compared to 43.6 percent (848,257) in FY 2011. The representation of women in the CLF was 46.3 percent in 2012, and the same in 2011.

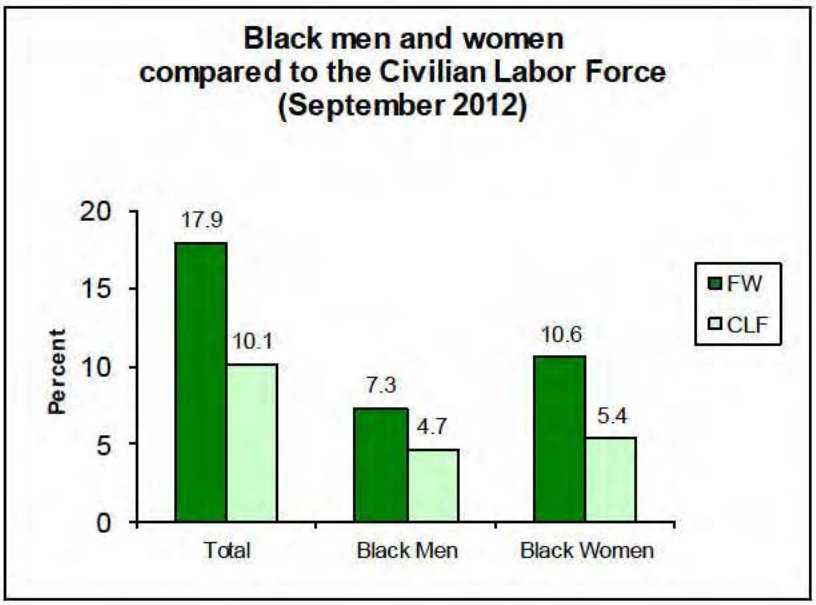
BLACKS IN THE FEDERAL WORKFORCE

BLACK EMPLOYMENT

Black employees represented 17.9 percent (346,824) of the permanent FW as of September 30, 2012 and 17.8 percent in FY 2011.

Black men represented 7.3 percent of the FW in FY 2012 and 7.2 percent in FY 2011.

Black women represented 10.6 percent of the FW in FY 2012 and 10.6 percent in FY 2011.



BLACK EMPLOYMENT BY OCCUPATIONAL CATEGORY

Black employment in professional occupations increased by 1,404, to 52,740 in FY 2012, from 51,336 in FY 2011. Blacks represented 10.7 percent of all Federal employees in this occupational category in FY 2012, compared to 10.6 percent in FY 2011.

Black employment in administrative occupations increased by 1,272 to 135,113 in FY 2012, from 133,841 in FY 2011. Blacks represented 18.4 percent of all Federal employees in this occupational category in FY 2012, compared to 18.3 percent in FY 2011.

2012	Black Employment	Percent of FW
Counts and Percentages of Blacks based on All Employees in Each Occupational Category (September 2012)		
Professional	52,740	10.7
Administrative	135,113	18.4
Technical	80,540	24.2
Clerical	33,242	27.4
Other	11,053	14.5
White-Collar (WC)	312,688	17.8
Blue-Collar (BC)	34,136	18.4
Total (WC + BC)	346,824	17.9

Black employment in technical occupations decreased by 389 to 80,540 in FY 2012, from 80,929 in FY 2011. Blacks represented 24.2 percent of all Federal employees in this occupational category in FY 2012, compared to 24 percent in FY 2011.

Black employment in clerical occupations decreased by 552 to 33,242 in FY 2012, from 33,794 in FY 2011. Blacks represented 27.4 percent of all Federal employees in this occupational category in FY 2012, compared to 27.3 percent in FY 2011.

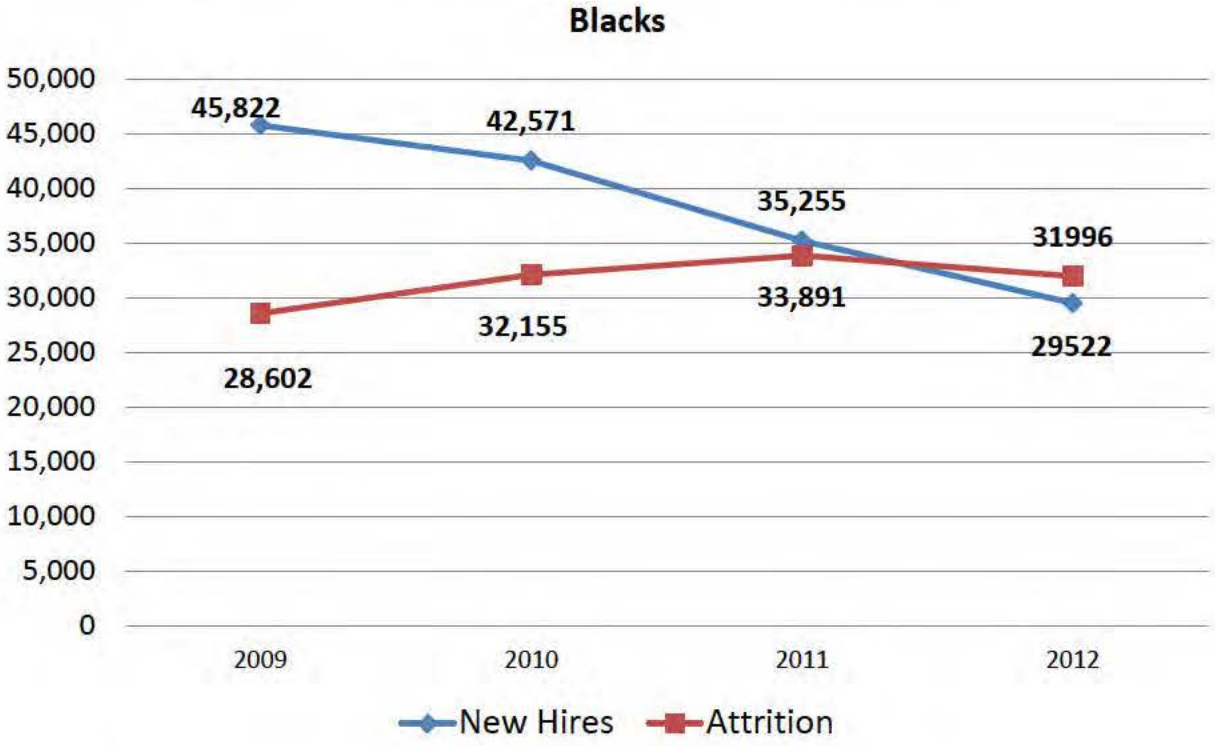
Black employment in "other" white-collar occupations decreased by 54 to 11,053 in FY 2012 from 11,107 in FY 2011. Blacks represented 14.5 percent of all Federal employees in this occupational category in FY 2012, compared to 14.4 in FY 2011.

Black employment in white-collar occupations increased by 1,681 to 312,688 in FY 2012 from 311,007 in FY 2011. Blacks represented 17.8 percent of all Federal employees in this occupational category in FY 2012, compared to 17.7 in FY 2011.

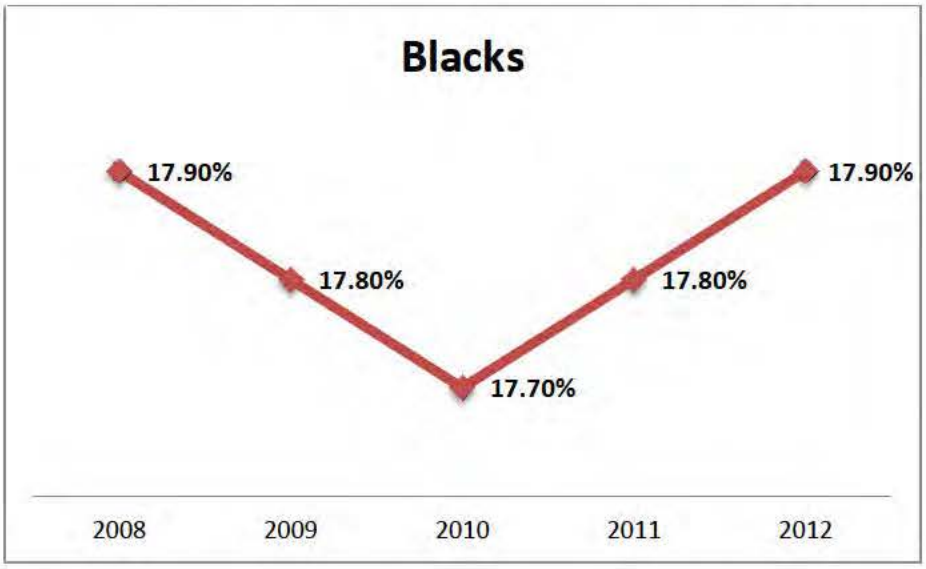
Black employment in blue-collar occupations decreased by 536, to 34,136 in FY 2012 from 34,672 in FY 2011. Blacks represented 18.4 percent of all Federal employees in this occupational category in FY 2012, as compared to 18.5 in FY 2011.

TRENDS

New Hires compared to Attrition Government-Wide[4]



Representation in the Federal Workforce over a 5-year period



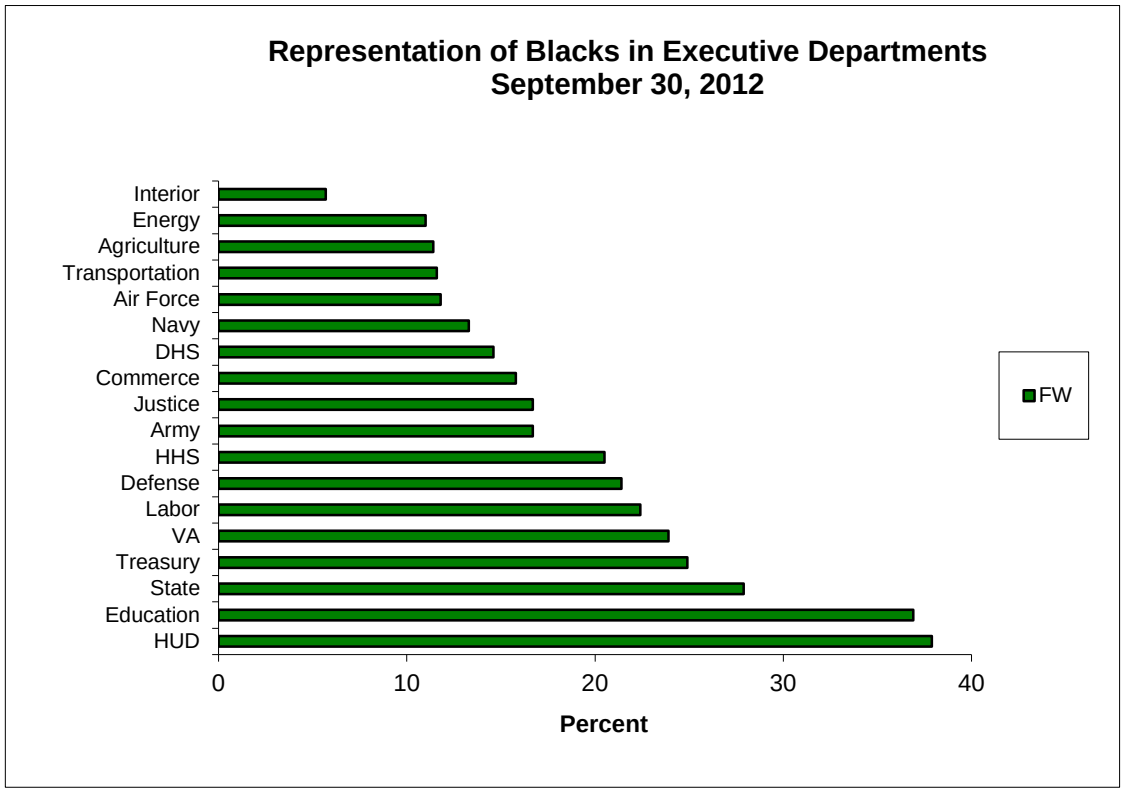
[4] The New Hires compared to Attrition chart does not include Transfers In, nor does it include Transfers Out. Furthermore, the Judicial Branch is entirely excluded and some Executive Branch agencies are not included. Please see data notes for details.

BLACK PERMANENT FEDERAL CIVILIAN EMPLOYMENT
SALARY TRENDS

WHITE-COLLAR / PAY SYSTEM GROUPS	2012		2011		DIFFERENCE 2011 TO 2012	
	#	%	#	%	#COUNT	%CHANGE
UP TO $20,000	0	0	0	0	0	0
$20,001 TO $40,000	36,216	2.6	37,347	2.7	-1,131	-3
$40,001 TO $60,000	84,849	6.1	86,485	6.2	-1,636	-1.9
$60,001 TO $80,000	61,045	4.4	59,442	4.3	1,603	2.7
$80,001 TO $100,000	43,037	3.1	41,313	3	1,724	4.2
$100,001 TO $120,000	25,486	1.8	24,539	1.8	947	3.9
$120,001 TO $140,000	9,377	0.7	8,915	0.6	462	5.2
$140,001 TO $160,000	3,940	0.3	3,713	0.3	227	6.1
$160,001 AND GREATER	105	0	122	0	-17	-13.9
UNSPECIFIED	244	0	281	0	-37	-13.2
TOTAL	264,299	18.9	262,157	18.8	2,142	0.8
SES						
$100,001 TO $120,000	5	0.1	4	0.1	1	25
$120,001 TO $140,000	27	0.3	27	0.3	0	0
$140,001 TO $160,000	238	3	216	2.8	22	10.2
$160,001 AND GREATER	546	6.9	528	6.8	18	3.4
UNSPECIFIED	0	0	0	0	0	0
TOTAL	816	10.4	775	10	41	5.3
OTHER WHITE COLLAR						
UP TO $20,000	60	0	50	0	10	20
$20,001 TO $40,000	8,780	2.5	9,050	2.6	-270	-3
$40,001 TO $60,000	7,668	2.2	7,980	2.3	-312	-3.9
$60,001 TO $80,000	10,323	3	10,645	3	-322	-3
$80,001 TO $100,000	8,171	2.3	8,208	2.3	-37	-0.5
$100,001 TO $120,000	5,596	1.6	5,553	1.6	43	0.8
$120,001 TO $140,000	2,822	0.8	2,689	0.8	133	4.9
$140,001 TO $160,000	2,086	0.6	2,024	0.6	62	3.1
$160,001 AND GREATER	2,058	0.6	1,869	0.5	189	10.1
UNSPECIFIED	9	0	7	0	2	28.6
TOTAL	47,573	13.6	48,075	13.6	-502	-1
TOTAL WHITE-COLLAR (PATCO)	312,688	17.8	311,007	17.7	1,681	0.5
TOTAL BLUE-COLLAR	34,136	18.4	34,672	18.5	-536	-1.5
TOTAL WHITE/BLUE-COLLAR	346,824	17.9	345,679	17.8	1,145	0.3

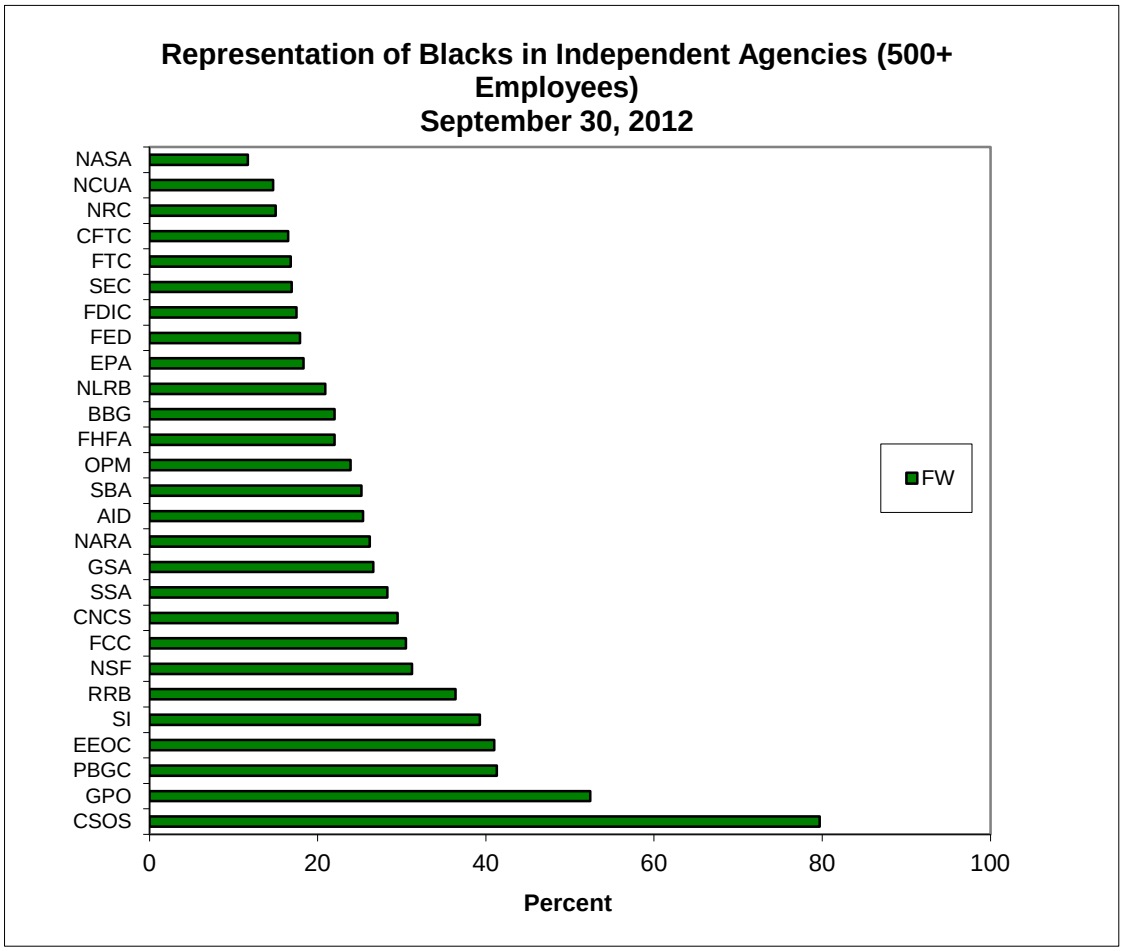
BLACKS REPRESENTATION IN EXECUTIVE DEPARTMENTS

REPRESENTATION IN PERMANENT FEDERAL WORKFORCE September 30, 2012 and September 30, 2011 BLACKS		
EXECUTIVE DEPARTMENTS	**2012 GROUP PCT.**	**2011 GROUP PCT**
DEPARTMENT OF THE AIR FORCE	11.8	11.8
DEPARTMENT OF AGRICULTURE	11.4	11.3
DEPARTMENT OF THE ARMY	16.7	16.7
DEPARTMENT OF COMMERCE	15.8	16
DEPARTMENT OF DEFENSE	21.4	21.4
DEPARTMENT OF JUSTICE	16.7	16.8
DEPARTMENT OF LABOR	22.4	22.4
DEPARTMENT OF ENERGY	11	11.1
DEPARTMENT OF EDUCATION	36.9	36.8
DEPARTMENT OF HEALTH AND HUMAN SERVICES	20.5	20.3
DEPARTMENT OF HOMELAND SECURITY	14.6	14.6
DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT	37.9	37.9
DEPARTMENT OF INTERIOR	5.7	5.7
DEPARTMENT OF THE NAVY	13.3	13.1
DEPARTMENT OF STATE	27.9	28.4
DEPARTMENT OF TRANSPORTATION	11.6	11.6
DEPARTMENT OF TREASURY	24.9	24.5
DEPARTMENT OF VETERANS AFFAIRS	23.9	23.8
GOVERNMENTWIDE	17.9	17.8


Representation of Blacks in Executive Departments
September 30, 2012
Interior
Energy
Agriculture
Transportation
Air Force
Navy
DHS
Commerce
Justice
Army
HHS
Defense
Labor
VA
Treasury
State
Education
HUD
0
10
20
30
40
Percent
FW

BLACKS REPRESENTATION IN INDEPENDENT AGENCIES

REPRESENTATION IN PERMANENT FEDERAL WORKFORCE September 30, 2012 and September 30, 2011 BLACKS		
INDEPENDENT AGENCIES	**2012 GROUP PCT.**	**2011 GROUP PCT.**
BROADCASTING BOARD OF GOVERNORS	22	22.4
COURT SERVICES AND OFFENDR SUPERVSN AGY	79.7	80.8
COMMODITY FUTURES TRADING COMMISSION	16.5	N/A
CORP FOR NATIONAL AND COMMUNITY SERVICE	29.5	30.6
ENVIRONMENTAL PROTECTION AGENCY	18.3	18.2
EQUAL EMPLOYMENT OPPORTUNITY COMMISSION	41	40.8
FEDERAL COMMUNICATIONS COMMISSION	30.5	31.3
FEDERAL DEPOSIT INSURANCE CORPORATION	17.5	17.6
FEDERAL HOUSING FINANCE AGENCY	22	N/A
FEDERAL RESERVE SYSTEM	17.9	N/A
FEDERAL TRADE COMMISSION	16.8	16.9
GENERAL SERVICES ADMINISTRATION	26.6	26.3
GOVERNMENT PRINTING OFFICE	52.4	53.6
NAT ARCHIVES AND RECORDS ADMINISTRATION	26.2	25.6
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	11.7	11.6
NATIONAL CREDIT UNION ADMINISTRATION	14.7	13.6
NATIONAL LABOR RELATIONS BOARD	20.9	21.5
NATIONAL SCIENCE FOUNDATION	31.2	31.7
NUCLEAR REGULATORY COMMISSION	15	15.1
OFFICE OF PERSONNEL MANAGEMENT	23.9	22.9
PENSION BENEFIT GUARANTY CORPORATION	41.3	41.6
RAILROAD RETIREMENT BOARD	36.4	34.8
SECURITIES AND EXCHANGE COMMISSION	16.9	17
SMALL BUSINESS ADMINISTRATION	25.2	25.2
SMITHSONIAN INSTITUTION	39.3	39.5
SOCIAL SECURITY ADMINISTRATION	28.3	28.4
US AID	25.4	25.7
GOVERMENTWIDE	17.9	17.8


Representation of Blacks in Independent Agencies (500+ Employees)
September 30, 2012
NASA
NCUA
NRC
CFTC
FTC
SEC
FDIC
FED
EPA
NLRB
BBG
FHFA
OPM
SBA
AID
NARA
GSA
SSA
CNCS
FCC
NSF
RRB
SI
EEOC
PBGC
GPO
CSOS
FW
0
20
40
60
80
100
Percent

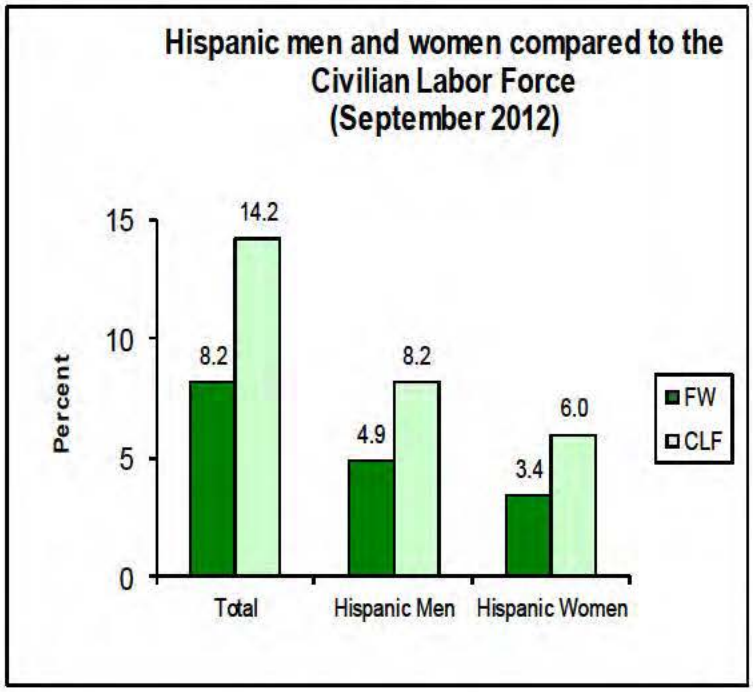
HISPANICS IN THE FEDERAL WORKFORCE

HISPANIC EMPLOYMENT

Hispanic employment represented 8.2 percent (159,639) of the permanent FW as of September 30, 2012 and 8.1 percent in FY 2011.

Hispanic men represented 4.9 percent of the permanent FW in FY 2012 and 4.8 percent in FY 2011.

Hispanic women represented 3.4 percent of the permanent FW in FY 2012 and 3.3 percent in FY 2011.



HISPANIC EMPLOYMENT BY OCCUPATIONAL CATEGORY

Hispanic employment in professional occupations increased by 839 to 25,746 in FY 2012 from 24,907 in FY 2011. Hispanics represented 5.2 percent of all Federal employees in this occupational category in FY 2012, compared to 5.1 in FY 2011.

Hispanic employment in administrative occupations increased by 1,080 to 59,736 in FY 2012 from 58,656 in FY 2011. Hispanics represented 8.1 percent of all Federal employees in this occupational category in FY 2012, compared to 8 percent in FY 2011.

Hispanic employment in technical occupations increased by 255 to 30,310 in FY 2012 from 30,055 in FY 2011. Hispanics represented 9.1 percent of all Federal employees in this occupational category in FY 2012, compared to 8.9 percent in FY 2011.

2012	Hispanic Employment	Percent of FW
Counts and Percentages of Hispanics based on All Employees in Each Occupational Category (September 2012		
Professional	25,746	5.2
Administrative	59,736	8.1
Technical	30,310	9.1
Clerical	13,608	11.2
Other	16,100	21.1
White-Collar (WC)	145,500	8.3
Blue-Collar (BC)	14,139	7.6
Total (WC + BC)	159,639	8.2

Hispanic employment in clerical occupations decreased by 29 to 13,608 in FY 2012 from 13,637 in FY 2011. Hispanics represented 11.2 percent of all Federal employees in this occupational category in FY 2012, compared to 11 percent in FY 2011.

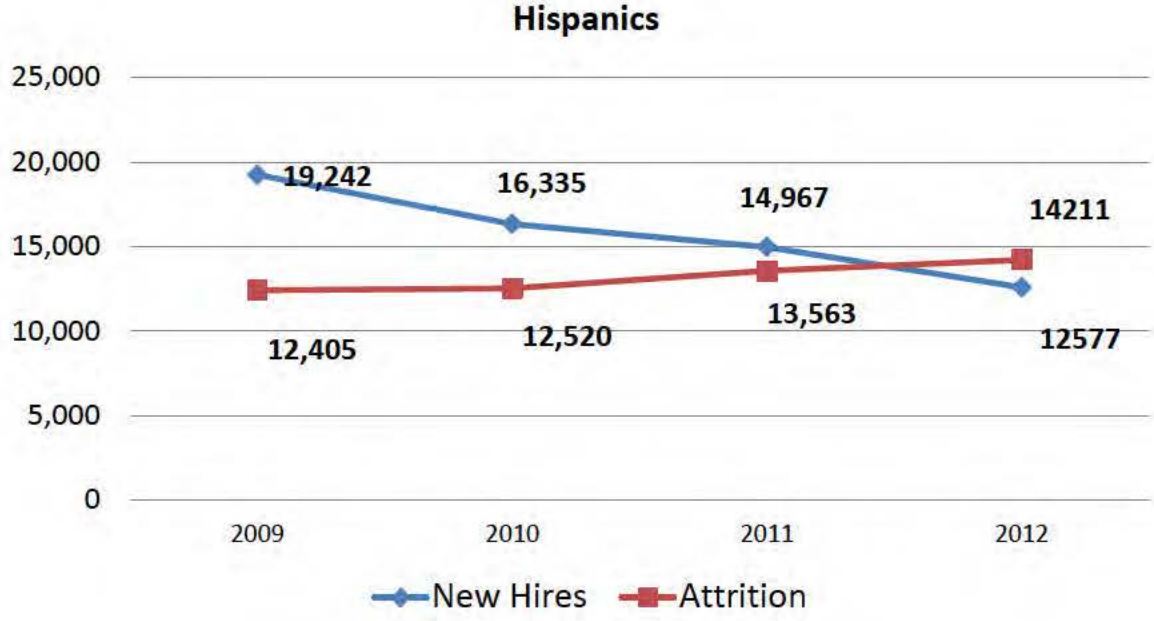
Hispanic employment in "other" white-collar occupations decreased by 25 to 16,100 in FY 2012 from 16,125 in FY 2011. Hispanics represented 21.1 percent of all Federal employees in this occupational category in FY 2012, compared to 20.8 in FY 2011.

Hispanic employment in white-collar occupations increased by 2,120 to 145,500 in FY 2012 from 143,380 in FY 2011. Hispanics represented 8.3 percent of all Federal employees in this occupational category in FY 2012, compared to 8.2 percent in FY 2011.

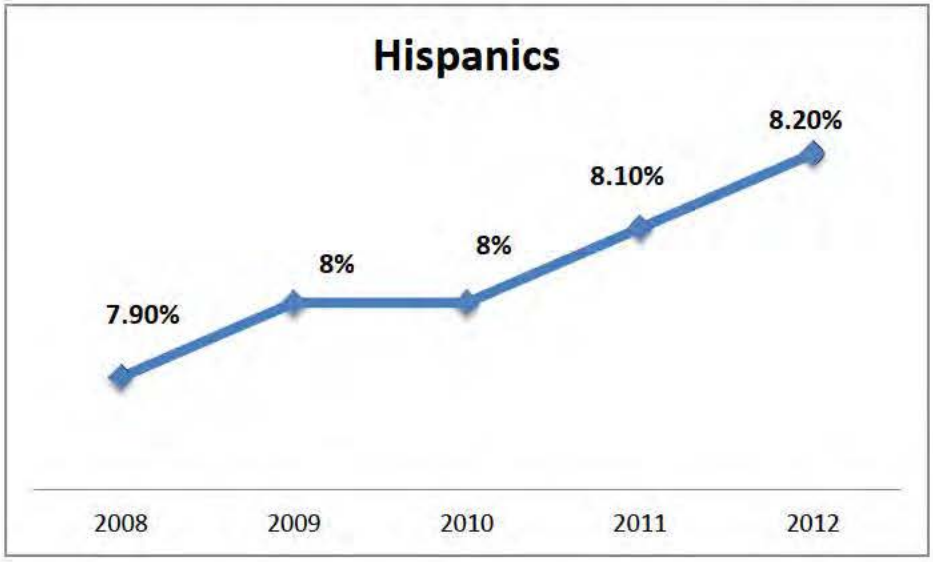
Hispanic employment in blue-collar occupations decreased by 129 to 14,139 in FY 2012 from 14,268 in FY 2011. Hispanics represented 7.6 percent of all Federal employees in this occupational category in FY 2012, same as in FY 2011.

TRENDS

New Hires compared to Attrition Government-Wide [5]



Representation in the Federal Workforce over a 5-year period



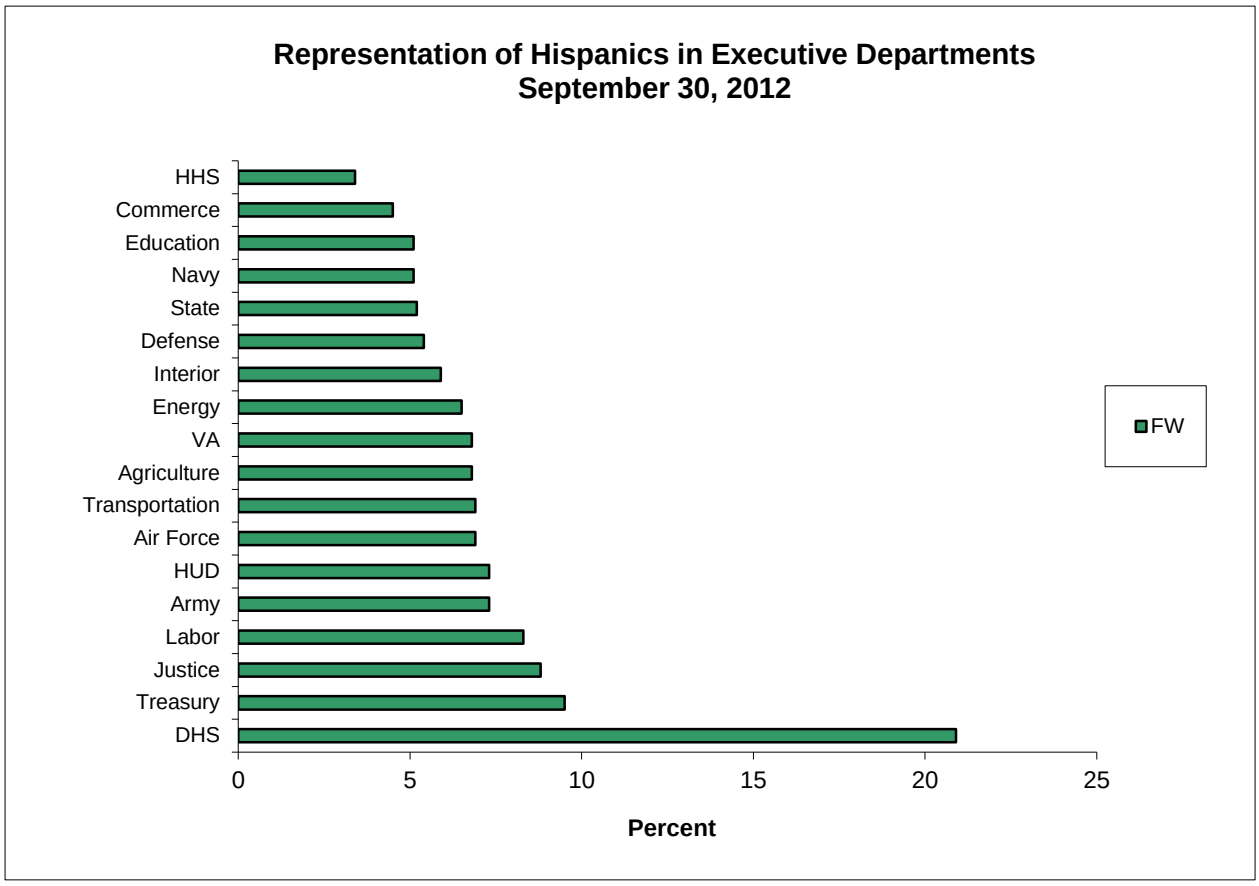
[5] The New Hires compared to Attrition chart does not include Transfers In, nor does it include Transfers Out. Furthermore, the Judicial Branch is entirely excluded and some Executive Branch agencies are not included. Please see data notes for details.

HISPANIC PERMANENT FEDERAL CIVILIAN EMPLOYMENT SALARY TRENDS

WHITE-COLLAR /z PAY SYSTEM GROUPS	2012		2011		DIFFERENCE 2011 TO 2012	
	#	%	#	%	#COUNT	%CHANGE
UP TO $20,000	0	0	1	0	-1	-100
$20,001 TO $40,000	12,347	0.9	13,226	0.9	-879	-6.6
$40,001 TO $60,000	33,683	2.4	35,618	2.6	-1,935	-5.4
$60,001 TO $80,000	35,696	2.6	33,754	2.4	1,942	5.8
$80,001 TO $100,000	21,681	1.5	19,940	1.4	1,741	8.7
$100,001 TO $120,000	9,850	0.7	9,233	0.7	617	6.7
$120,001 TO $140,000	3,133	0.2	2,905	0.2	228	7.8
$140,001 TO $160,000	1,473	0.1	1,390	0.1	83	6
$160,001 AND GREATER	55	0	57	0	-2	-3.5
UNSPECIFIED	76	0	98	0	-22	-22.4
TOTAL	117,994	8.4	116,222	8.3	1,772	1.5
SES						
$100,001 TO $120,000	1	0	0	0	1	0
$120,001 TO $140,000	11	0.1	12	0.2	-1	-8.3
$140,001 TO $160,000	89	1.1	86	1.1	3	3.5
$160,001 AND GREATER	223	2.8	219	2.8	4	1.8
UNSPECIFIED	0	0	0	0	0	0
TOTAL	324	4.1	317	4.1	7	2.2
OTHER WHITE COLLAR						
UP TO $20,000	26	0	35	0	-9	-25.7
$20,001 TO $40,000	7,034	2	7,051	2	-17	-0.2
$40,001 TO $60,000	4,221	1.2	4,262	1.2	-41	-1
$60,001 TO $80,000	4,591	1.3	4,645	1.3	-54	-1.2
$80,001 TO $100,000	3,715	1.1	3,626	1	89	2.5
$100,001 TO $120,000	2,838	0.8	2,830	0.8	8	0.3
$120,001 TO $140,000	1,692	0.5	1,542	0.4	150	9.7
$140,001 TO $160,000	1,222	0.3	1,180	0.3	42	3.6
$160,001 AND GREATER	1,838	0.5	1,666	0.5	172	10.3
UNSPECIFIED	5	0	4	0	1	25
TOTAL	27,182	7.8	26,841	7.6	341	1.3
TOTAL WHITE-COLLAR (PATCO)	145,500	8.3	143,380	8.2	2,120	1.5
TOTAL BLUE-COLLAR	14,139	7.6	14,268	7.6	-129	-0.9
TOTAL WHITE/BLUE-COLLAR	159,639	8.2	157,648	8.1	1,991	1.3

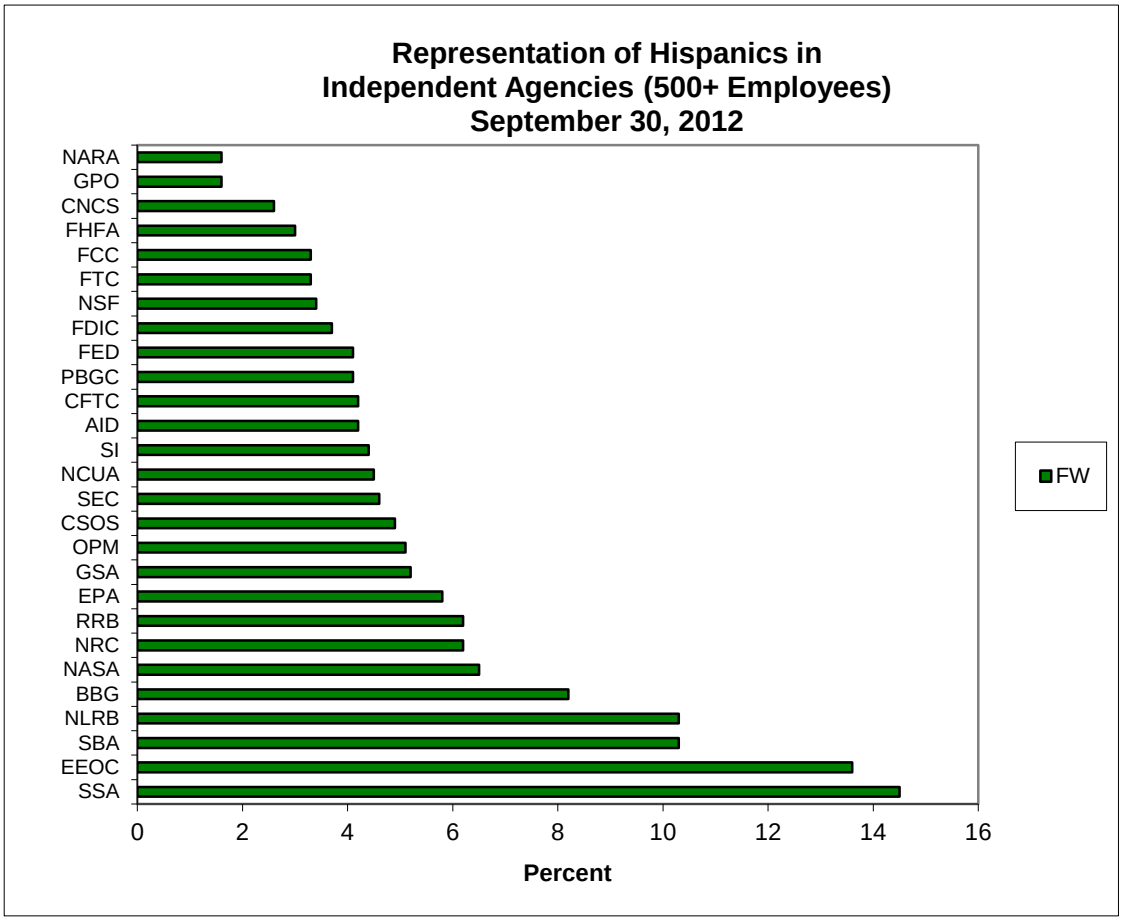
HISPANICS REPRESENTATION IN EXECUTIVE DEPARTMENTS

REPRESENTATION IN PERMANENT FEDERAL WORKFORCE September 30, 2012 and September 30, 2011 HISPANICS		
EXECUTIVE DEPARTMENTS	2012 GROUP PCT.	2011 GROUP PCT.
DEPARTMENT OF THE AIR FORCE	6.9	6.8
DEPARTMENT OF AGRICULTURE	6.8	6.4
DEPARTMENT OF THE ARMY	7.3	7.2
DEPARTMENT OF COMMERCE	4.5	4.2
DEPARTMENT OF DEFENSE	5.4	5.2
DEPARTMENT OF JUSTICE	8.8	8.7
DEPARTMENT OF LABOR	8.3	7.9
DEPARTMENT OF ENERGY	6.5	6.5
DEPARTMENT OF EDUCATION	5.1	5.1
DEPARTMENT OF HEALTH AND HUMAN SERVICES	3.4	3.2
DEPARTMENT OF HOMELAND SECURITY	20.9	21
DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT	7.3	7.1
DEPARTMENT OF INTERIOR	5.9	5.7
DEPARTMENT OF THE NAVY	5.1	4.9
DEPARTMENT OF STATE	5.2	5
DEPARTMENT OF TRANSPORTATION	6.9	6.8
DEPARTMENT OF TREASURY	9.5	9.1
DEPARTMENT OF VETERANS AFFAIRS	6.8	6.8
GOVERNMENTWIDE	8.2	8.1


Representation of Hispanics in Executive Departments
September 30, 2012
HHS
Commerce
Education
Navy
State
Defense
Interior
Energy
VA
Agriculture
Transportation
Air Force
HUD
Army
Labor
Justice
Treasury
DHS
0
5
10
15
20
25
Percent
FW

HISPANICS REPRESENTATION IN 27 INDEPENDENT AGENCIES

REPRESENTATION IN PERMANENT FEDERAL WORKFORCE September 30, 2012 and September 30, 2011 HISPANICS		
INDEPENDENT AGENCIES	**2012 GROUP PCT.**	**2011 GROUP PCT.**
BROADCASTING BOARD OF GOVERNORS	8.2	8.5
COMMODITY FUTURES TRADING COMMISSION	4.2	N/A
CORP FOR NATIONAL AND COMMUNITY SERVICE	2.6	2.7
COURT SERVICES AND OFFENDR SUPERVSN AGY	4.9	4.3
ENVIRONMENTAL PROTECTION AGENCY	5.8	5.8
EQUAL EMPLOYMENT OPPORTUNITY COMMISSION	13.6	13.4
FEDERAL COMMUNICATIONS COMMISSION	3.3	3.2
FEDERAL DEPOSIT INSURANCE CORPORATION	3.7	3.7
FEDERAL HOUSING FINANCE AGENCY	3	N/A
FEDERAL RESERVE SYSTEM	4.1	N/A
FEDERAL TRADE COMMISSION	3.3	3.7
GENERAL SERVICES ADMINISTRATION	5.2	5.2
GOVERNMENT PRINTING OFFICE	1.6	1.5
NAT ARCHIVES AND RECORDS ADMINISTRATION	1.6	1.6
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	6.5	6.2
NATIONAL CREDIT UNION ADMINISTRATION	4.5	4.1
NATIONAL LABOR RELATIONS BOARD	10.3	9.7
NATIONAL SCIENCE FOUNDATION	3.4	2.9
NUCLEAR REGULATORY COMMISSION	6.2	6
OFFICE OF PERSONNEL MANAGEMENT	5.1	4.7
PENSION BENEFIT GUARANTY CORPORATION	4.1	3.8
RAILROAD RETIREMENT BOARD	6.2	5.8
SECURITIES AND EXCHANGE COMMISSION	4.6	4.8
SMALL BUSINESS ADMINISTRATION	10.3	10.1
SMITHSONIAN INSTITUTION	4.4	4.4
SOCIAL SECURITY ADMINISTRATION	14.5	14.3
US AID	4.2	3.3
GOVERMENTWIDE	8.2	8.1


Representation of Hispanics in
Independent Agencies (500+ Employees)
September 30, 2012
NARA
GPO
CNCS
FHFA
FCC
FTC
NSF
FDIC
FED
PBGC
CFTC
AID
SI
NCUA
SEC
CSOS
OPM
GSA
EPA
RRB
NRC
NASA
BBG
NLRB
SBA
EEOC
SSA
0
2
4
6
8
10
12
14
16
Percent
FW

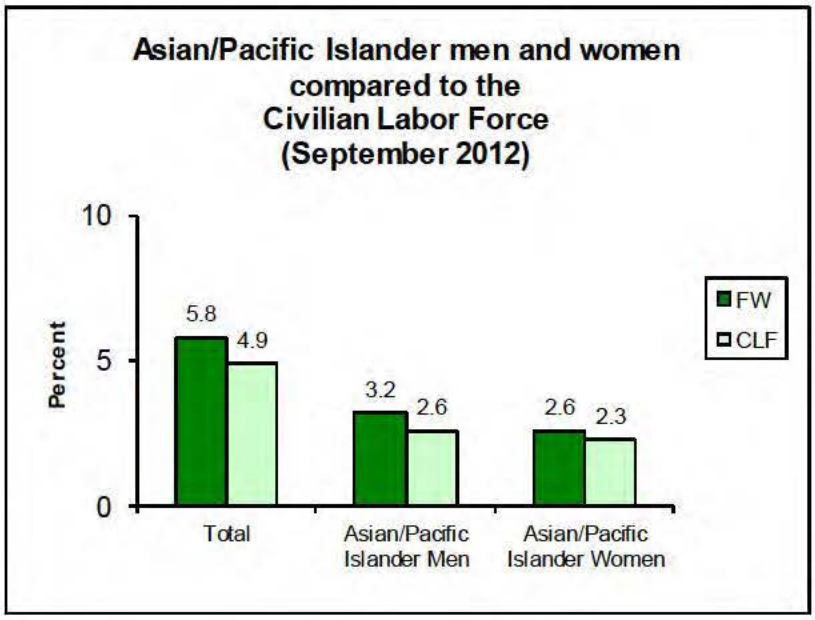
ASIAN/PACIFIC ISLANDERS IN THE FEDERAL WORKFORCE

ASIAN/PACIFIC ISLANDER EMPLOYMENT

Asian/Pacific Islander employees represented 5.8 percent (112,261) of the permanent FW as of September 30, 2012 and 5.6 percent in FY 2011.

Asian/Pacific Islander men represented 3.2 percent of the FW in FY 2012 and 3.1 percent in FY 2011.

Asian/Pacific Islander women represented 2.6 percent of the FW in FY 2012 and 2.6 percent in FY 2011.



ASIAN/PACIFIC ISLANDER EMPLOYMENT BY OCCUPATIONAL CATEGORY

Asian/Pacific Islander employment in professional occupations increased by

1,426 to 45,462 in FY 2012, from 44,036 in FY 2011. Asian/Pacific Islanders represented 9.2 percent of all Federal employees in this occupational category in FY 2012, compared to 9.1 percent in FY 2011.

2012	Asian/Pacific Islander Employment	Percent of FW
Counts and Percentages of Asian/Pacific Islanders based on All Employees in Each Occupational Category (September 2012)		
Professional	45,462	9.2
Administrative	33,541	4.6
Technical	14,867	4.5
Clerical	5,950	4.9
Other	2,118	2.8
White-Collar (WC)	101,938	5.8
Blue-Collar (BC)	10,323	5.6
Total (WC + BC)	112,261	5.8

Asian/Pacific Islander employment in administrative occupations increased by 935 to 33,541 in FY 2012 from 32,606 in FY 2011. Asian/Pacific Islanders represented 4.6 percent of Federal employees in this occupational category in FY 2012, compared to 4.5 percent in FY 2011.

Asian/Pacific Islander employment in technical occupations increased by 37 to 14,867 in FY 2012 from 14,830 in FY 2011. Asian/Pacific Islanders represented 4.5 percent of all Federal employees in this occupational category in FY 2012, compared to4.4 in FY 2011.

Asian/Pacific Islander employment in clerical occupations decreased by 64 to 5,950 in FY 2012 from 6,014 in FY 2011. Asian/Pacific Islanders represented 4.9 percent of all Federal employees in this occupational category in FY 2012, same as in FY 2011.

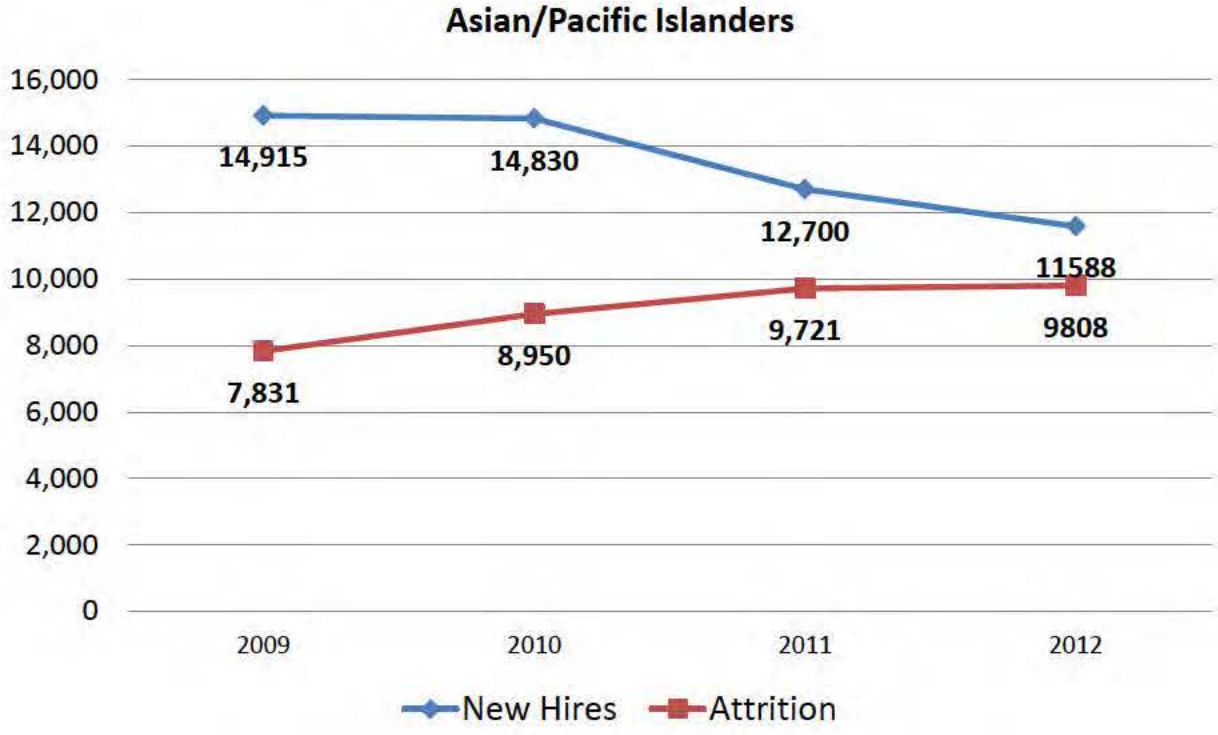
Asian/Pacific Islander employment in "other" white-collar occupations increased by 52 to 2,118 in 2012 from 2,066 in 2011. Asian/Pacific Islanders represented 2.8 percent of all Federal employees in this occupational category in FY 2012, compared to 2.7 in FY 2011.

Asian/Pacific Islander employment in white-collar occupations increased by 2.386 to 101,938 in FY 2012 from 99,552 in FY 2011. Asian/Pacific Islanders represented 5.8 percent of all Federal employees in this occupational category in FY 2012, compared to 5.7 in FY 2011.

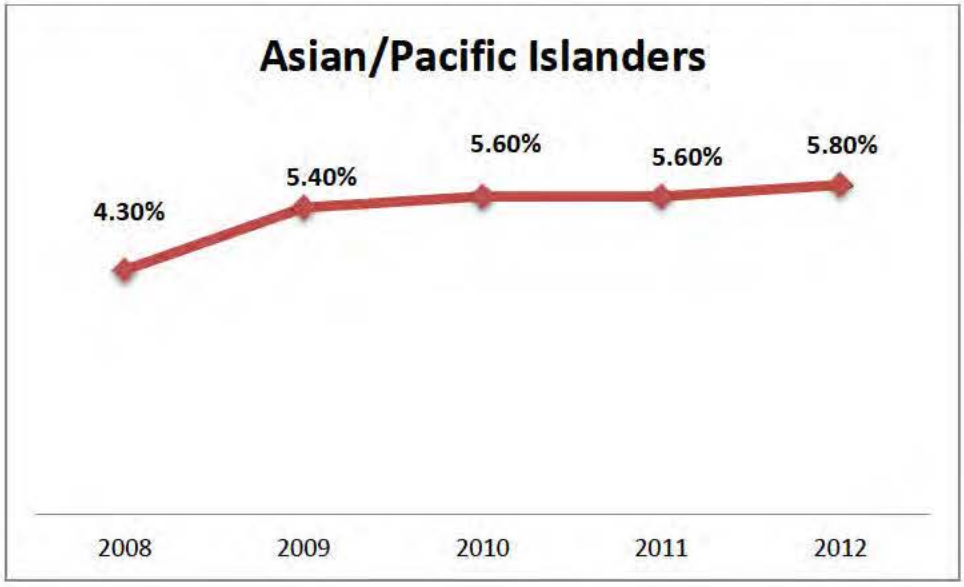
Asian/Pacific Islander employment in blue-collar occupations increased by 4 to 10,323 in FY 2012 from 10,319 in FY 2011. Asian/Pacific Islanders represented 5.6 percent of all Federal employees in this occupational category in FY 2012, compared to 5.5 in FY 2011.

TRENDS

New Hires compared to Attrition[6]



Representation in the Federal Workforce over a 5-year period



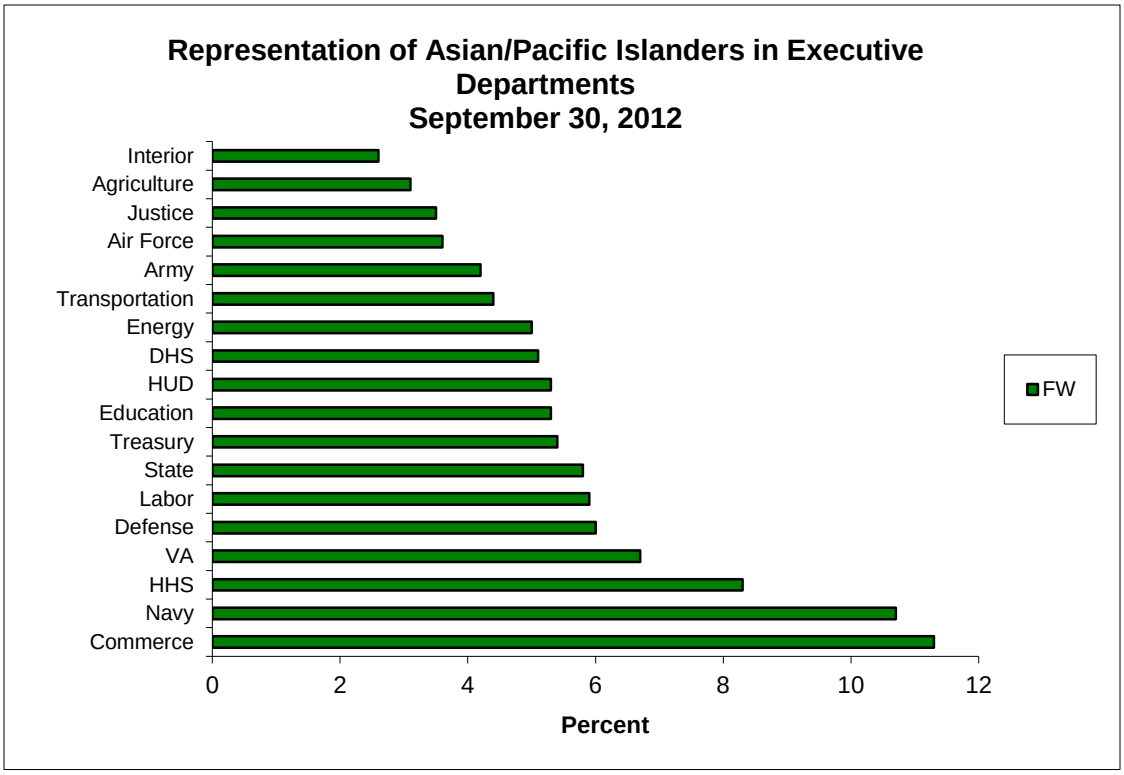
[6] The New Hires compared to Attrition chart does not include Transfers In, nor does it include Transfers Out. Furthermore, the Judicial Branch is entirely excluded and some Executive Branch agencies are not included. Please see data notes for details.

ASIAN/PACIFIC ISLANDER PERMANENT FEDERAL CIVILIAN EMPLOYMENT SALARY TRENDS

WHITE-COLLAR / PAY SYSTEM GROUPS GS,GM,GL	2012		2011		DIFFERENCE 2011 TO 2012	
	#	%	#	%	#COUNT	%CHANGE
UP TO $20,000	0	0	1	0	-1	-100
$20,001 TO $40,000	6,518	0.5	7,034	0.5	-516	-7.3
$40,001 TO $60,000	15,725	1.1	16,425	1.2	-700	-4.3
$60,001 TO $80,000	17,033	1.2	16,356	1.2	677	4.1
$80,001 TO $100,000	16,567	1.2	15,438	1.1	1,129	7.3
$100,001 TO $120,000	12,052	0.9	11,130	0.8	922	8.3
$120,001 TO $140,000	5,496	0.4	5,067	0.4	429	8.5
$140,001 TO $160,000	2,410	0.2	2,207	0.2	203	9.2
$160,001 AND GREATER	54	0	81	0	-27	-33.3
UNSPECIFIED	34	0	46	0	-12	-26.1
TOTAL	75,889	5.4	73,785	5.3	2,104	2.9
SES						
$120,001 TO $140,000	15	0.2	10	0.1	5	50
$140,001 TO $160,000	53	0.7	50	0.6	3	6
$160,001 AND GREATER	189	2.4	188	2.4	1	0.5
UNSPECIFIED	0	0	0	0	0	0
TOTAL	257	3.3	248	3.2	9	3.6
OTHER WHITE COLLAR						
UP TO $20,000	2	0	4	0	-2	-50
$20,001 TO $40,000	1,866	0.5	1,918	0.5	-52	-2.7
$40,001 TO $60,000	2,069	0.6	2,136	0.6	-67	-3.1
$60,001 TO $80,000	3,539	1	3,699	1	-160	-4.3
$80,001 TO $100,000	4,886	1.4	4,982	1.4	-96	-1.9
$100,001 TO $120,000	4,536	1.3	4,505	1.3	31	0.7
$120,001 TO $140,000	2,100	0.6	2,044	0.6	56	2.7
$140,001 TO $160,000	1,894	0.5	1,860	0.5	34	1.8
$160,001 AND GREATER	4,900	1.4	4,368	1.2	532	12.2
UNSPECIFIED	0	0	3	0	-3	-100
TOTAL	25,792	7.4	25,519	7.2	273	1.1
TOTAL WHITE-COLLAR (PATCO)	101,938	5.8	99,552	5.7	2,386	2.4
TOTAL BLUE-COLLAR	10,323	5.6	10,319	5.5	4	0
TOTAL WHITE/BLUE-COLLAR	112,261	5.8	109,871	5.6	2,390	2.2

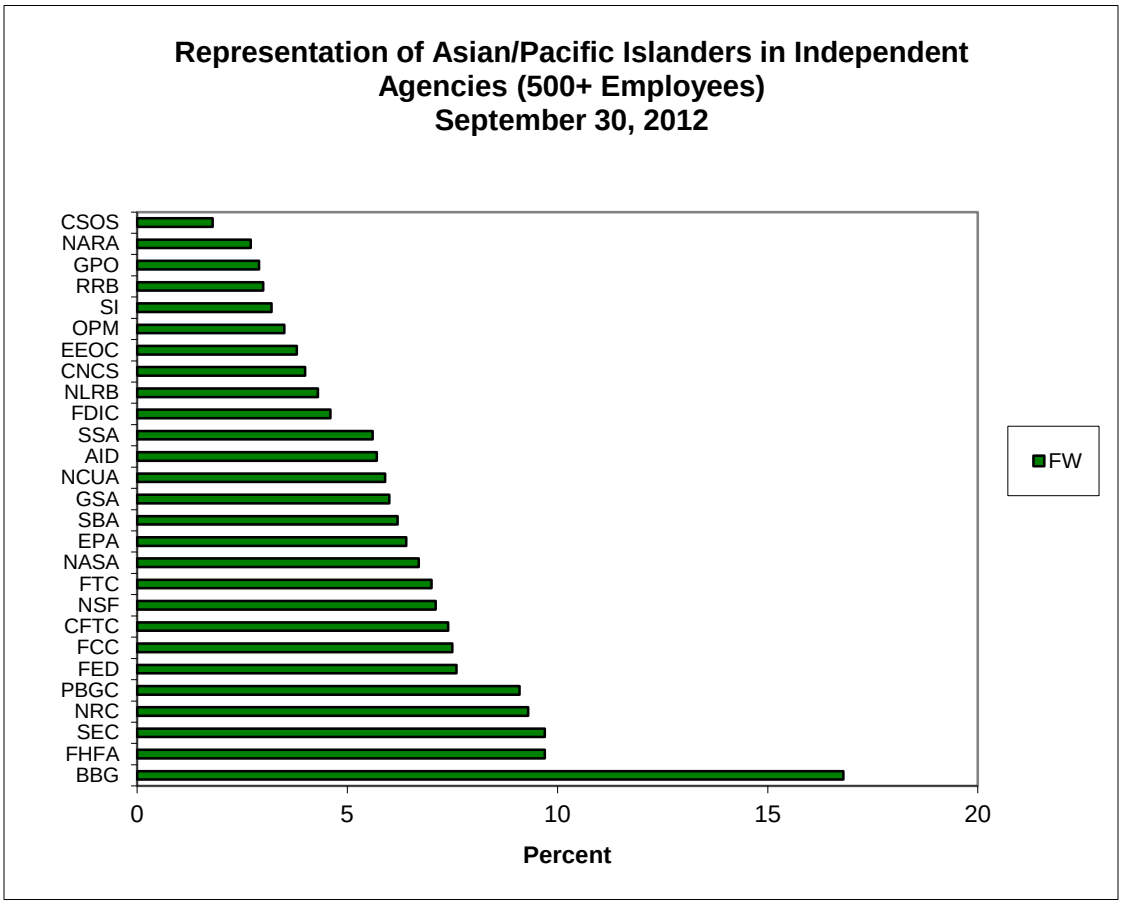
ASIAN/PACIFIC ISLANDERS REPRESENTATION IN EXECUTIVE DEPARTMENTS

REPRESENTATION IN PERMANENT FEDERAL WORKFORCE September 30, 2012 and September 30, 2011 ASIANS		
EXECUTIVE DEPARTMENTS	**2012 GROUP PCT.**	**2011 GROUP PCT.**
DEPARTMENT OF THE AIR FORCE	3.6	3.6
DEPARTMENT OF AGRICULTURE	3.1	3
DEPARTMENT OF THE ARMY	4.2	4.2
DEPARTMENT OF COMMERCE	11.3	10.6
DEPARTMENT OF DEFENSE	6	5.9
DEPARTMENT OF JUSTICE	3.5	3.4
DEPARTMENT OF LABOR	5.9	5.6
DEPARTMENT OF ENERGY	5	4.9
DEPARTMENT OF EDUCATION	5.3	5.4
DEPARTMENT OF HEALTH AND HUMAN SERVICES	8.3	8
DEPARTMENT OF HOMELAND SECURITY	5.1	5
DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT	5.3	5.3
DEPARTMENT OF INTERIOR	2.6	2.5
DEPARTMENT OF THE NAVY	10.7	10.7
DEPARTMENT OF STATE	5.8	5.2
DEPARTMENT OF TRANSPORTATION	4.4	4.4
DEPARTMENT OF TREASURY	5.4	5.3
DEPARTMENT OF VETERANS AFFAIRS	6.7	6.6
GOVERNMENTWIDE	5.8	5.6


Representation of Asian/Pacific Islanders in Executive Departments
September 30, 2012
Interior
Agriculture
Justice
Air Force
Army
Transportation
Energy
DHS
HUD
Education
Treasury
State
Labor
Defense
VA
HHS
Navy
Commerce
0
2
4
6
8
10
12
Percent
FW

ASIAN/PACIFIC ISLANDERS REPRESENTATION IN 27 INDEPENDENT AGENCIES

REPRESENTATION IN PERMANENT FEDERAL WORKFORCE September 30, 2012 and September 30, 2011 ASIANS		
INDEPENDENT AGENCIES	**2012 GROUP PCT.**	**2011 GROUP CT.**
BROADCASTING BOARD OF GOVERNORS	16.8	15.4
COMMODITY FUTURES TRADING COMMISSION	7.4	N/A
CORP FOR NATIONAL AND COMMUNITY SERVICE	4	4.2
COURT SERVICES AND OFFENDR SUPERVSN AGY	1.8	1.5
ENVIRONMENTAL PROTECTION AGENCY	6.4	6.5
EQUAL EMPLOYMENT OPPORTUNITY COMMISSION	3.8	3.8
FEDERAL COMMUNICATIONS COMMISSION	7.5	7.1
FEDERAL DEPOSIT INSURANCE CORPORATION	4.6	4.1
FEDERAL HOUSING FINANCE AGENCY	9.7	N/A
FEDERAL RESERVE SYSTEM	7.6	N/A
FEDERAL TRADE COMMISSION	7	6.5
GENERAL SERVICES ADMINISTRATION	6	5.8
GOVERNMENT PRINTING OFFICE	2.9	2.6
NAT ARCHIVES AND RECORDS ADMINISTRATION	2.7	2.6
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	6.7	6.5
NATIONAL CREDIT UNION ADMINISTRATION	5.9	5.2
NATIONAL LABOR RELATIONS BOARD	4.3	4.2
NATIONAL SCIENCE FOUNDATION	7.1	7.1
NUCLEAR REGULATORY COMMISSION	9.3	9.1
OFFICE OF PERSONNEL MANAGEMENT	3.5	3.3
PENSION BENEFIT GUARANTY CORPORATION	9.1	9.1
RAILROAD RETIREMENT BOARD	3	2.7
SECURITIES AND EXCHANGE COMMISSION	9.7	9.2
SMALL BUSINESS ADMINISTRATION	6.2	5.9
SMITHSONIAN INSTITUTION	3.2	3.1
SOCIAL SECURITY ADMINISTRATION	5.6	5.4
US AID	5.7	6
GOVERMENTWIDE	5.8	5.6


Representation of Asian/Pacific Islanders in Independent Agencies (500+ Employees)
September 30, 2012
CSOS
NARA
GPO
RRB
SI
OPM
EEOC
CNCS
NLRB
FDIC
SSA
AID
NCUA
GSA
SBA
EPA
NASA
FTC
NSF
CFTC
FCC
FED
PBGC
NRC
SEC
FHFA
BBG
0
5
10
15
20
Percent
FW

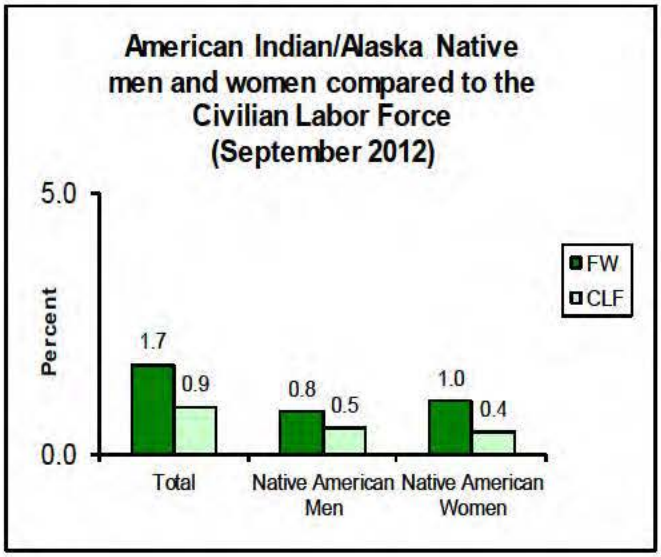
AMERICAN INDIAN/ALASKA NATIVES IN THE FEDERAL WORKFORCE

AMERICAN INDIAN/ALASKA NATIVE EMPLOYMENT

American Indian/Alaska Native employment represented 1.7 percent (33,171) of the permanent FW as of September 30, 2012 and 1.7 percent in FY 2011.

American Indian/Alaska Native men represented 0.8 percent of the FW in FY 2012 and 0.8 in FY 2011.

American Indian/Alaska Native women represented 1.0 percent of the FW in FY 2012 and 1.0 percent in FY 2011.



AMERICAN INDIAN/ALASKA NATIVE EMPLOYMENT BY OCCUPATIONAL CATEGORY

American Indian/Alaska Native employment in professional occupations increased by 35 to 5,946 in FY 2012 from 5,911 in FY 2011. American Indian/Alaska Natives represented 1.2 percent of all Federal employees in this occupational category in FY 2012, the same as in FY 2011.

American Indian/Alaska Native employment in administrative occupations decreased by 142 to 9,126 in FY 2012 from 9,268 in FY 2011. American Indian/Alaska Natives represented 1.2 percent of all Federal employees in this occupational category in FY 2012, compared to 1.3 in FY 2011.

2012	American Indian/ Alaska Native Employment	Percent of FW
Counts and Percentages of American Insian/Alaska Native based on All Employees in Each Occupational Category (September 2012)		
Professional	5,946	1.2
Administrative	9,126	1.2
Technical	9,420	2.8
Clerical	3,330	2.7
Other	1,226	1.6
White-Collar (WC)	29,048	1.7
Blue-Collar (BC)	4,123	2.2
Total (WC + BC)	33,171	1.7

American Indian/Alaska Native employment in technical occupations decreased by 180 to 9,420 in FY 2012 from 9,600 in FY 2011. American Indian/Alaska Natives represented 2.8 percent of all Federal employees in this occupational category in FY 2012, the same as in FY 2011.

American Indian/Alaska Native employment in clerical occupations decreased by 156 to 3,330 in FY 2012 from 3,486 in FY 2011. American Indian/Alaska Natives represented 2.7 percent of all employees in this occupational category in FY 2012, compared to 2.8 percent in FY 2011.

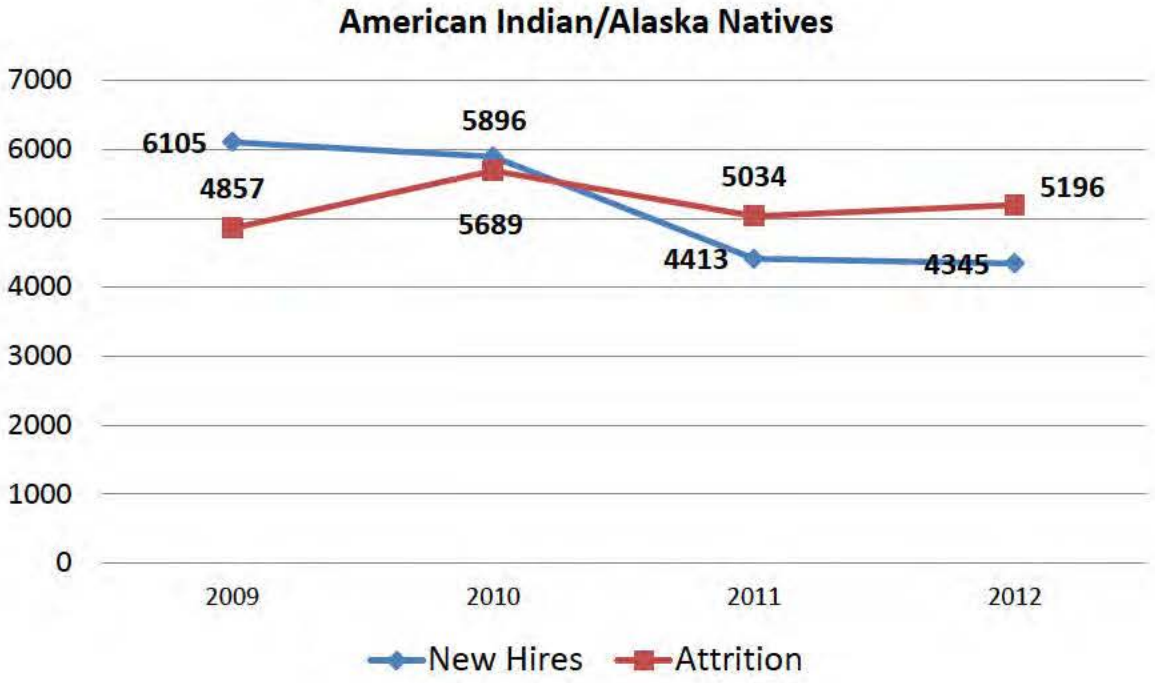
American Indian/Alaska Native employment in "other" white-collar occupations decreased by 32 to 1,226 in FY 2012 from 1,258 in FY 2011. American Indian/Alaska Natives represented 1.6 percent of this occupational category in FY 2012, the same as in FY 2011.

American Indian/Alaska Native employment in white-collar occupations decreased by 475 to 29,048 in FY 2012 from 29,523 in FY 2011. American Indian/Alaska Natives represented 1.7 percent of this occupational category in FY 2012, the same as in FY 2011.

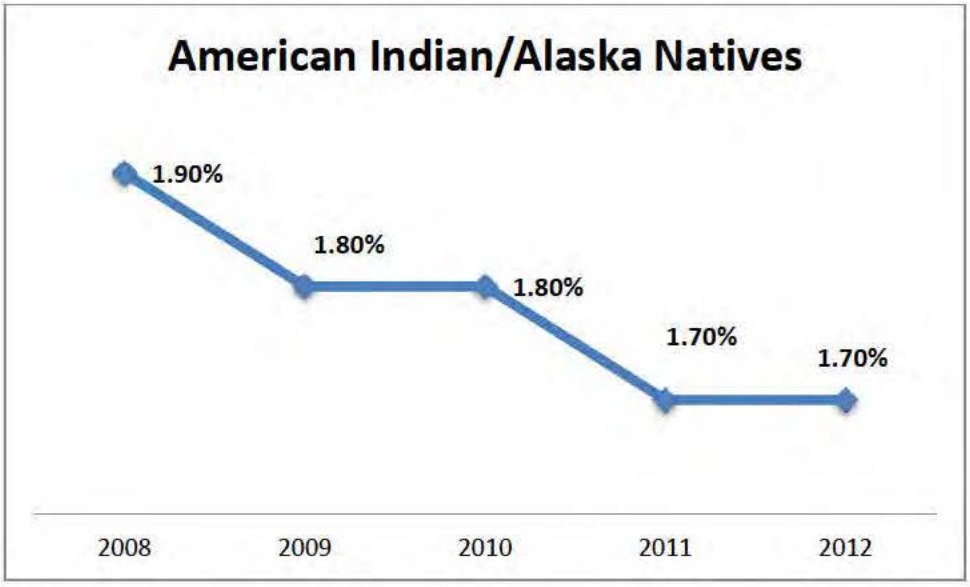
American Indian/Alaska Native employment in blue-collar occupations decreased by 115 to 4,123 in FY 2012 from 4,238 in FY 2011. American Indian/Alaska Natives represented 2.2 percent of this occupational category in FY 2012, compared to 2.3 percent in FY 2011.

TRENDS

New Hires compared to Attrition[7]



Representation in the Federal Workforce over a 5-year period



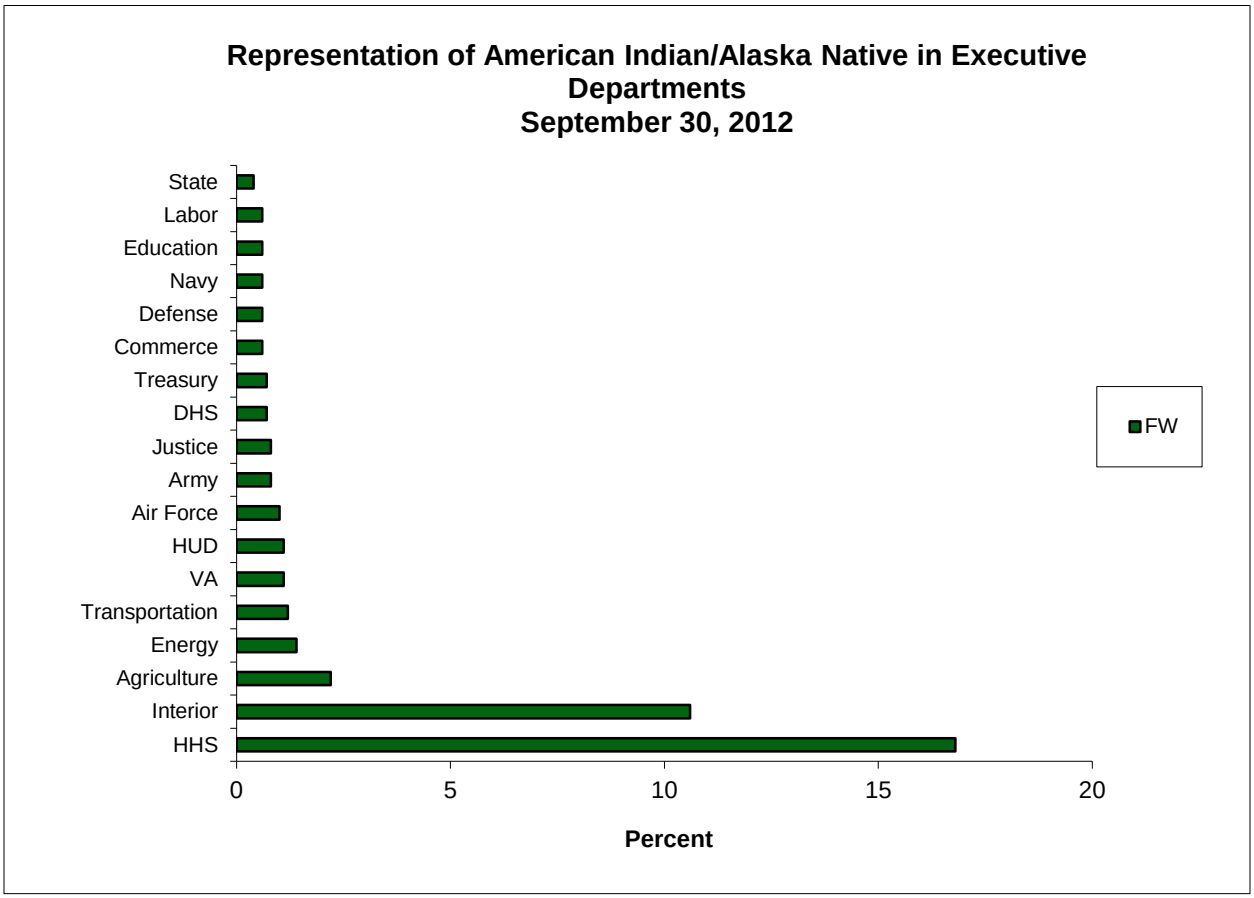
[7] The New Hires compared to Attrition chart does not include Transfers In, nor does it include Transfers Out. Furthermore, the Judicial Branch is entirely excluded and some Executive Branch agencies are not included. Please see data notes for details.

AMERICAN INDIAN/ALASKA NATIVE PERMANENT FEDERAL CIVILIAN EMPLOYMENT SALARY TRENDS

WHITE-COLLAR / PAY SYSTEM GROUPS GS,GM,GL	2012		2011		DIFFERENCE 2011 TO 2012	
	#	%	#	%	#COUNT	%CHANGE
UP TO $20,000	0	0	0	0	0	0
$20,001 TO $40,000	5,941	0.4	6,195	0.4	-254	-4.1
$40,001 TO $60,000	8,853	0.6	9,070	0.6	-217	-2.4
$60,001 TO $80,000	5,432	0.4	5,434	0.4	-2	0
$80,001 TO $100,000	3,258	0.2	3,179	0.2	79	2.5
$100,001 TO $120,000	1,527	0.1	1,497	0.1	30	2
$120,001 TO $140,000	578	0	584	0	-6	-1
$140,001 TO $160,000	222	0	226	0	-4	-1.8
$160,001 AND GREATER	9	0	14	0	-5	-35.7
UNSPECIFIED	41	0	50	0	-9	-18
TOTAL	25,861	1.8	26,249	1.9	-388	-1.5
SES						
$100,001 TO $120,000	2	0	2	0	0	0
$120,001 TO $140,000	5	0.1	5	0.1	0	0
$140,001 TO $160,000	25	0.3	22	0.3	3	13.6
$160,001 AND GREATER	57	0.7	59	0.8	-2	-3.4
TOTAL	89	1.1	88	1.1	1	1.1
OTHER WHITE COLLAR						
UP TO $20,000	2	0	4	0	-2	-50
$20,001 TO $40,000	331	0.1	404	0.1	-73	-18.1
$40,001 TO $60,000	418	0.1	423	0.1	-5	-1.2
$60,001 TO $80,000	570	0.2	583	0.2	-13	-2.2
$80,001 TO $100,000	518	0.1	528	0.1	-10	-1.9
$100,001 TO $120,000	411	0.1	421	0.1	-10	-2.4
$120,001 TO $140,000	237	0.1	231	0.1	6	2.6
$140,001 TO $160,000	235	0.1	248	0.1	-13	-5.2
$160,001 AND GREATER	376	0.1	344	0.1	32	9.3
TOTAL	3,098	0.9	3,186	0.9	-88	-2.8
TOTAL WHITE-COLLAR (PATCO)	29,048	1.7	29,523	1.7	-475	-1.6
TOTAL BLUE-COLLAR	4,123	2.2	4,238	2.3	-115	-2.7
TOTAL WHITE/BLUE-COLLAR	33,171	1.7	33,761	1.7	-590	-1.7

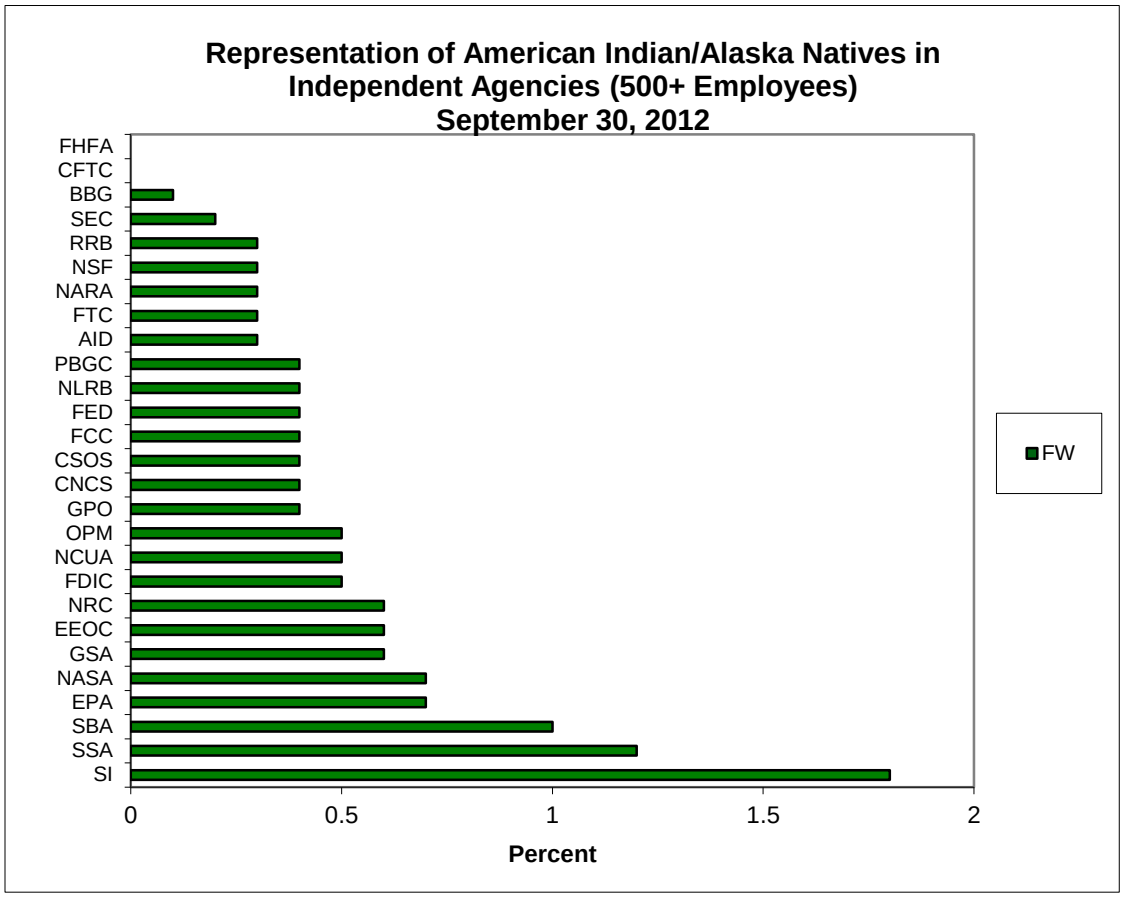
AMERICAN INDIAN/ALASKA NATIVES REPRESENTATION IN EXECUTIVE DEPARTMENTS

REPRESENTATION IN PERMANENT FEDERAL WORKFORCE September 30, 2012 and September 30, 2011 AMERICAN INDIAN/ALASKA NATIVES		
EXECUTIVE DEPARTMENTS	**2012 GROUP PCT.**	**2011 GROUP PCT.**
DEPARTMENT OF THE AIR FORCE	1	1
DEPARTMENT OF AGRICULTURE	2.2	2.2
DEPARTMENT OF THE ARMY	0.8	0.9
DEPARTMENT OF COMMERCE	0.6	0.6
DEPARTMENT OF DEFENSE	0.6	0.6
DEPARTMENT OF JUSTICE	0.8	0.8
DEPARTMENT OF LABOR	0.6	0.6
DEPARTMENT OF ENERGY	1.4	1.3
DEPARTMENT OF EDUCATION	0.6	0.6
DEPARTMENT OF HEALTH AND HUMAN SERVICES	16.8	17.2
DEPARTMENT OF HOMELAND SECURITY	0.7	0.7
DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT	1.1	1.1
DEPARTMENT OF INTERIOR	10.6	10.9
DEPARTMENT OF THE NAVY	0.6	0.6
DEPARTMENT OF STATE	0.4	0.4
DEPARTMENT OF TRANSPORTATION	1.2	1.2
DEPARTMENT OF TREASURY	0.7	0.7
DEPARTMENT OF VETERANS AFFAIRS	1.1	1.1
GOVERNMENTWIDE	1.7	1.7


Representation of American Indian/Alaska Native in Executive Departments
September 30, 2012
State
Labor
Education
Navy
Defense
Commerce
Treasury
DHS
Justice
Army
Air Force
HUD
VA
Transportation
Energy
Agriculture
Interior
HHS
0
5
10
15
20
Percent
FW

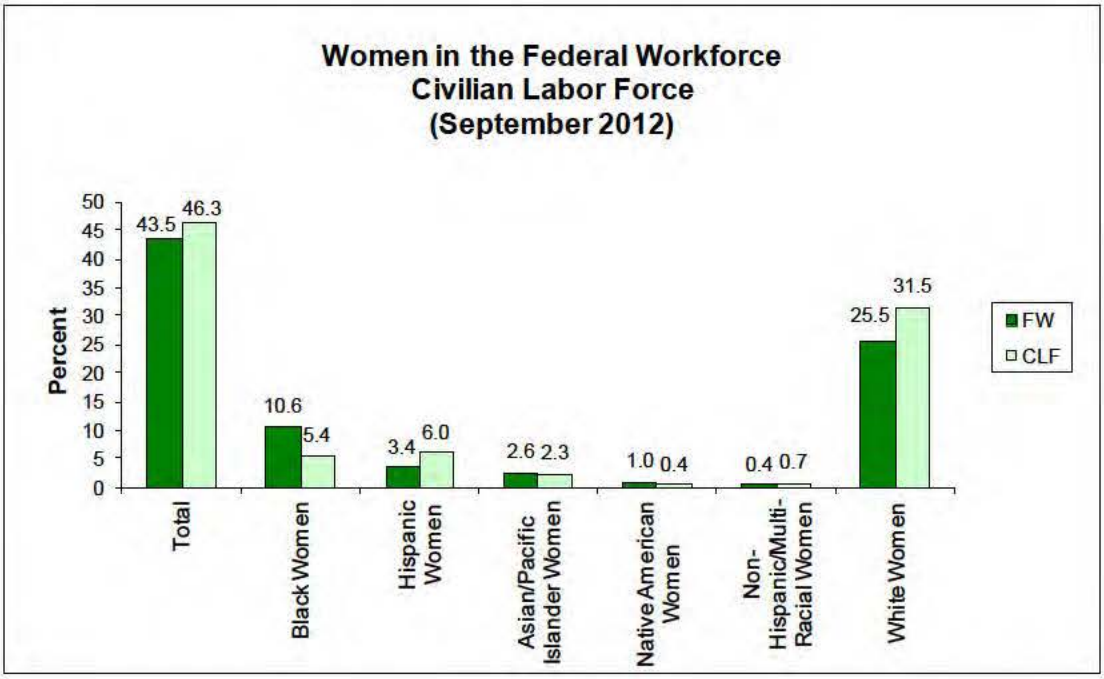
AMERICAN INDIAN/ALASKA NATIVES REPRESENTATION IN 27 INDEPENDENT AGENCIES

REPRESENTATION IN PERMANENT FEDERAL WORKFORCE September 30, 2012 and September 30, 2011 AMERICAN INDIAN/ALASKA NATIVES		
INDEPENDENT AGENCIES	**2012 GROUP PCT.**	**2011 GROUP PCT.**
BROADCASTING BOARD OF GOVERNORS	0.1	0.2
COMMODITY FUTURES TRADING COMMISSION	0	N/A
CORP FOR NATIONAL AND COMMUNITY SERVICE	0.4	0.4
COURT SERVICES AND OFFENDR SUPERVSN AGY	0.4	0.3
ENVIRONMENTAL PROTECTION AGENCY	0.7	0.7
EQUAL EMPLOYMENT OPPORTUNITY COMMISSION	0.6	0.6
FEDERAL COMMUNICATIONS COMMISSION	0.4	0.3
FEDERAL DEPOSIT INSURANCE CORPORATION	0.5	0.5
FEDERAL HOUSING FINANCE AGENCY	0	N/A
FEDERAL RESERVE SYSTEM	0.4	N/A
FEDERAL TRADE COMMISSION	0.3	0.3
GENERAL SERVICES ADMINISTRATION	0.6	0.6
GOVERNMENT PRINTING OFFICE	0.4	0.5
NAT ARCHIVES AND RECORDS ADMINISTRATION	0.3	0.3
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	0.7	0.7
NATIONAL CREDIT UNION ADMINISTRATION	0.5	0.4
NATIONAL LABOR RELATIONS BOARD	0.4	0.5
NATIONAL SCIENCE FOUNDATION	0.3	0.2
NUCLEAR REGULATORY COMMISSION	0.6	0.7
OFFICE OF PERSONNEL MANAGEMENT	0.5	0.4
PENSION BENEFIT GUARANTY CORPORATION	0.4	0.4
RAILROAD RETIREMENT BOARD	0.3	0.3
SECURITIES AND EXCHANGE COMMISSION	0.2	0.2
SMALL BUSINESS ADMINISTRATION	1	1
SMITHSONIAN INSTITUTION	1.8	1.7
SOCIAL SECURITY ADMINISTRATION	1.2	1.2
US AID	0.3	0.4
GOVERMENTWIDE	1.7	1.7


Representation of American Indian/Alaska Natives in Independent Agencies (500+ Employees)
September 30, 2012
FHFA
CFTC
BBG
SEC
RRB
NSF
NARA
FTC
AID
PBGC
NLRB
FED
FCC
CSOS
CNCS
GPO
OPM
NCUA
FDIC
NRC
EEOC
GSA
NASA
EPA
SBA
SSA
SI
0
0.5
1
1.5
2
Percent
FW

WOMEN IN THE FEDERAL WORKFORCE

EMPLOYMENT OF WOMEN



- Women represented 43.5 percent (844,223) of the permanent FW as of September 30, 2012.
- In FY 2011, Women made up 43.6 percent of the FW.
- Black women represented 10.6 percent of the FW in FY 2012 and FY 2011.
- Hispanic women represented 3.4 percent of the FW in FY 2012 and 3.3 percent in FY 2011.
- Asian/Pacific Islander women represented 2.6 percent of the FW in FY 2012 and FY 2011.
- American Indian/Alaska Native women represented 1.0 percent of the FW in FY 2012 and FY 2011.
- Non-Hispanic Multi-Racial women represented 0.4 percent of the FW in FY 2012 and FY 2011.
- White women represented 25.5 percent of the FW in FY 2012, compared to 25.8 percent in FY 2011.

WOMEN BY OCCUPATIONAL CATEGORY

The number of women in professional occupations increased by 4,572 to 226,589 in FY 2012 from 222,017 in FY 2011. Women represented 46.1 percent of all professional Federal employees in FY 2012, compared to 45.6 percent in FY 2011.

The number of women in administrative occupations decreased by 2,552 to 316,538 in FY 2012 from 319,090 in FY 2011. Women represented 43.1 percent of all Federal employees in this occupational category in FY 2012, compared to 43.6 percent in FY 2011.

2012	Employment of Women	Percent of FW
Counts and Percentages of Women based on All employees in Each Occupational Category September 2012)		
Professional	226,589	46.1
Administrative	316,538	43.1
Technical	192,524	57.8
Clerical	80,518	66.4
Other	10,006	13.1
White-Collar (WC)	826,175	47
Blue-Collar (BC)	18,048	9.8
Total (WC + BC)	844,223	43.5

The number of women in technical occupations decreased by 3,174 to 192,524 in FY 2012 from 195,698 in FY 2011. Women represented 57.8 percent of all Federal employees in this occupational category in FY 2012, compared to 58.1 percent in FY 2011.

The number of women in clerical occupations decreased by 2,352 to 80,518 in FY 2012 from 82,870 in FY 2011. Women represented 66.4 percent of all Federal employees in this occupational category in FY 2012, compared to 66.8 percent in FY 2011.

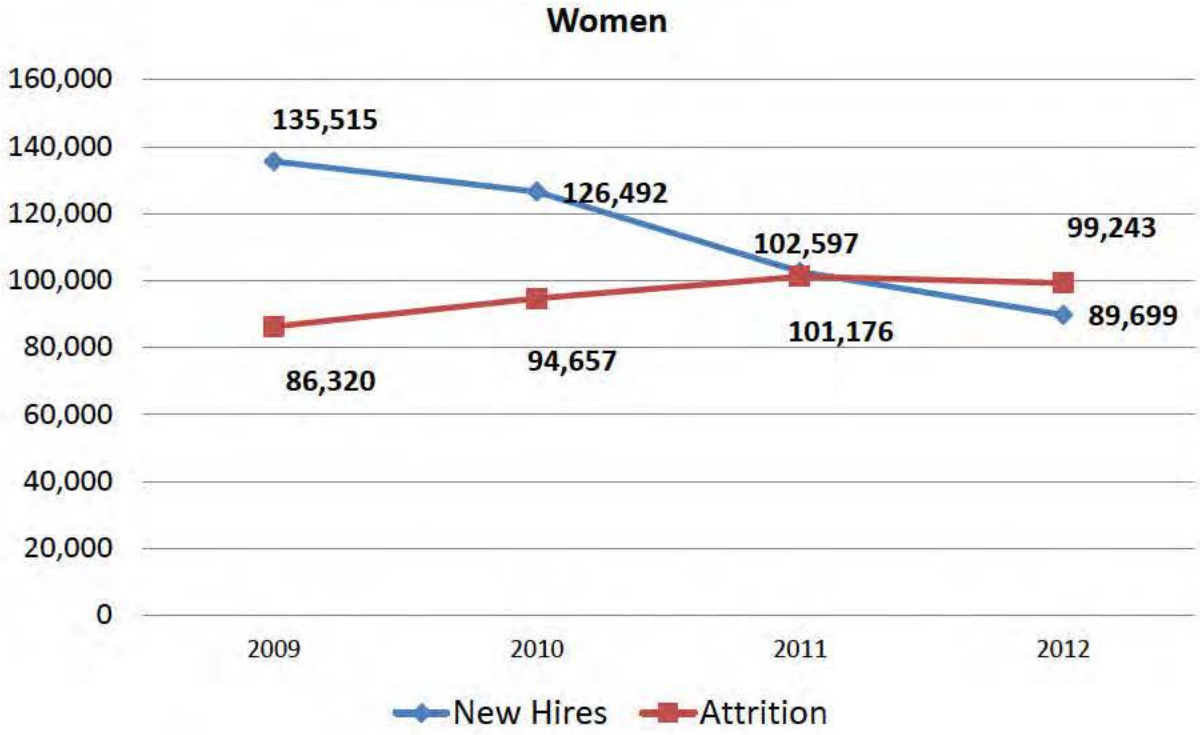
The number of women in "other" white-collar occupations decreased by 182 to 10,006 in FY 2012 from 10,188 in FY 2011. Women represented 13.1 percent of all Federal employees in this occupational category in FY 2012, compared to 13.2 percent in FY 2011.

The number of women in white-collar occupations decreased by 3,688 to 826,175 in FY 2012 from 829,863 in FY 2011. Women represented 47 percent of all Federal employees in this occupational category in FY 2012, compared to 47.2 percent in FY 2011.

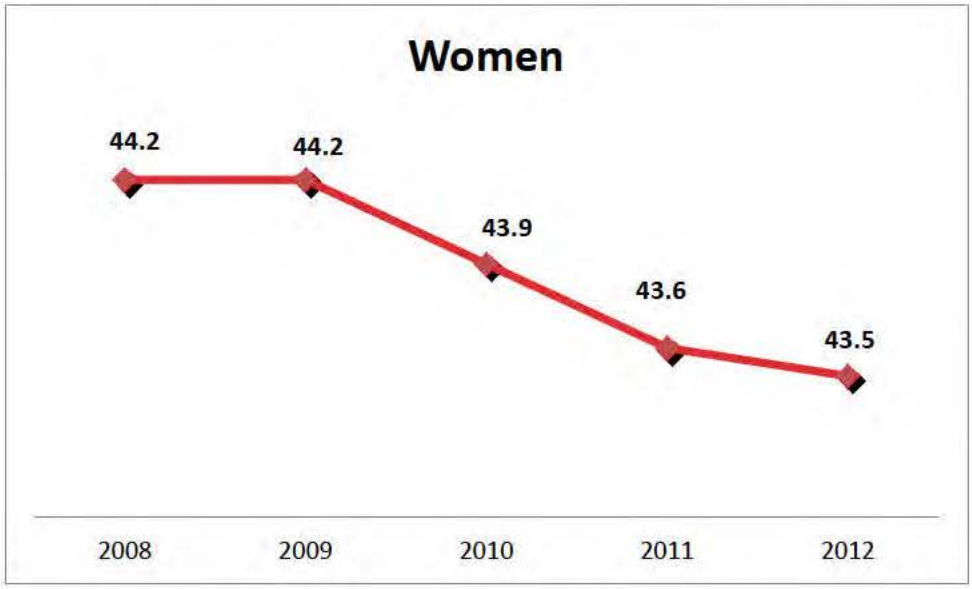
The number of women, in blue-collar occupations, decreased by 346 to 18,048 in FY 2012 from 18,394 in FY 2011. Women represented 9.8 percent of all Federal employees in this occupational category in FY 2012, the same as in FY 2011.

TRENDS

New Hires compared to Attrition[8]



Representation in the Federal Workforce over a 5-year period



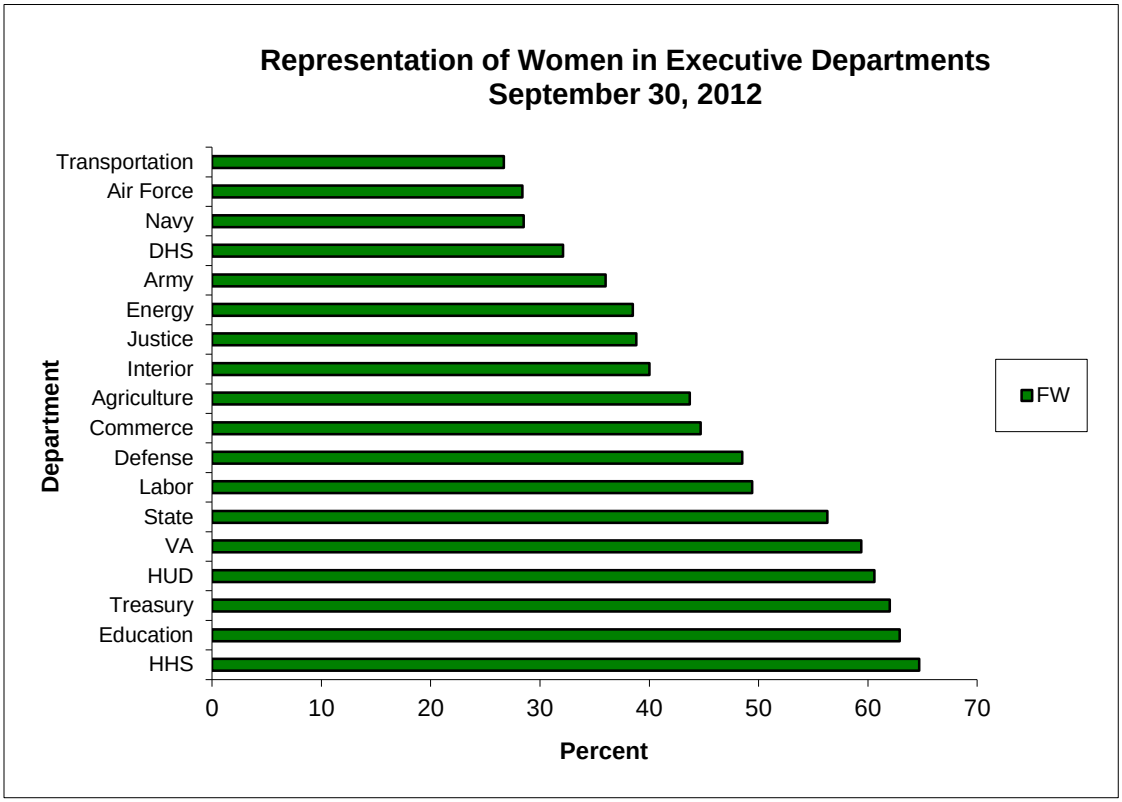
[8] The New Hires compared to Attrition chart does not include Transfers In, nor does it include Transfers Out. Furthermore, the Judicial Branch is entirely excluded and some Executive Branch agencies are not included. Please see data notes for details.

WOMEN PERMANENT NON-POSTAL FEDERAL CIVILIAN EMPLOYMENT SALARY TRENDS

WHITE-COLLAR / PAY SYSTEM GROUPS	2012		2011		DIFFERENCE 2011 TO 2012	
	#	%	#	%	#COUNT	%CHANGE
UP TO $20,000	0	0	1	0	-1	-100
$20,001 TO $40,000	87,670	6.3	92,777	6.6	-5,107	-5.5
$40,001 TO $60,000	202,527	14.5	209,844	15	-7,317	-3.5
$60,001 TO $80,000	156,220	11.2	152,525	10.9	3,695	2.4
$80,001 TO $100,000	114,248	8.2	110,440	7.9	3,808	3.4
$100,001 TO $120,000	68,772	4.9	66,567	4.8	2,205	3.3
$120,001 TO $140,000	27,544	2	26,305	1.9	1,239	4.7
$140,001 TO $160,000	14,244	1	13,702	1	542	4
$160,001 AND GREATER	434	0	508	0	-74	-14.6
UNSPECIFIED	552	0	652	0	-100	-15.3
TOTAL	672,211	48	673,321	48.2	-1,110	-0.2
SES						
$100,001 TO $120,000	14	0.2	15	0.2	-1	-6.7
$120,001 TO $140,000	106	1.3	94	1.2	12	12.8
$140,001 TO $160,000	618	7.9	563	7.2	55	9.8
$160,001 AND GREATER	1,887	24	1,840	23.6	47	2.6
UNSPECIFIED	8	0.1	0	0	8	0
TOTAL	2,633	33.5	2,512	32.3	121	4.8
OTHER WHITE COLLAR						
UP TO $20,000	154	0	153	0	1	0.7
$20,001 TO $40,000	17,437	5	17,761	5	-324	-1.8
$40,001 TO $60,000	21,709	6.2	22,701	6.4	-992	-4.4
$60,001 TO $80,000	35,612	10.2	37,042	10.5	-1,430	-3.9
$80,001 TO $100,000	28,544	8.2	29,504	8.4	-960	-3.3
$100,001 TO $120,000	19,001	5.4	19,511	5.5	-510	-2.6
$120,001 TO $140,000	9,520	2.7	9,193	2.6	327	3.6
$140,001 TO $160,000	8,239	2.4	8,161	2.3	78	1
$160,001 AND GREATER	11,094	3.2	9,983	2.8	1,111	11.1
UNSPECIFIED	21	0	21	0	0	0
TOTAL	151,331	43.3	154,030	43.7	-2,699	-1.8
TOTAL WHITE-COLLAR (PATCO)	826,175	47	829,863	47.2	-3,688	-0.4
TOTAL BLUE-COLLAR	18,048	9.8	18,394	9.8	-346	-1.9
TOTAL WHITE/BLUE-COLLAR	844,223	43.5	848,257	43.6	-4,034	-0.5

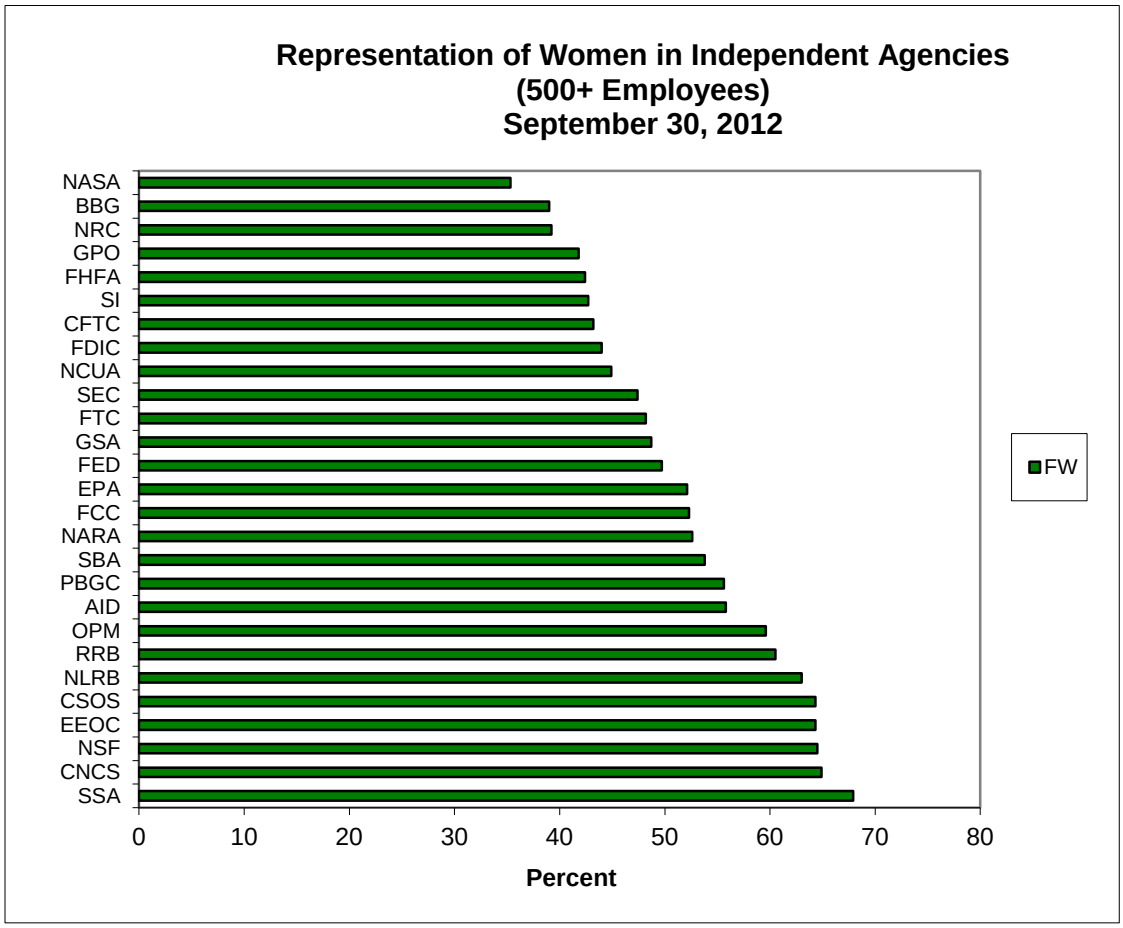
WOMEN REPRESENTATION IN EXECUTIVE DEPARTMENTS

REPRESENTATION IN PERMANENT FEDERAL WORKFORCE September 30, 2012 and September 30, 2011 WOMEN		
EXECUTIVE DEPARTMENTS	**2012 GROUP PCT.**	**2011 GROUP PCT.**
DEPARTMENT OF THE AIR FORCE	28.4	29
DEPARTMENT OF AGRICULTURE	43.7	44
DEPARTMENT OF THE ARMY	36	36.1
DEPARTMENT OF COMMERCE	44.7	45.4
DEPARTMENT OF DEFENSE	48.5	48.9
DEPARTMENT OF JUSTICE	38.8	39.1
DEPARTMENT OF LABOR	49.4	49.4
DEPARTMENT OF ENERGY	38.5	38.3
DEPARTMENT OF EDUCATION	62.9	62.6
DEPARTMENT OF HEALTH AND HUMAN SERVICES	64.7	64.7
DEPARTMENT OF HOMELAND SECURITY	32.1	31.9
DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT	60.6	60.5
DEPARTMENT OF INTERIOR	40	40
DEPARTMENT OF THE NAVY	28.5	28.9
DEPARTMENT OF STATE	56.3	56.6
DEPARTMENT OF TRANSPORTATION	26.7	26.8
DEPARTMENT OF TREASURY	62	62.2
DEPARTMENT OF VETERANS AFFAIRS	59.4	59.5
GOVERNMENTWIDE	43.5	43.6


Representation of Women in Executive Departments
September 30, 2012
Transportation
Air Force
Navy
DHS
Army
Energy
Justice
Interior
Agriculture
Commerce
Defense
Labor
State
VA
HUD
Treasury
Education
HHS
Department
0
10
20
30
40
50
60
70
Percent
FW

WOMEN REPRESENTATION IN 27 INDEPENDENT AGENCIES

REPRESENTATION IN PERMANENT FEDERAL WORKFORCE September 30, 2012 and September 30, 2011 WOMEN		
INDEPENDENT AGENCIES	**2012 GROUP PCT.**	**2011 GROUP PCT.**
BROADCASTING BOARD OF GOVERNORS	39	40
COMMODITY FUTURES TRADING COMMISSION	43.2	N/A
CORP FOR NATIONAL AND COMMUNITY SERVICE	64.9	65.6
COURT SERVICES AND OFFENDR SUPERVSN AGY	64.3	64.2
ENVIRONMENTAL PROTECTION AGENCY	52.1	52
EQUAL EMPLOYMENT OPPORTUNITY COMMISSION	64.3	64
FEDERAL COMMUNICATIONS COMMISSION	52.3	52.8
FEDERAL DEPOSIT INSURANCE CORPORATION	44	43.9
FEDERAL HOUSING FINANCE AGENCY	42.4	N/A
FEDERAL RESERVE SYSTEM	49.7	N/A
FEDERAL TRADE COMMISSION	48.2	49.5
GENERAL SERVICES ADMINISTRATION	48.7	48.6
GOVERNMENT PRINTING OFFICE	41.8	41.2
NAT ARCHIVES AND RECORDS ADMINISTRATION	52.6	52.9
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	35.3	35.6
NATIONAL CREDIT UNION ADMINISTRATION	44.9	44.9
NATIONAL LABOR RELATIONS BOARD	63	63.4
NATIONAL SCIENCE FOUNDATION	64.5	65
NUCLEAR REGULATORY COMMISSION	39.2	39.5
OFFICE OF PERSONNEL MANAGEMENT	59.6	59.2
PENSION BENEFIT GUARANTY CORPORATION	55.6	55.5
RAILROAD RETIREMENT BOARD	60.5	60.6
SECURITIES AND EXCHANGE COMMISSION	47.4	48.2
SMALL BUSINESS ADMINISTRATION	53.8	54.7
SMITHSONIAN INSTITUTION	42.7	42.4
SOCIAL SECURITY ADMINISTRATION	67.9	68.2
US AID	55.8	54.5
GOVERMENTWIDE	43.5	43.6


Representation of Women in Independent Agencies
(500+ Employees)
September 30, 2012
NASA
BBG
NRC
GPO
FHFA
SI
CFTC
FDIC
NCUA
SEC
FTC
GSA
FED
EPA
FCC
NARA
SBA
PBGC
AID
OPM
RRB
NLRB
CSOS
EEOC
NSF
CNCS
SSA
0
10
20
30
40
50
60
70
80
Percent
FW

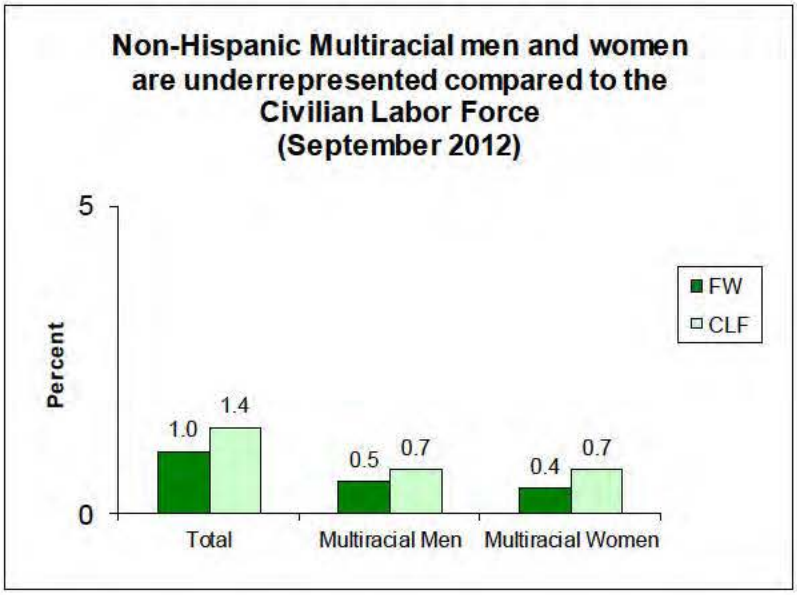
NON-HISPANIC/MULTI-RACIAL EMPLOYMENT IN THE FEDERAL WORKFORCE

NON-HISPANIC/MULTI-RACIAL EMPLOYMENT

Non-Hispanic Multi-Racial employees were 1.0 percent (18,958) of the permanent FW as of September 30, 2012 and 0.8 percent in FY 2011.

Non-Hispanic Multi-Racial men comprised 0.5 percent of the FW in FY 2012 and 0.4 percent in FY 2011.

Non-Hispanic Multi-Racial women comprised 0.4 percent of the FW in FY 2012 and 0.4 percent in FY 2011.



NON-HISPANIC/MULTI-RACIAL[9] BY OCCUPATIONAL CATEGORY

2012	Non-Hispanic Multi-racial Employment	Percent of FW
Counts and Percentages of Non-Hispanic/Multi-Racial based on All Employees in Each Occupational Category (September 2012)		
Professional	4,039	0.8
Administrative	7,849	1.1
Technical	3,014	0.9
Clerical	1,536	1.3
Other	893	1.2
White-Collar (WC)	17,331	1
Blue-Collar (BC)	1,627	0.9
Total (WC + BC)	18,958	1

Non-Hispanic/Multi-Racial employment in professional occupations increased by 631 to 4,039 in FY 2012, from 3,408 in FY 2011. Non-Hispanic/ Multi-Racial employees represented 0.8 percent of all Federal employees in this occupational category in FY 2012, compared to 0.7 percent in FY 2011.

Non-Hispanic/Multi-Racial employment in administrative occupations increased by 1,234 to 7,849 in FY 2012, from 6,615 in FY 2011. Non-Hispanic/ Multi-Racial employees represented 1.1 percent of all Federal employees in this occupational category in FY 2012, compared to 0.9 percent in FY 2011.

Non-Hispanic/Multi-Racial employment in technical occupations increased by 424 to 3,014 in FY 2012, from 2,590 in FY 2011. Non-Hispanic/Multi-Racial employees represented 0.9 percent of all Federal employees in this occupational category in FY 2012, compared to 0.8 percent in FY 2011.

Non-Hispanic/Multi-Racial employment in clerical occupations increased by 275 to 1,536 in FY 2012, from 1,261 in FY 2011. Non-Hispanic/Multi-Racial employees represented 1.3 percent of all Federal employees in this occupational category in FY 2012, compared to1 percent in FY 2011.

Non-Hispanic/Multi-Racial employment in "other" white-collar occupations increased by 76 to 893 in FY 2012, from to 817 in FY 2011. Non-Hispanic/Multi-Racial employees represented 1.2 percent of all Federal employees in this occupational category in FY 2012, compared to 1.1 percent in FY 2011.

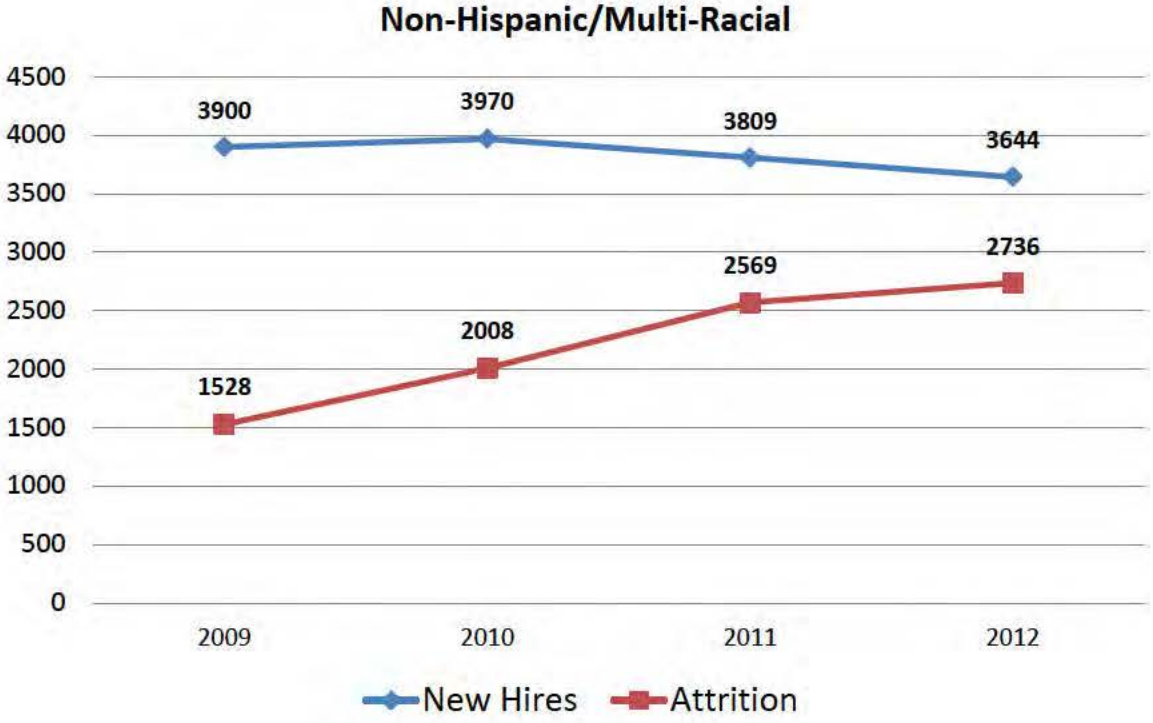
Non-Hispanic/Multi-Racial employment in white-collar occupations increased by 2,640 to 17,331 in FY 2012, from 14,691 in FY2011. Non-Hispanic/Multi-Racial employees represented 1 percent of all Federal employees in this occupational category in FY 2012, compared to 0.8 percent in FY 2011.

[9] Although this new category is not a minority group as determined under 5 U.S.C. § 7201, collection and representation of this data is consistent with the new Racial/National Origin structure required by the Office of Management and Budget. OPM guidance to agencies required use of the new codes for all accessions occurring on or after January 1, 2006. However, while agencies were not required to resurvey their workforce, they had the option to do so. As a result, the Federal civilian employees in this category do not reflect total numbers in the FW; they reflect only those who completed the new Standard Form 181, Ethnicity and Race Identification (dated July 2005).

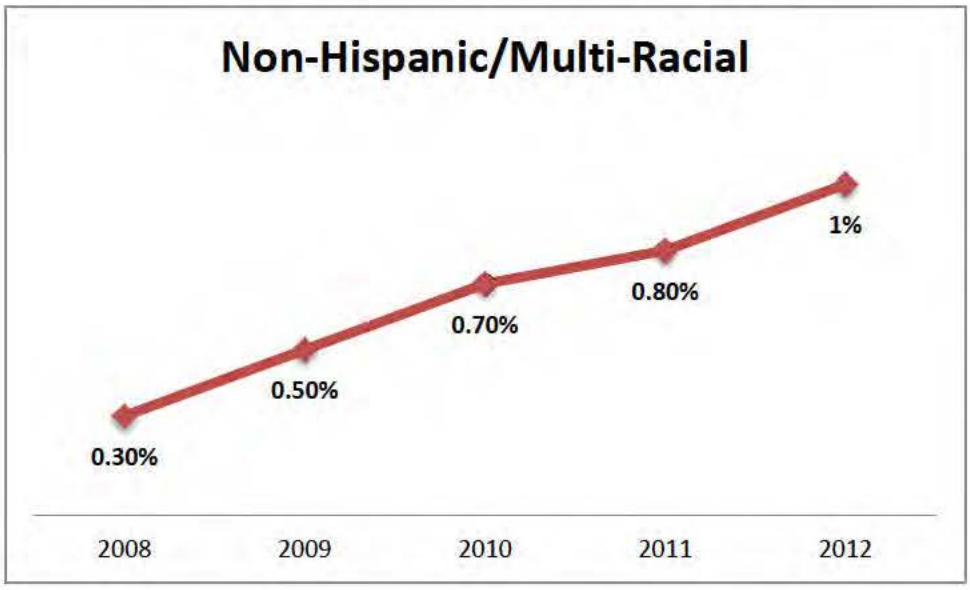
Non-Hispanic/Multi-Racial employment in blue-collar occupations increased by 286 to 1,627 in FY 2012, from 1,341 in FY 2011. Non-Hispanic/Multi-Racial employees represented 0.9 percent of all Federal employees in this occupational category in FY 2012, compared to 0.7 in FY 2011.

TRENDS

New Hires compared to Attrition[10]



Representation in the Federal Workforce over a 5-year period



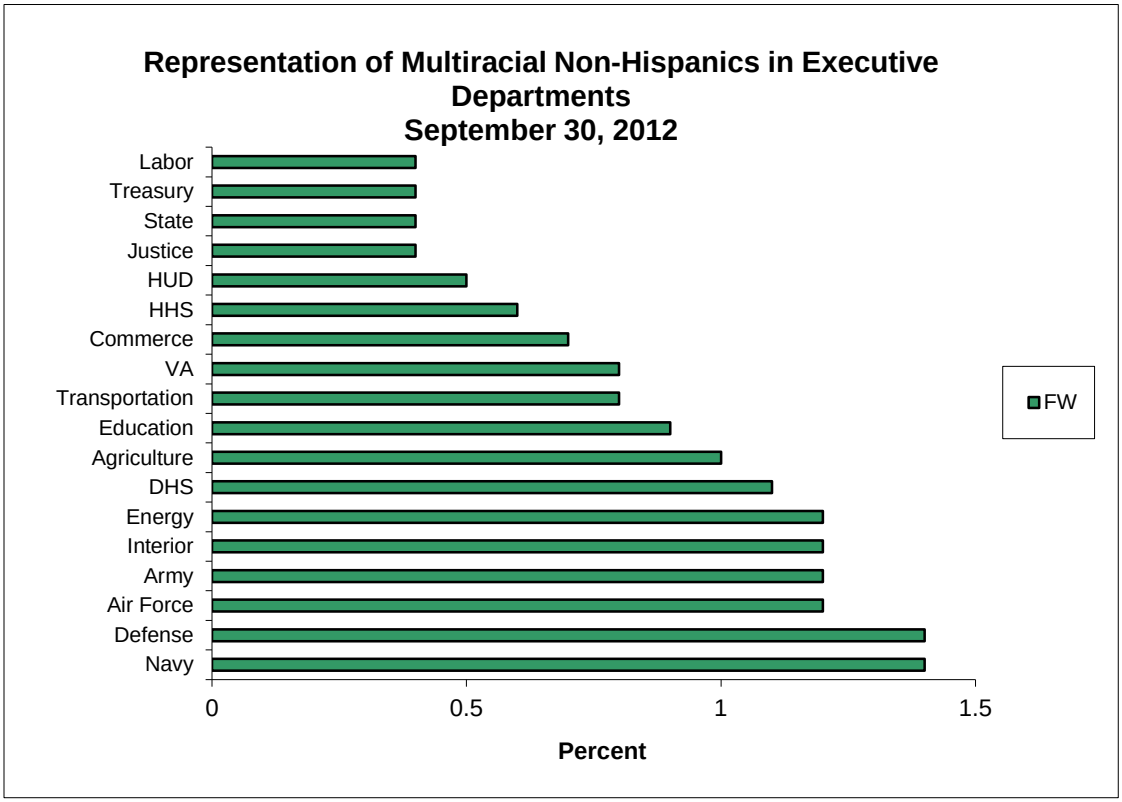
[10] The above chart does not include Transfers In nor does it include Transfers Out. Furthermore, the Judicial Branch is entirely excluded and some Executive Branch agencies are not included. Please see data notes for details.

NON-HISPANIC/MULTI-RACIAL PERMANENT NON-POSTAL FEDERAL CIVILIAN EMPLOYMENT SALARY TRENDS

WHITE-COLLAR / PAY SYSTEM GROUPS GS,GM,GL	2012		2011		DIFFERENCE 2011 TO 2012	
	#	%	#	%	#COUNT	%CHANGE
$20,001 TO $40,000	2,153	0.2	1,952	0.1	201	10.3
$40,001 TO $60,000	3,971	0.3	3,603	0.3	368	10.2
$60,001 TO $80,000	3,971	0.3	3,290	0.2	681	20.7
$80,001 TO $100,000	2,540	0.2	2,020	0.1	520	25.7
$100,001 TO $120,000	1,243	0.1	969	0.1	274	28.3
$120,001 TO $140,000	442	0	344	0	98	28.5
$140,001 TO $160,000	202	0	164	0	38	23.2
$160,001 AND GREATER	14	0	17	0	-3	-17.6
UNSPECIFIED	14	0	10	0	4	40
TOTAL	14,550	1	12,369	0.9	2,181	17.6
SES						
$100,001 TO $120,000	1	0	0	0	1	0
$120,001 TO $140,000	6	0.1	4	0.1	2	50
$140,001 TO $160,000	14	0.2	13	0.2	1	7.7
$160,001 AND GREATER	23	0.3	19	0.2	4	21.1
TOTAL	44	0.6	36	0.5	8	22.2
OTHER WHITE COLLAR						
UP TO $20,000	1	0	1	0	0	0
$20,001 TO $40,000	449	0.1	354	0.1	95	26.8
$40,001 TO $60,000	351	0.1	336	0.1	15	4.5
$60,001 TO $80,000	605	0.2	542	0.2	63	11.6
$80,001 TO $100,000	472	0.1	401	0.1	71	17.7
$100,001 TO $120,000	395	0.1	293	0.1	102	34.8
$120,001 TO $140,000	164	0	120	0	44	36.7
$140,001 TO $160,000	145	0	112	0	33	29.5
$160,001 AND GREATER	155	0	127	0	28	22
TOTAL	2,737	0.8	2,286	0.6	451	19.7
TOTAL WHITE-COLLAR (PATCO)	17,331	1	14,691	0.8	2,640	18
TOTAL BLUE-COLLAR	1,627	0.9	1,341	0.7	286	21.3
TOTAL WHITE/BLUE-COLLAR	18,958	1	16,032	0.8	2,926	18.3

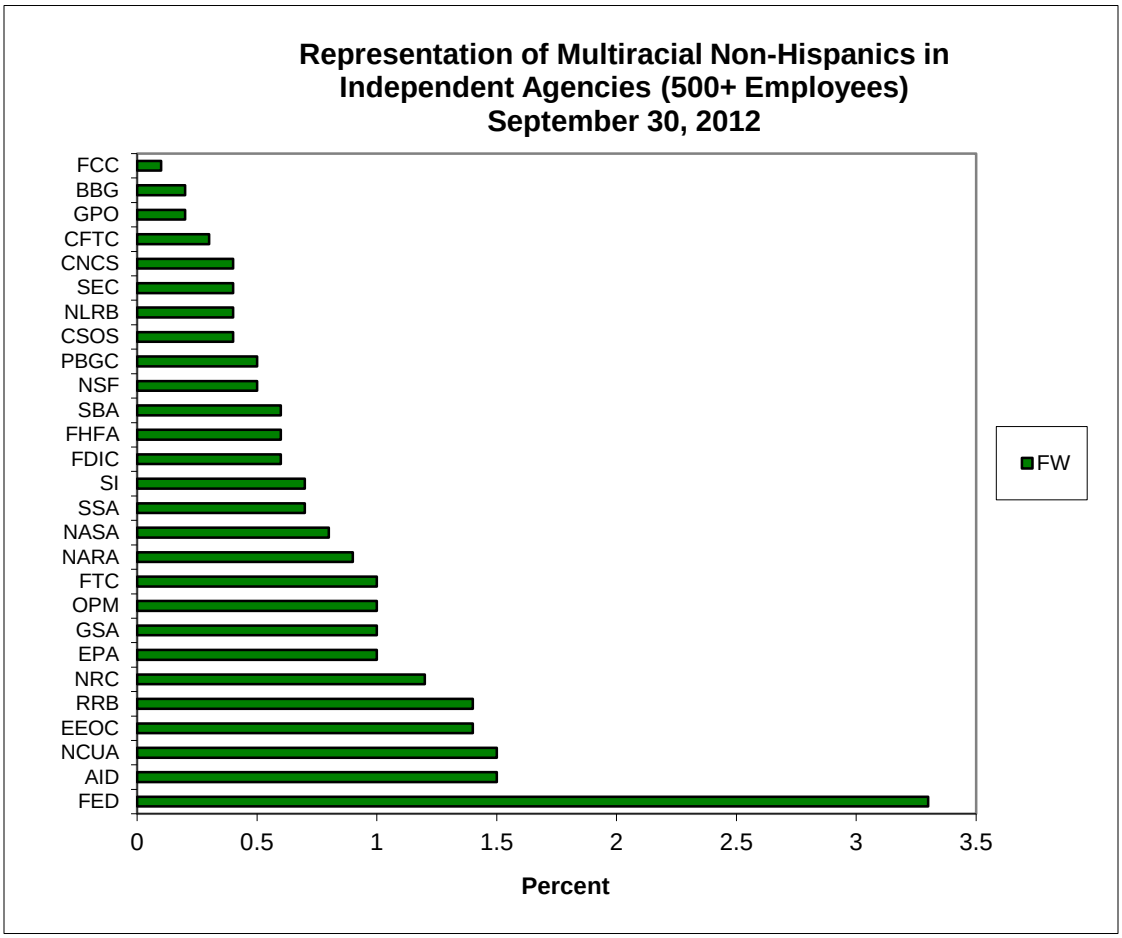
NON-HISPANIC/MULTI-RACIAL REPRESENTATION IN EXECUTIVE DEPARTMENTS

REPRESENTATION IN PERMANENT FEDERAL WORKFORCE September 30, 2012 and September 30, 2011 NON-HISPANIC/MULTI-RACIAL		
EXECUTIVE DEPARTMENTS	**2012 GROUP PCT.**	**2011 GROUP PCT.**
DEPARTMENT OF THE AIR FORCE	1.2	1.1
DEPARTMENT OF AGRICULTURE	1	0.7
DEPARTMENT OF THE ARMY	1.2	1.1
DEPARTMENT OF COMMERCE	0.7	0.5
DEPARTMENT OF DEFENSE	1.4	1.2
DEPARTMENT OF JUSTICE	0.4	0.3
DEPARTMENT OF LABOR	0.4	0.2
DEPARTMENT OF ENERGY	1.2	1
DEPARTMENT OF EDUCATION	0.9	0.8
DEPARTMENT OF HEALTH AND HUMAN SERVICES	0.6	0.3
DEPARTMENT OF HOMELAND SECURITY	1.1	1
DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT	0.5	0.4
DEPARTMENT OF INTERIOR	1.2	1.1
DEPARTMENT OF THE NAVY	1.4	1.1
DEPARTMENT OF STATE	0.4	0
DEPARTMENT OF TRANSPORTATION	0.8	0.7
DEPARTMENT OF TREASURY	0.4	0.2
DEPARTMENT OF VETERANS AFFAIRS	0.8	0.7
GOVERNMENTWIDE	1	0.8


Representation of Multiracial Non-Hispanics in Executive Departments
September 30, 2012
Labor
Treasury
State
Justice
HUD
HHS
Commerce
VA
Transportation
Education
Agriculture
DHS
Energy
Interior
Army
Air Force
Defense
Navy
0
0.5
1
1.5
Percent
FW

NON-HISPANIC/MULTI-RACIAL REPRESENTATION IN 27 INDEPENDENT AGENCIES

REPRESENTATION IN PERMANENT FEDERAL WORKFORCE September 30, 2012 and September 30, 2011 NON-HISPANIC/MULTI-RACIAL		
INDEPENDENT AGENCIES	**2012 GROUP PCT.**	**2011 GROUP PCT.**
BROADCASTING BOARD OF GOVERNORS	0.2	0.2
COMMODITY FUTURES TRADING COMMISSION	0.3	N/A
CORP FOR NATIONAL AND COMMUNITY SERVICE	0.4	0.4
COURT SERVICES AND OFFENDR SUPERVSN AGY	0.4	0.3
ENVIRONMENTAL PROTECTION AGENCY	1	1
EQUAL EMPLOYMENT OPPORTUNITY COMMISSION	1.4	1.4
FEDERAL COMMUNICATIONS COMMISSION	0.1	0.1
FEDERAL DEPOSIT INSURANCE CORPORATION	0.6	0.5
FEDERAL HOUSING FINANCE AGENCY	0.6	N/A
FEDERAL RESERVE SYSTEM	3.3	N/A
FEDERAL TRADE COMMISSION	1	0.6
GENERAL SERVICES ADMINISTRATION	1	0.9
GOVERNMENT PRINTING OFFICE	0.2	0.3
NAT ARCHIVES AND RECORDS ADMINISTRATION	0.9	0.9
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	0.8	0.7
NATIONAL CREDIT UNION ADMINISTRATION	1.5	1.5
NATIONAL LABOR RELATIONS BOARD	0.4	0.3
NATIONAL SCIENCE FOUNDATION	0.5	0.6
NUCLEAR REGULATORY COMMISSION	1.2	0.9
OFFICE OF PERSONNEL MANAGEMENT	1	0.7
PENSION BENEFIT GUARANTY CORPORATION	0.5	0.5
RAILROAD RETIREMENT BOARD	1.4	1.2
SECURITIES AND EXCHANGE COMMISSION	0.4	0.4
SMALL BUSINESS ADMINISTRATION	0.6	0.4
SMITHSONIAN INSTITUTION	0.7	0.4
SOCIAL SECURITY ADMINISTRATION	0.7	0.6
US AID	1.5	0.8
GOVERMENTWIDE	1	0.8


Representation of Multiracial Non-Hispanics in Independent Agencies (500+ Employees) September 30, 2012
FCC
BBG
GPO
CFTC
CNCS
SEC
NLRB
CSOS
PBGC
NSF
SBA
FHFA
FDIC
SI
SSA
NASA
NARA
FTC
OPM
GSA
EPA
NRC
RRB
EEOC
NCUA
AID
FED
0
0.5
1
1.5
2
2.5
3
3.5
Percent
FW

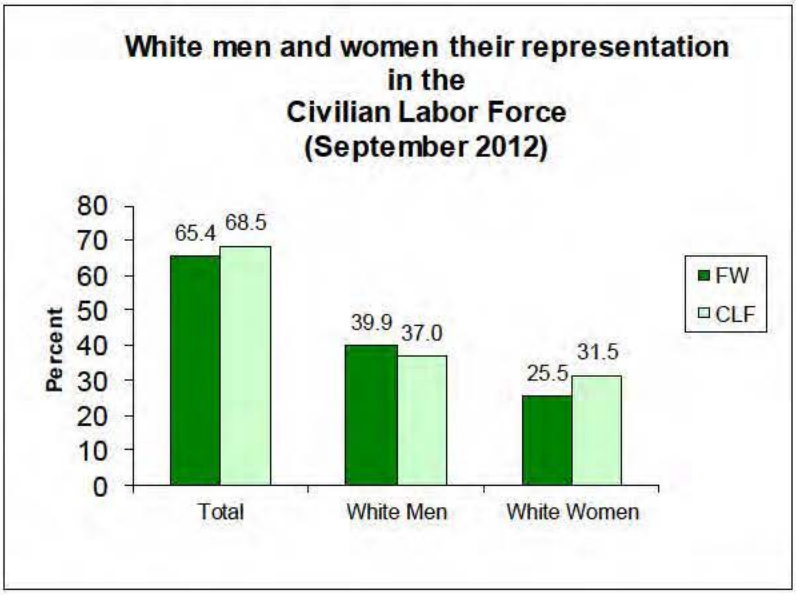
WHITES IN THE FEDERAL WORKFORCE

WHITE EMPLOYMENT

White employees comprised 65.4 percent (1,270,362) of the permanent FW as of September 30, 2012 and 65.9 percent in FY 2011.

White men comprised 39.9 percent of the FW in FY 2012 and 40.1 percent in FY 2011.

White women comprised 25.5 percent of the FW in FY 2012 and 25.8 percent in FY 2011.



WHITES[11] BY OCCUPATIONAL CATEGORY

White employment in professional occupations increased by 716 to

357,590 in FY 2012, from 356,874 in FY 2011. Whites represented 72.8 percent of all Federal employees in this occupational category in FY 2012, compared to 73.4 percent in FY 2011.

White employment in administrative occupations decreased by 2,529 to 488,615 in FY 2012, from 491,144 in FY 2011. Whites represented 66.6 percent of all Federal employees in this occupational category in FY 2012, compared to 67.1 percent in FY 2011.

White employment in technical occupations decreased by 4,009 to 194,924 in FY 2012, from 198,933 in FY 2011. Whites represented 58.5 percent of all Federal employees in this occupational category in FY 2012, compared to 59 percent in FY 2011.

2012	White Employment	Percent of FW
Counts and Percentages of White based on All Employees in Each Occupational Category (September 2012)		
Professional	357,590	72.8
Administrative	488,615	66.6
Technical	194,924	58.5
Clerical	63,612	52.5
Other	44,890	58.8
White-Collar (WC)	1,149,631	65.5
Blue-Collar (BC)	120,731	65.2
Total (WC + BC)	1,270,362	65.4

White employment in clerical occupations decreased by 2,192, to 63,612 in FY 2012, from 65,804 in FY 2011. Whites represented 52.5 percent of all Federal employees in this occupational category in FY 2012, compared to 53.1 percent in FY 2011.

White employment in "other" white-collar occupations decreased by 1,084, to 44,890 in FY 2012 from 45,974 in FY 2011. Whites represented 58.8 percent of all Federal employees in this occupational category in FY 2012, compared to 59.4 percent in FY 2011.

White employment in white-collar occupations decreased by 9,098 to 1,149,631 in FY 2012 from 1,158,729 in FY 2011. Whites represented 65.5 percent of all Federal employees in this occupational category in FY 2012, compared to 66 percent in FY 2011.

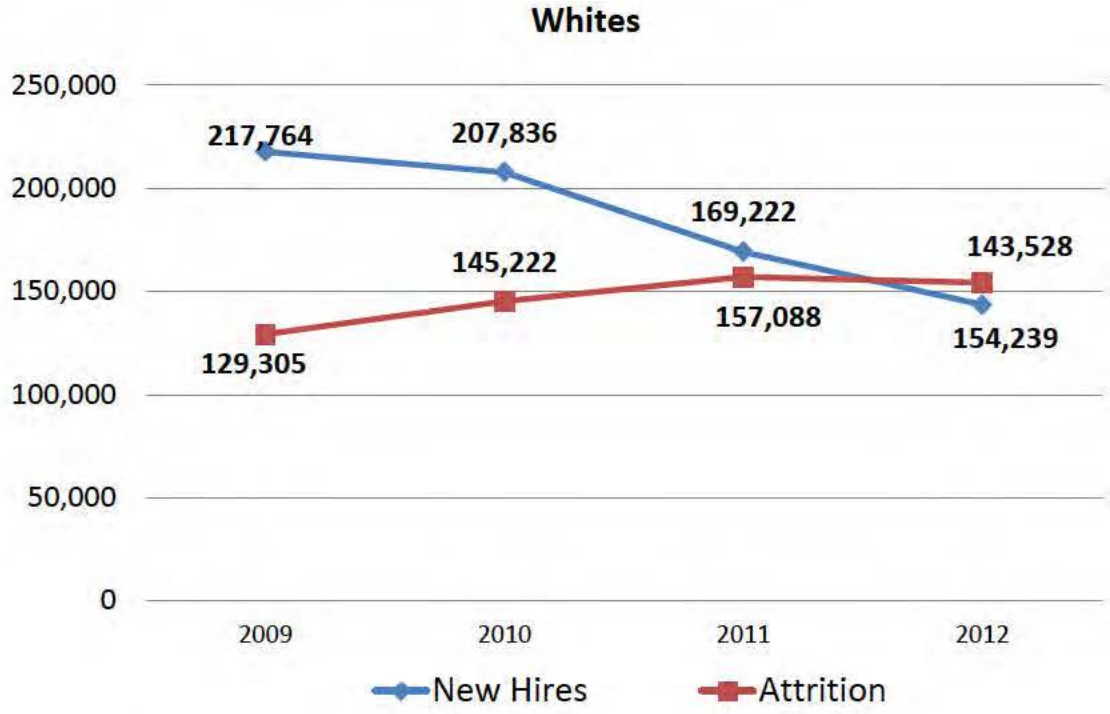
---

[11] Although this new category is not a minority group as determined under 5 U.S.C. § 7201, collection and representation of this data is consistent with the new Racial/National Origin structure required by the Office of Management and Budget. OPM guidance to agencies required use of the new codes for all accessions occurring on or after January 1, 2006. However, while agencies were not required to resurvey their workforce, they had the option to do so. As a result, the Federal civilian employees in this category do not reflect total numbers in the FW; they reflect only those who completed the new Standard Form 181, Ethnicity and Race Identification (dated July 2005).

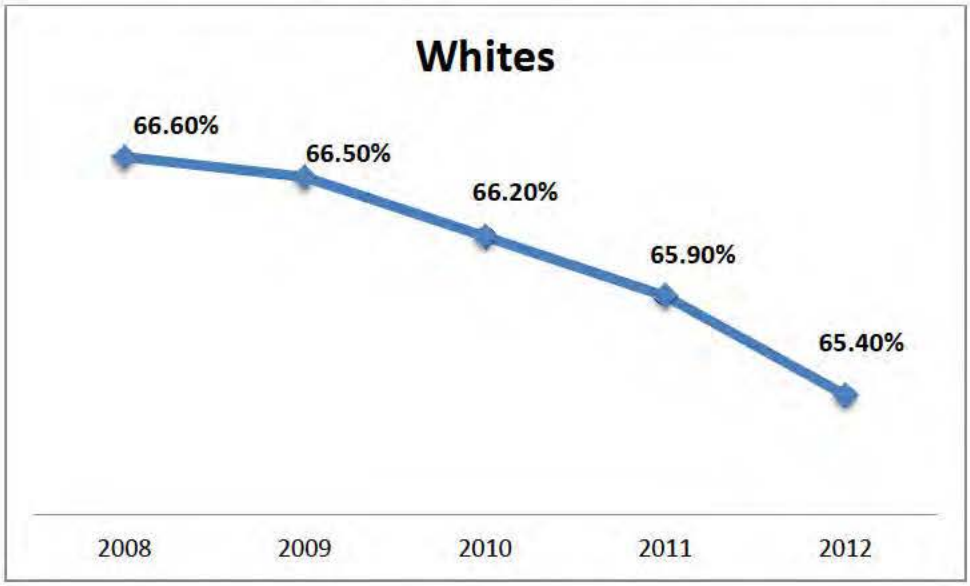
White employment in blue-collar occupations decreased by 2,199, to 120,731 in FY 2012 from 122,930 in FY 2011. Whites represented 65.2 percent of all Federal employees in this occupational category in FY 2012, as compared to 65.5 percent in FY 2011.

TRENDS

New Hires compared to Attrition[12]



Representation in the Federal Workforce over a 5-year period



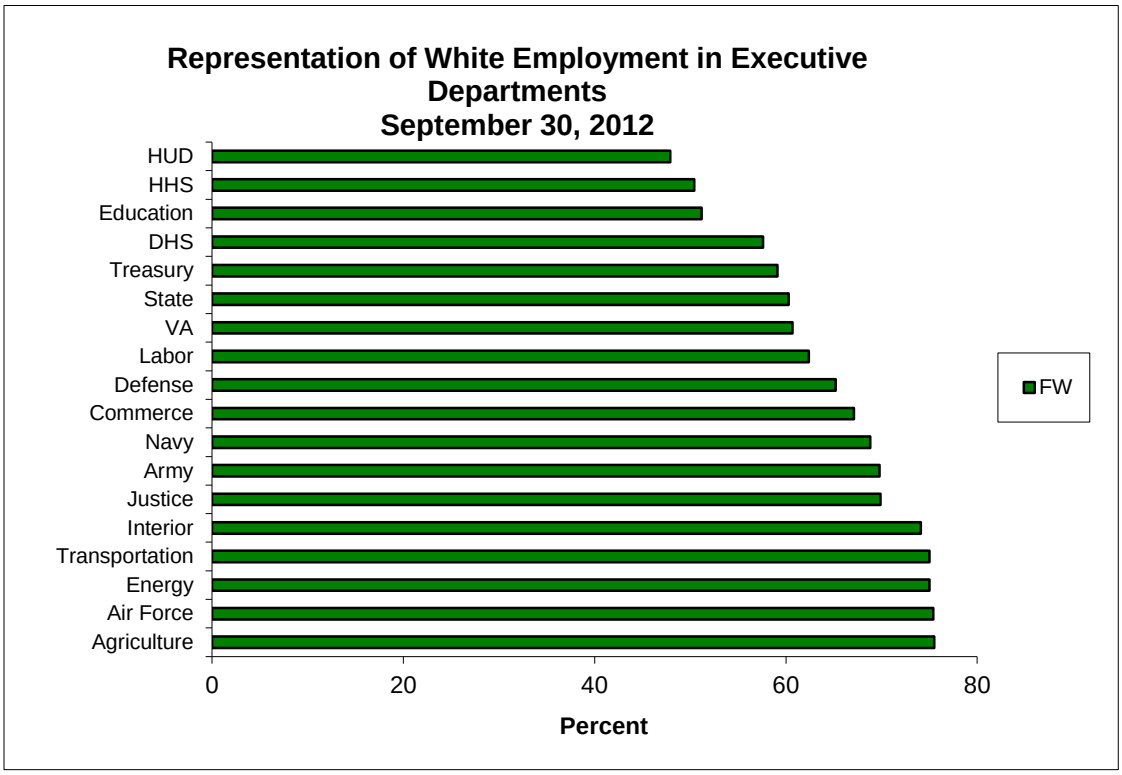
[12] The New Hires compared to Attrition chart does not include Transfers In, nor does it include Transfers Out. Furthermore, the Judicial Branch is entirely excluded and some Executive Branch agencies are not included. Please see data notes for details.

WHITE PERMANENT NON-POSTAL FEDERAL CIVILIAN EMPLOYMENT SALARY TRENDS

WHITE-COLLAR / PAY SYSTEM GROUPS GS,GM,GL	2012		2011		DIFFERENCE 2011 TO 2012	
	#	%	#	%	#COUNT	%CHANGE
UP TO $20,000	0	0	1	0	-1	-100
$20,001 TO $40,000	80,256	5.7	85,320	6.1	-5,064	-5.9
$40,001 TO $60,000	211,498	15.1	222,008	15.9	-10,510	-4.7
$60,001 TO $80,000	218,159	15.6	213,414	15.3	4,745	2.2
$80,001 TO $100,000	183,302	13.1	180,131	12.9	3,171	1.8
$100,001 TO $120,000	121,264	8.7	119,645	8.6	1,619	1.4
$120,001 TO $140,000	51,687	3.7	50,784	3.6	903	1.8
$140,001 TO $160,000	32,108	2.3	31,724	2.3	384	1.2
$160,001 AND GREATER	1,671	0.1	1,931	0.1	-260	-13.5
UNSPECIFIED	585	0	727	0.1	-142	-19.5
TOTAL	900,530	64.4	905,685	64.9	-5,155	-0.6
SES						
$100,001 TO $120,000	15	0.2	15	0.2	0	0
$120,001 TO $140,000	152	1.9	135	1.7	17	12.6
$140,001 TO $160,000	1,285	16.3	1,183	15.2	102	8.6
$160,001 AND GREATER	4,873	61.9	4,990	64.1	-117	-2.3
UNSPECIFIED	15	0.2	0	0	15	0
TOTAL	6,340	80.6	6,323	81.2	17	0.3
OTHER WHITE COLLAR						
UP TO $20,000	117	0	117	0	0	0
$20,001 TO $40,000	19,818	5.7	21,063	6	-1,245	-5.9
$40,001 TO $60,000	25,504	7.3	27,087	7.7	-1,583	-5.8
$60,001 TO $80,000	43,202	12.4	44,803	12.7	-1,601	-3.6
$80,001 TO $100,000	40,774	11.7	41,990	11.9	-1,216	-2.9
$100,001 TO $120,000	39,437	11.3	40,600	11.5	-1,163	-2.9
$120,001 TO $140,000	23,462	6.7	22,542	6.4	920	4.1
$140,001 TO $160,000	23,190	6.6	23,066	6.5	124	0.5
$160,001 AND GREATER	27,226	7.8	25,413	7.2	1,813	7.1
UNSPECIFIED	31	0	40	0	-9	-22.5
TOTAL	242,761	69.5	246,721	70	-3,960	-1.6
TOTAL WHITE-COLLAR (PATCO)	1,149,631	65.5	1,158,729	66	-9,098	-0.8
TOTAL BLUE-COLLAR	120,731	65.2	122,930	65.5	-2,199	-1.8
TOTAL WHITE/BLUE-COLLAR	1,270,362	65.4	1,281,659	65.9	-11,297	-0.9

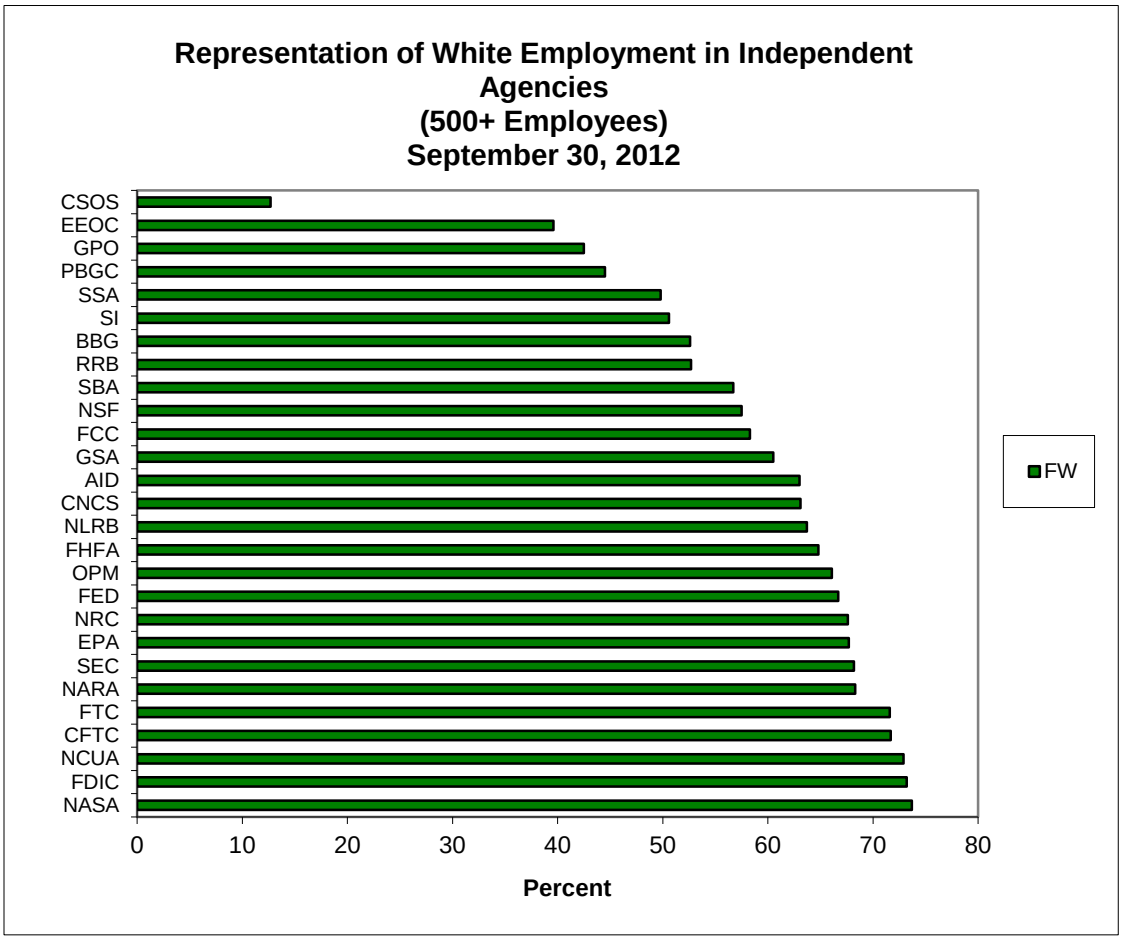
WHITE REPRESENTATION IN EXECUTIVE DEPARTMENTS

REPRESENTATION IN PERMANENT FEDERAL WORKFORCE September 30, 2012 and September 30, 2011 WHITES		
EXECUTIVE DEPARTMENTS	**2012 GROUP PCT.**	**2011 GROUP PCT.**
DEPARTMENT OF THE AIR FORCE	75.5	75.7
DEPARTMENT OF AGRICULTURE	75.4	76.5
DEPARTMENT OF THE ARMY	69.8	69.9
DEPARTMENT OF COMMERCE	67.1	68.1
DEPARTMENT OF DEFENSE	65.2	65.7
DEPARTMENT OF JUSTICE	57.6	70
DEPARTMENT OF LABOR	51.2	63.2
DEPARTMENT OF ENERGY	75	75.1
DEPARTMENT OF EDUCATION	50.4	51.2
DEPARTMENT OF HEALTH AND HUMAN SERVICES	47.9	51
DEPARTMENT OF HOMELAND SECURITY	74.1	57.7
DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT	69.9	48.3
DEPARTMENT OF INTERIOR	62.4	74.1
DEPARTMENT OF THE NAVY	68.8	69.5
DEPARTMENT OF STATE	60.3	61.1
DEPARTMENT OF TRANSPORTATION	75	75.3
DEPARTMENT OF TREASURY	59.1	60.1
DEPARTMENT OF VETERANS AFFAIRS	60.7	60.9
GOVERNMENTWIDE	65.4	65.9


Representation of White Employment in Executive Departments
September 30, 2012
HUD
HHS
Education
DHS
Treasury
State
VA
Labor
Defense
Commerce
Navy
Army
Justice
Interior
Transportation
Energy
Air Force
Agriculture
0
20
40
60
80
Percent
FW

WHITE REPRESENTATION IN 27 INDEPENDENT AGENCIES

REPRESENTATION IN PERMANENT FEDERAL WORKFORCE September 30, 2012 and September 30, 2011 WHITES		
INDEPENDENT AGENCIES	**2012 GROUP PCT.**	**2011 GROUP PCT.**
BROADCASTING BOARD OF GOVERNORS	52.6	53.4
COMMODITY FUTURES TRADING COMMISSION	71.7	N/A
CORP FOR NATIONAL AND COMMUNITY SERVICE	63.1	61.8
COURT SERVICES AND OFFENDR SUPERVSN AGY	12.7	12.8
ENVIRONMENTAL PROTECTION AGENCY	67.7	67.9
EQUAL EMPLOYMENT OPPORTUNITY COMMISSION	39.6	40.1
FEDERAL COMMUNICATIONS COMMISSION	58.3	58.1
FEDERAL DEPOSIT INSURANCE CORPORATION	73.2	73.7
FEDERAL HOUSING FINANCE AGENCY	64.8	N/A
FEDERAL RESERVE SYSTEM	66.7	N/A
FEDERAL TRADE COMMISSION	71.6	72
GENERAL SERVICES ADMINISTRATION	60.5	61.1
GOVERNMENT PRINTING OFFICE	42.5	41.5
NAT ARCHIVES AND RECORDS ADMINISTRATION	68.3	69.1
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	73.7	74.3
NATIONAL CREDIT UNION ADMINISTRATION	72.9	75.2
NATIONAL LABOR RELATIONS BOARD	63.7	63.8
NATIONAL SCIENCE FOUNDATION	57.5	57.5
NUCLEAR REGULATORY COMMISSION	67.6	68.2
OFFICE OF PERSONNEL MANAGEMENT	66.1	68
PENSION BENEFIT GUARANTY CORPORATION	44.5	44.5
RAILROAD RETIREMENT BOARD	52.7	55.2
SECURITIES AND EXCHANGE COMMISSION	68.2	68.4
SMALL BUSINESS ADMINISTRATION	56.7	57.5
SMITHSONIAN INSTITUTION	50.6	50.8
SOCIAL SECURITY ADMINISTRATION	49.8	50.2
US AID	63	63.9
GOVERMENTWIDE	65.4	43.6


Representation of White Employment in Independent Agencies
(500+ Employees)
September 30, 2012
CSOS
EEOC
GPO
PBGC
SSA
SI
BBG
RRB
SBA
NSF
FCC
GSA
AID
CNCS
NLRB
FHFA
OPM
FED
NRC
EPA
SEC
NARA
FTC
CFTC
NCUA
FDIC
NASA
0
10
20
30
40
50
60
70
80
Percent
FW

AGENCY FEORP CURRENT PRACTICES

AGENCY FEORP INITIATIVES

In FY 2012, agencies reported that they continued their human resources initiatives in support of the Federal Equal Opportunity Recruitment Program (FEORP).

OPM requested agencies to provide diversity and inclusion training conducted for agency managers and supervisors; and the steps taken to assess the performance of managers and senior executives with respect to supporting diversity and inclusion. The following practices are highlighted in the area of learning.

National Aeronautics and Space Administration (NASA)

NASA's Offices of Human Capital Management (OHCM) and Diversity and Equal Opportunity (ODEO) have partnered closely to enhance the agency's recruitment strategies, allowing the agency to reach a broader and more diverse talent pool through implementation of the new Pathways Program.

NASA's Office of Education implemented a series of innovative projects designed to stimulate student interest in order to motivate higher levels of study in science, technology, engineering and mathematics (STEM), and expand the diversity of the nation's current and future STEM labor force pipeline.

The Science and Engineering Mathematics Aerospace Academy (SEMAA) is NASA's national project designed to increase the participation and retention of historically underserved and underrepresented K-12 youth in STEM. With respect to E.O. 13171 of October 12, 2000, NASA reports that a total of 6,631 Hispanic students participated, or 30 percent of the total students served.

Department of Interior (DOI)

Nearly 2,000 DOI managers and supervisors completed the Championing Diversity workshop in FY 2012. The Championing Diversity workshop was in part due to DOI's partnership with a private entity with a proven track record of achieving diversity and inclusion mind-set shifts and buy-in.

DOI's new approach is to educate managers and supervisors on diversity and inclusion so they understand that inclusivity is not just about whether whom they hire has paid off. They now embrace the various dimensions of diversity and recognize that the multiple frameworks and underpinning diversity and inclusion are important to achieving the mission and goals of the agency.

DOI is particularly proud of its Diversity Change Agent Program. DOI established the program to affect and mobilize stakeholders to embrace and enact its Inclusive Workplace Strategy.

DOI trained 265 new diversity change agents in FY2012, as well as established partnerships with other Federal agencies to conduct diversity agent training.

Department of Treasury

The Department of Treasury's Treasury Executive Institute (TEI) began a pilot-coaching program that has thus far served 202 clients. TEI also has plans to expand coaching training in FY 2013.

In March 2013, the Department of Treasury implemented a new Treasury-wide mentoring program aimed at employees with less than three years of Federal experience. The program initially targeted 75 mentees matched with 75 mentors. The mentoring program consists of orientation, training, mid-point evaluation and end-of-year evaluation.

Social Security Administration (SSA)

In FY 2012, SSA developed a cost-effective approach to training by creating a bi-lingual portal, which provides a region-wide training product that teaches more employees. Additionally, with respect to E.O. 13171 of October 12, 2000, SSA reports that 6.36 percent of our developmental program participants in FY 2012 were Hispanic.

National Transportation Safety Board (NTSB)

The Professional Development Program (PDP) is open to permanent staff in grades GS-9 through 13 and is based on enhancing core competencies focusing on career development and goal setting and providing assistance in overall career direction and progression.

The Leadership Development Program (LDP) is open to permanent staff in grades GS-13 through 15.

In FY 2012, the Office of EEO, Diversity and Inclusion completed the Diversity DARE branding campaign and video. The branding campaign and video demonstrate the importance of diversity and inclusion at the NTSB and also illustrate how employees from diverse backgrounds bring different perspectives to problem solving, creativity, innovation and management, making teams stronger and more effective. Because NTSB needs problem solvers, this approach is key to the accomplishment of the transportation safety mission.

Department of Veterans Affairs (VA)

The Department of Veterans Affairs, worked with OPM's Office of Diversity and Inclusion (ODI) to create a measurement tool that can help agencies measure their employees' perceptions of inclusion. This measurement tool is called the New IQ or the New Inclusion Quotient (IQ). The New IQ includes training developed based on research and questions from the Federal Employee Viewpoint Survey (EVS). The training helps supervisors hone inclusive habits that help create fair, open, cooperative, supportive, and empowering work environments. The VA hopes this tool will improve teamwork and better

utilization of talent, increase resiliency and retention, increase innovation and creativity, and improve team performance and productivity.

With respect to E.O. 13171, VA reports that the VA National Cemetery Administration (NCA) developed and is implementing the Hispanic Veterans Careers Coalition, an initiative that reviews VA Hispanic employment practices and develop improved processes to increase Hispanic Veteran employment. This initiative will also address reasons for high joblessness, the impact of current outreach strategies and the exploration of Veterans business enterprise as a source of employment for Hispanic Operation Enduring Freedom and Operation Iraqi Freedom heroes.

The NCA will continue its collaboration with the League of United Latin American Citizens on its strategy for integrating education, employment, outreach and entrepreneurship to increase educational and occupational opportunities for Hispanic and disabled Veterans.

Agency Successful/Promising Practices

Agencies were asked to submit their successful or promising practices from the agency-specific Diversity and Inclusion Strategic Plans. The following are some of those practices:

Corporation for National and Community Service (CNCS)

To broaden the scope and agency conversation regarding diversity and inclusion (D&I), CNCS developed CELEBRATE Diversity Month. This program engages staff in a series of activities beyond the normal "special emphasis" to heighten their awareness of the many facets of diversity and inclusion. Each year a new program theme is used as the lens to view different aspects of D&I, and how it relates to ALL of us. CNCS is infused with opportunities to celebrate through educational experiences in presentations, music, art, photography, dance and literature. Collaborative partnerships with other Federal entities, non-governmental agencies and CNCS's Affinity groups ensure the richness in their programming.

Department of Agriculture (USDA)

USDA Monthly Cultural Transformation Milestones and Metrics Reports contain key metrics that are reported to the Secretary to measure progress in the following areas: Diversity and Inclusion, Disability Hiring, Veterans Hiring, Diversity of Student Employment, Telework participation, Communication, Process Improvement, Labor Relations, Equal Employment Opportunity Accountability, Hiring Reform, Employee Development, and Employee Viewpoint Survey Results (Annually). In addition, the Milestone and Metrics Report is tied to performance management of all USDA Senior Executives. Monthly Report Cards/Mid-Year Report Card Ranking is also used to measure and rate progress as reaching or achieving set targets for all metrics, except Diversity and Inclusion/Student Diversity. Similarly, USDA assesses the performance of

supervisors, managers and senior executives with respect to supporting diversity and inclusion.

In addition, USDA hires over six thousand student interns annually. The Student Intern Program is the agency's pipeline for future USDA employees, and the agency has developed strong programs dedicated to attracting candidates from all segments of society, including, for example, African Americans, American Indians/Alaska Natives, Hispanics, Asians, and Students with Disabilities. Moreover, the USDA Student Portal is a one-stop application process where students can apply for internships across the United States within the 17 USDA agencies.

Department of Commerce (Commerce)

Commerce has a dedicated manager for hiring people with disabilities in addition to the program manager required for Veterans employment. The Department's Minority Business Development Agency voluntarily agreed that before advertising vacancies and filling them through the competitive process, it would check with the disability program manager to determine whether there were qualified candidates with disabilities who were eligible for non-competitive appointments under 5 C.F.R. 213.3102(u). The Department's National Technical Information Service is considering becoming the second bureau to voluntarily follow the same process.

Department of Defense (DoD)

DoD's Veterans Employment Initiative was established in January of 2010, in support of Presidential Executive Order 13518 - making promoting opportunities for Veterans in the Federal Government a top priority. The initiative encourages DoD component collaboration and support on Veterans' issues and includes providing career guidance and assistance to transitioning service members and Veterans through multiple modes of communication and outreach venues, such as personalized one-on-one interaction and assistance; interagency hiring fairs; and the Hiring Heroes Program. The Hiring Heroes Program provides career fairs to assist wounded warriors, transitioning service members, and Veterans and military spouses in their search for employment.

Department of Education (ED)

The Department of Education is the smallest of the cabinet level agencies and must effectively utilize internal resources as well as leverage external partnerships to achieve diversity and inclusion. To provide diversity and inclusion awareness and opportunities, ED has successfully developed and strengthened partnerships with:

- OPM's Office of Diversity and Inclusion (ODI); and
- The National Organizations (i.e. League of United Latin American Citizens (LULAC) and Federal Asian Pacific American Council (FAPAC)), and reinvigorated internship programs with diverse organizations such as: Conference on Asian Pacific American Leadership (CAPAL) and Hispanic Association of Colleges and Universities (HACU).

ED also has strengthened linkages to the mission side of the organization to leverage research and partnerships to inform strategic recruitment and outreach. These linkages include partnerships with:

- National Center for Education Statistics;
- White House Initiative Office on Education Excellence for Hispanics;
- White House Initiative Office on Asian American and Pacific Islanders;
- White House Initiative Office on American Indian and Alaska Native Education; and
- White House Initiative Office on Historically Black Colleges and Universities.

Department of Energy (DOE)

The Secretary of Energy established DOE's Diversity and Inclusion Council to help create a performance-based culture that better fosters diversity and inclusion. The Council is an extension of the Chief Operating Officer's Board (COOB), DOE's most senior career leaders. It ensures that the values underlying diversity and inclusion are institutionalized and integrated in all strategic management initiatives. The Council, meeting bi-weekly, uses a systematic approach to align DOE's strategies, processes, structures, and people and makes recommendations on how to overcome barriers impacting diversity and inclusion. The Council's goal is to improve mission execution through high performance, resulting from a mission-focused, accountable, and inclusive workforce.

Department of Health and Human Services (HHS)

HHS honors the diversity of its Veterans. HHS launched its own Veterans History Project with participating Veterans reflecting the full spectrum of diversity

including women, Hispanics, and persons with disabilities. This project reignited HHS's Veterans' passion by allowing them to share their military stories on video in the Secretary's Recording Studio. With over 20 stories filmed and an additional 30 scheduled, their powerful reflections will hold a permanent place in history at the Library of Congress. This effort gained praise from HHS Veterans and will have a positive impact on their attrition rates as HHS promotes and celebrates their Veterans.

Department of Homeland Security (DHS)

DHS adopted a diversity advocate performance standard for all SES and equivalent level employees two years ago and is enhancing performance management by ensuring consistent review and assessment. The Executive Director for Diversity and Inclusion, Office of the Chief Human Capital Officer and the Deputy Officer for the Office for Civil Rights and Civil Liberties review the Senior Executive Service (SES) diversity advocate performance standard.

Department of Housing and Urban Development (HUD)

The Department of Housing and Urban Development has established a Diversity Council that includes representatives from all of the major Program Offices, Affinity Groups, and Unions. Senior Executives at the highest levels of leadership are engaged to ensure the Department's commitment is upheld to celebrate the diversity of its employees. HUD has used state-of-the-art technology by offering webinars, with high quality content, to reach supervisors across the country to provide diversity awareness training. Representatives have participated in outreach recruitment efforts to market opportunities with the Department to a diverse pool of applicants.

Department of Interior (DOI)

The Department of the Interior established a *Diversity Change Agent* program to affect and mobilize a critical mass of stakeholders to embrace and enact its *Inclusive Workplace Strategy*. Participants in the program include influential leaders who have enormous credibility from a mission standpoint. The agents are trained to assist in efforts to educate the workforce on diversity and inclusion as mission critical imperatives. The agents are serving as catalysts for change and they are successfully drawing the workforce into the inclusivity debate. They are also effectively positioning diversity and inclusion as strategic opportunities as opposed to requirements or mandates.

Department of Justice (DOJ)

In 2011, DOJ's Office of Justice Programs (OJP) partnered with the Partnership for Public Service (PPS) on a collaborative pilot program to design and deploy a strategy to effectively recruit and hire interns with disabilities while assisting hiring managers in identifying and overcoming attitudinal barriers or concerns. Building off of existing diversity and inclusion processes, OJP's Disability Hiring

Initiative (FedRecruit) was designed to educate and engage hiring managers, work with campus service providers and disability awareness advocacy groups, and explore what attracts students to Federal service and what is necessary to make their experience a success.

Department of Labor (DOL)

The Department of Labor's Employee Benefits Security Administration (EBSA) Diversity Committee implemented a successful outreach strategy that is fostering greater workforce diversity. In FY 2010, EBSA established a relationship with Howard University Law School, a Historically Black University, through which EBSA senior employees taught a course on the Employee Retirement Income Security Act of 1974, which introduced students to employee benefits law as a potential career choice. A similar partnership with Southwestern Law School in Los Angeles, California, a law school recognized for its diverse student population, was established in 2012. These partnerships have enhanced the diversity of EBSA's candidate pools for both student and entry-level positions.

Department of State

At the Department of State, the Secretary and the Director General have mandated that the opportunity for mentoring be provided at all levels. They have four programs: Civil Service (CS) mentoring, Foreign Service (FS) mentoring, situational mentoring, and Locally Employed Staff situational mentoring. In its tenth year, the CS program has grown to over 400 participants per year while during this same period 6,701 entry-level generalists and specialists (85% of all new hires) have been paired in the Foreign Service mentoring program. The situational mentoring programs have over 600 volunteer mentors available every year to any employee in need.

Department of Treasury

Women in Finance Series: To support Treasury's human capital strategic goal to recruit and hire a highly skilled and diverse workforce, Treasury, under the auspices of the Treasurer, sponsored the first ever "*Women in Finance"* Symposium on March 29, 2010, during Women's History Month. The Symposium consisted of two panel discussions and presentations from senior administrative officials and women leaders in the financial sector, described by Time Magazine as *"The New Sheriffs of Wall Street, The Women Charged With Cleaning Up The Mess."* The article highlighted opening comments from Treasury's Secretary, Timothy Geithner, and the extraordinary careers of the Symposium panelists. Accordingly, the Department of the Treasury became the only agency whose Women's History Month event was featured on the cover of a national publication.

The goal of the Symposium was to recognize the contributions of women in all economic agencies and to discuss the best means to foster success among future generations of women in public and private finance. Additionally, as part of the

Symposium, senior staff from the Treasury and the White House moderated working lunches with Symposium participants discussing the future of women in finance, best practices in particular organizations, recommendations for young women entering finance, and development of concrete ideas about how the Federal Government can attract top women from the financial sector into public service.

While the event was by invitation only, business students at a number of universities across the country as well as employees throughout the Federal and private sector watched the event live on CSPAN or through the Treasury website and submitted questions to panelists through Twitter and email. The Departments of Energy and Education, among others, reported hosting watch parties.

On July 12, 2011, the Treasurer hosted a second "*Women in Leadership Symposium*." This symposium focused on the role that institutional investors play in the economic recovery to create local jobs, bring liquidity to markets and spur long-term growth and innovation. Specifically highlighted was the role that women are playing in the institutional investment space, with women in senior positions at domestic public pension funds, corporate pension funds, savings plans, foundations, and endowments. These women are managing well over $2 trillion worth of assets in the United States, and many of them were recent appointees who had not been widely publicized or recognized.

Development of an EEO and Diversity Competencies Model: An EEO Competencies Team has been charged with strategically developing a model for addressing gaps in EEO Human Capital competencies within the Department of the Treasury. The Team's analyses of numerous competencies within the various areas of Human Capital revealed that there are competency and skills gaps on both the macro level (Department-wide) and on the micro-level (bureau-specific), within each of these areas. As a result of these findings, Competencies Project Teams were developed to address these gaps and inconsistencies.

Department of Veterans Affairs (VA)

VA has developed two new indices to efficiently measure workforce diversity and workplace inclusion in the Federal sector. The Diversity Index measures aggregate workforce diversity by race, ethnicity, and gender (REG) as compared to the Civilian Labor Force (CLF). It is a percentage value that represents the mean ratio of each demographic group relative to its corresponding CLF group. The Inclusion Index measures organizational inclusion based on employee perceptions as reported in the Federal Employee Viewpoint Survey (EVS). This index represents the mean percentage of favorable responses to 20 empirically validated survey items relating to workplace inclusion as broadly defined (including but not limited to REG issues). Both metrics are based on valid, defensible benchmarks; are scalable to various organizational parameters; and

are applicable government-wide. These Indices have proven to be an efficient approach to track diversity and inclusion and drive organizational performance.

Environmental Protection Agency (EPA)

The U.S. Environmental Protection Agency launched a Diversity Dashboard as a robust performance measurement and reporting tool for promoting workplace diversity and inclusion. The quarterly Dashboard reports synthesize comprehensive Regional and Program Office diversity data on all EPA employees, including specific employee demographics. The multiple easy to read drill-down and high-level graphic view capabilities have proven invaluable in workforce and strategic planning, benchmarking and assessing the continuing effectiveness of diversity and inclusion efforts. The Dashboard also provides transparency for open dialogue and communications for pursuing efforts to foster a diverse and inclusive work environment.

Equal Employment Opportunity Commission (EEOC)

In response to the recent Federal Employee Viewpoint results, the EEOC launched its BEST Initiative (Building Employee Satisfaction Together) to focus on strategies for improving employee satisfaction. BEST has its own site on EEOC's intranet and its own e-mailbox for employees to send in suggestions or feedback to be evaluated and considered for implementation. The initial focus of BEST will be in the following areas: Reprisal, Workplace Health & Safety, and Skill Development & Workload Management. Improvement in the above areas will help to improve the work environment, and by extension, promote diversity and inclusion.

Export-Import Bank

The Export-Import Bank began implementation of a Rotational Program in FY 2011, which is designed to encourage job development by having participants engage in work activities of a different organizational division. The rotation cycle is for a period of 120 days, and affords program participants an opportunity to gain a new knowledge base/skillset while also gaining a broader understanding of the organization. As part of the program, individual development plans are developed as a means for targeting technical and developmental benchmarks.

Farm Credit Administration

The Farm Credit Administration adopted a final rule on operating and strategic business planning to require that Farm Credit System institutions develop human capital and marketing plans that promote diversity and inclusion. The human capital plan must contain an assessment of the strengths and weaknesses of the institution's workforce and management and a description of the institution's succession programs for its workforce and management. The marketing plan must contain strategies and action for marketing the institution's products and

services to all eligible and creditworthy persons, including outreach to foster diversity and inclusion within each market segment.

Federal Energy Regulatory Commission

Office of the Executive Director's FARM Team: In an effort to foster improved professional relationships within the Office of the Executive Director (OED) and to ensure staff is informed of OED priorities, the FARM (Fun, Activities, Recognition and Morale) team, a diverse cross section of volunteers, was formed to build a more unified (collaborative) informed organization with a common sense of identity and mission. The FARM Team coordinates and implements activities in support of these broad objectives. A few examples of activities are: Employee Feedback Forums; Social luncheons and after-hour events; Agency Mission-related Activities: Executive Director meet and greets, FERC field trips; Team Building coordination at OED's All-Hands meetings; and Employee Recognition Programs.

Council for Workforce Improvement: The Council for Workforce Improvement (CWI) is a staff-led initiative formed to advise Commission leadership at all levels on workplace diversity and professional development issues at all stages of the employee career cycle. The Council's mission is to foster a highly skilled inclusive workplace where diversity and individual strengths are developed, valued, and utilized by the Commission to advance the public interest. The Council serves as a source of input to Commission leadership regarding recruiting strategies to attract and select a qualified, diverse workforce and development opportunities for existing staff, including training, performance measurement, leadership development, and promotion policies.

Federal Mediation and Conciliation Service (FMCS)

As a best practice, the Federal Mediation & Conciliation Service ensures that all employees are involved in the planning and execution of special emphasis programs. If employees have specialties (talent, planning, procurement, public speaking), the agency utilizes those specialties to enhance the programs. In addition to having the Agency Director, Deputies, and the Chief Financial Officer (CFO) open and close the programs, the agency asks FMCS employees to participate in the development and presentation of the programs. The programs belong to *all* of the employees. When they are involved early in the process, and serve in key roles, they are more likely to continue to participate and encourage other employees to "get involved" as well. FMCS is a small, yet inclusive agency with a sense of belonging and great morale.

Federal Trade Commission (FTC)

The FTC's inaugural Diversity Summit, *Beyond the Numbers: Creating an Inclusive Environment*, included panel discussions from recognized experts and leaders in the area of diversity. It was followed by a Diversity Town Hall, which provided an opportunity for discussion among the Commissioners and employees about

diversity and inclusion. At the Town Hall, the agency's Diversity Council and EEO Director provided information on activities and our demographic data. These are examples of FTC's efforts to create and sustain an environment that values different points of view, recognizes individuals' contributions, and promotes inclusion.

National Aeronautics and Space Administration (NASA)

NASA has established a fully realized presence for diversity and inclusion (D&I), as well as equal employment opportunity (EEO), in the Agency's Strategic Plan and Performance and Accountability reporting structure. Through a strong partnership between the Agency Offices of Diversity and Equal Opportunity and Human Capital Management, NASA has specific and measurable outcomes and performance goals for D&I. NASA also established an agency D&I Strategic Partnership, inclusive of the full spectrum of senior leadership positions, to better ensure diverse inputs into D&I decision-making and fully shared accountability, as well as to create sustainability through an institutionalized D&I structure.

National Archives and Records Administration (NARA)

At the National Archives, the agency believes that a manager who values diversity and exhibits inclusive behaviors will more naturally select, collaborate with, and retain diverse talent. Therefore, NARA is building "inclusion competency" into the selection processes for managers and supervisors. Specifically, NARA is building diversity and inclusion-focused questions into the structured interviewing process for manager and supervisor positions. NARA is developing competency-based behavioral interview questions and evaluation standards that assess how candidates' past actions demonstrate experience and skill in managing diverse teams and fostering an inclusive work environment.

National Science Foundation (NSF)

NSF uses training opportunities on implicit bias as an excellent example of the link between mission focus and internal diversity and inclusion. The concept of implicit bias comes out of NSF-sponsored research in the social and behavioral sciences. The purpose of the training is to provide knowledge of how unconscious biases can affect the diversity of the NSF workforce and its grantees. While initially used for panelists evaluating grant proposals, recently the training has been broadened to address implicit bias in evaluation processes, inclusive of the selection process. As part of a pilot initiative, the training discusses ways in which implicit bias can impact one's decision-making process, particularly in making selections for higher-level positions, which is where it has the most significant underrepresentation. The pilot is part of a partnership between the Office of Diversity and Inclusion, Human Resource Management, and the Directorate for Engineering that also builds on continuing interactions between the directorate and its community through professional societies. The pilot will be expanded to other NSF directorates and offices.

Nuclear Regulatory Commission (NRC)

Annually and jointly, the Directors of the Office of the Chief Human Capital Officer and the Office of Small Business and Civil Rights provide a formal briefing to the Chairman and Commissioners of the NRC. These highly successful briefings provide an opportunity to update senior executives on progress made on topics relating to the agency's most valuable resource, the people. Topics include civil rights program updates, workforce data, organizational assessments, performance management, and diversity and inclusion. The meeting is open to all staff, and participation is encouraged. The meeting is broadcast out to the agency's regional offices as well.

Office of the Director of National Intelligence (ODNI)

The ODNI's workforce development approach focuses on highlighting opportunities for career development, ensuring structured and inclusive processes for selecting employees for these opportunities, increasing communication between management and the workforce, and fostering a professionally diverse, highly skilled workforce. A cornerstone of this approach is the development of Career Advisory Boards (CAB) comprised of senior leadership from ODNI components, under the governance of the Executive Review Board. CABs are responsible for managing their employees as a corporate asset; providing them with career path information, mentoring, and feedback to plan their professional growth; and helping employees navigate their careers. Taking a holistic look at each employee, CABs ensure each individual is fairly considered for training, assignments, professional development, promotion, pay and performance bonuses.

In addition, with the agency's focus on intelligence integration and the need to leverage the full range of the Community's diverse talent, ODNI created a Civilian Joint Manning Document to optimize staff composition, integrate Community expertise, and tailor core-contracting resources.

The Civilian Joint Manning Document (CJMD) process is the protocol for outlining the ODNI organizational structure that is aligned with the budget and Full Time Equivalent (FTE) allocations. It provides the mechanism for ongoing management of the civilian cadre structure. Further, it provides for the refreshing of ideas and talent from across the IC by identifying specific positions available for detailees through rotational assignments from the other IC elements.

Office of Navajo and Hopi Indian Relocation

To cultivate a supportive, welcoming, inclusive and fair work environment, the Office of Navajo and Hopi Indian Relocation utilizes workplace policies that encourage employee engagement and empowerment including, alternative work schedules, wellness programs, training needs, and support of employee needs to balance work and life issues.

Office of Personnel Management (OPM)

Knowledge Transfer: The OPM recognizes that knowledge constitutes a valuable intangible asset for sustaining high performance and organizational effectiveness. In order to address the potential loss of organizational knowledge when individuals retire or leave the agency, OPM is implementing a comprehensive knowledge transfer strategy that includes the development of a video based, knowledge capture system that allows individuals in strategic positions to outline key aspects of their jobs/careers and the way they performed their work, including tacit and explicit knowledge.

Railroad Retirement Board (RRB)

One of RRB's best practices is the utilization of technology to provide diversity and EEO compliance information to employees. Video training modules are produced via the RRB's in-house multimedia presentation system. The RRB's version of "YouTube" is a cost effective way to deliver a variety of diversity related programming, as well as training on anti-discrimination laws. The system is accessed through the agency's intranet, which allows employees to conveniently view a program at their workstations. Using the system also ensures that the delivery of the information is consistent.

Small Business Administration (SBA)

SBA's best practice for diversity and inclusion is the addition of a diversity statement in Human Capital (HC) policies. It demonstrates commitment to meritorious practices in talent acquisition and HC management, and reads:
It is SBA's policy to uphold merit systems principles and implement [the particular topic] fairly and equitably without discrimination for any non-merit reason such as race, color, religion, age, gender, national origin, political affiliation, sexual orientation, marital or family status, personal favoritism, membership or non-membership in an employee organization or holding office in an employee organization. SBA provides reasonable accommodation to applicants and employees with disabilities.

Social Security Administration (SSA)

SSA streamlined the process that its Human Resource professionals use to refer qualified veterans and individuals with disabilities to managers for non-competitive appointments. SSA further assists its managers and new hires with a centralized funding mechanism that is used solely to procure and train on assistive technology.

APPENDIX A: DATA NOTES

NEW HIRES AND ATTRITION NOTES

Notes about the data source

Data from...

- FY 2005 and later pulled from OPM's Enterprise Human Resources Integration Statistical Data Mart (EHRI-SDM).

Coverage is limited to Federal civilian employees with the following inclusions or exclusions:

Executive Branch exclusions:

- U.S. Postal Service
- Postal Rate Commission
- Central Intelligence Agency
- National Security Agency
- Defense Intelligence Agency
- National Geospatial-Intelligence Agency
- Office of the Director of National Intelligence
- White House Office
- Office of the Vice President
- Foreign Service Personnel at the State Department
- Tennessee Valley Authority
- Board of Governors of the Federal Reserve
- Public Health Service's Commissioned Officer Corps
- Non-appropriated fund employees
- Foreign Nationals Overseas

Legislative Branch inclusions:

- Government Printing Office
- U.S. Tax Court
- Dwight D. Eisenhower Memorial Commission
- Financial Crisis Inquiry Commission
- Ronald Reagan Centennial Commission
- Medicare Payment Advisory Commission
- U.S. - China Economic and Security Review Commission
- U.S. Commission on International Religious Freedom

Judicial Branch exclusions:

- Entirely excluded

The above represents current coverage and is subject to change over time.

Recent significant changes to coverage:

- The Bureau of Consumer Financial Protection, a component of the Federal Reserve, began reporting in March 2011.
- The Federal Bureau of Investigation did not report data on personnel actions until FY 2007.
- The State Department stopped providing data on Foreign Service Personnel in March 2006.

More information about data sources can be found at http://www.opm.gov/feddata/guidance.asp

Notes about your request

Counts include all employees in pay status, meaning work schedule, type of appointment, tenure, etc. are ignored.

UNITED STATES
OFFICE OF PERSONNEL MANAGEMENT

Office of Diversity & Inclusion

1900 E Street, NW
Washington, DC 20415

D&I/02-14

United States Government Accountability Office

GAO

February 2009

FEDERAL INFORMATION SYSTEM CONTROLS AUDIT MANUAL (FISCAM)

GAO-09-232G

United States Government Accountability Office
Washington, DC 20548

February 2009

TO AUDIT OFFICIALS, CIOS, AND OTHERS INTERESTED IN FEDERAL AND OTHER GOVERNMENTAL INFORMATION SYSTEM CONTROLS AUDITING AND REPORTING

This letter transmits the revised Government Accountability Office (GAO) *Federal Information System Controls Audit Manual* (FISCAM). The FISCAM presents a methodology for performing information system (IS) control[1] audits of federal and other governmental entities in accordance with professional standards, and was originally issued in January 1999. We have updated the FISCAM for significant changes affecting IS audits.

This revised FISCAM reflects consideration of public comments received from professional accounting and auditing organizations, independent public accounting firms, state and local audit organizations, and interested individuals on the FISCAM Exposure Draft issued on July 31, 2008 (GAO-08-1029G).

GAO would like to thank the Council of the Inspectors General on Integrity and Efficiency and the state and local auditor community for their significant input into the development of this revised FISCAM.

Summary of Major Revisions to FISCAM

The revised FISCAM reflects changes in (1) technology used by government entities, (2) audit guidance and control criteria issued by the National Institute of Standards and Technology (NIST), and (3) generally accepted government auditing standards (GAGAS),

[1]Information system (IS) controls consist of those internal controls that are dependent on information systems processing and include general controls (entitywide, system, and business process application levels), business process application controls (input, processing, output, master file, interface, and data management system controls), and user controls (controls performed by people interacting with information systems).

as presented in *Government Auditing Standards* (also known as the "Yellow Book").[2] The FISCAM provides a methodology for performing information system (IS) control audits in accordance with GAGAS, where IS controls are significant to the audit objectives. However, at the discretion of the auditor, this manual may be applied on other than GAGAS audits. As defined in GAGAS, IS controls consist of those internal controls that are dependent on information systems processing and include general controls and application controls. This manual focuses on evaluating the effectiveness of such general and application controls. This manual is intended for both (1) auditors to assist them in understanding the work done by IS controls specialists, and (2) IS controls specialists to plan and perform the IS controls audit. The FISCAM is not intended to be used as a basis for audits where the audit objectives are to specifically evaluate broader information technology (IT) controls (e.g., enterprise architecture and capital planning) beyond the context of general and business process application controls.

The FISCAM is consistent with the GAO/PCIE *Financial Audit Manual* (FAM). Also, the FISCAM control activities are consistent with the NIST Special Publication (SP) 800-53 and other NIST and OMB IS control-related policies and guidance and all SP 800-53 controls have been mapped to FISCAM.[3]

The FISCAM is organized to facilitate effective and efficient IS control audits. Specifically, the methodology in the FISCAM incorporates:

- Top-down, risk based approach that considers materiality and significance in determining effective and efficient audit procedures and is tailored to achieve the audit objectives.

[2]GAO, *Government Auditing Standards*, GAO-07-162G (Washington, D.C.: July 2007).

[3]To assist the auditor in identifying criteria that may be used in the evaluation of IS controls, Chapters 3 and 4 include references, where appropriate, to NIST SP 800-53, other NIST standards and guidance, and OMB policy and guidance. Also, Appendix IV includes a summary of the mapping of the FISCAM controls to such criteria. In addition, audit procedures in FISCAM are designed to enable the auditor to determine if related control techniques are achieved.

- Evaluation of entitywide controls and their effect on audit risk.
- Evaluation of general controls and their pervasive impact on business process application controls.
- Evaluation of security management at all levels (entitywide, system, and business process application levels).
- A control hierarchy (control categories, critical elements, and control activities) to assist in evaluating the significance of identified IS control weaknesses.
- Groupings of control categories consistent with the nature of the risk.
- Experience gained in GAO's performance and review of IS control audits, including field testing the concepts in this revised FISCAM.

As discussed above, this manual is organized in a hierarchical structure to assist the auditor in performing the IS controls audit. Chapter 3 (general controls) and Chapter 4 (business process application level controls) contain several control categories, which are groupings of related controls pertaining to similar types of risk. For each control category, the manual identifies critical elements—tasks that are essential for establishing adequate controls within the category. For each critical element, there is a discussion of the associated control activities that are generally necessary to achieve the critical element, as well as related potential control techniques and suggested audit procedures. This hierarchical structure facilitates the auditor's audit planning and the auditor's analysis of identified control weaknesses.

Because control activities are generally necessary to achieve the critical elements, they are generally relevant to a GAGAS audit unless the related control category is not relevant, the audit scope is limited, or the auditor determines that, due to significant IS control weaknesses, it is not necessary to assess the effectiveness of all relevant IS controls. Within each relevant control activity, the auditor should identify control techniques implemented by the entity and determine whether the control techniques, as designed, are sufficient to achieve the control activity, considering IS risk and the audit objectives. The auditor may be able to determine whether control techniques are sufficient to achieve a particular control activity without evaluating and testing all of the control techniques.

Also, depending on IS risk and the audit objectives, the nature and extent of control techniques necessary to achieve a particular control objective will vary.

If control techniques are sufficient as designed, the auditor should determine whether the control techniques are implemented (placed in operation) and are operating effectively. Also, the auditor should evaluate the nature and extent of testing performed by the entity. Such information can assist in identifying key controls and in assessing risk, but the auditor should not rely on testing performed by the entity in lieu of appropriate auditor testing. If the control techniques implemented by the entity, as designed, are not sufficient to address the control activity, or the control techniques are not effectively implemented as designed, the auditor should determine the effect on IS controls and the audit objectives.

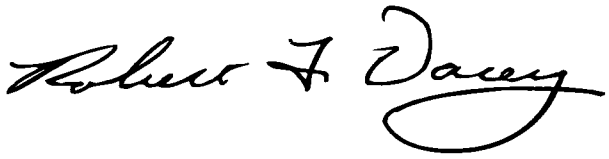
Throughout the updated FISCAM, revisions were made to reflect today's networked environment. The nature of IS risks continues to evolve. Protecting government computer systems has never been more important because of the complexity and interconnectivity of systems (including Internet and wireless), the ease of obtaining and using hacking tools, the steady advances in the sophistication and effectiveness of attack technology, and the emergence of new and more destructive attacks.

In addition, the FISCAM includes narrative that is designed to provide a basic understanding of the methodology (Chapter 2), general controls (Chapter 3) and business process application controls (Chapter 4) addressed by the FISCAM. The narrative may also be used as a reference source by the auditor and the IS control specialist. More experienced auditors and IS control specialists may find it unnecessary to routinely refer to such narrative in performing IS control audits. For example, a more experienced auditor may have sufficient knowledge, skills, and abilities to directly use the control tables in Chapters 2 and 3 (which are summarized in Appendices II and III).

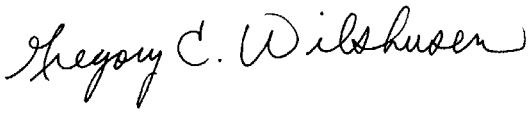
A summary of significant changes to FISCAM from the prior version is presented on pages 6-10.

Future updates to the FISCAM, including any implementation tools and related materials, will be posted to the FISCAM website at http://www.gao.gov/special.pubs/fiscam.html.

The revised FISCAM is available only in electronic form at http://www.gao.gov/products/GAO-09-232G on GAO's Web page. This version supersedes previously issued versions of the FISCAM through January 2001. Should you need additional information, please contact us at FISCAM@gao.gov or call Robert Dacey at (202) 512-7439 or Greg Wilshusen at (202) 512-6244. GAO staff who made key contributions to the FISCAM are listed on page 15.



Robert F. Dacey
Chief Accountant



Gregory C. Wilshusen
Director, Information
Security Issues

Attachment and enclosures

SUMMARY OF SIGNIFICANT CHANGES TO THE FISCAM[4]

Chapter 1

- Expanded purpose
  - provide guidance for performing effective and efficient Information System (IS) controls audits, either alone or as part of a performance audit, a financial audit, or an attestation engagement, including communication of any identified IS control weaknesses; and
  - inform financial, performance, and attestation auditors about IS controls and related audit issues, so that they can (1) plan their work in accordance with Generally Accepted Government Auditing Standards (GAGAS) and (2) integrate the work of IS controls specialists with other aspects of the financial or performance audit or attestation engagement.

- Conformity with July 2007 Revision to *Government Auditing Standards* – ("Yellow Book")(GAGAS), including information system control categories

- Conformity with AICPA auditing standards, including new risk standards

- An overall framework of IS control objectives (see summary on pages 11-13)

[4]This section summarizes significant changes to the FISCAM since the prior version.

- IS audit methodology consistent with GAGAS and FAM, including planning, testing, and reporting phases (see a summary of methodology steps on pages 14-15), which incorporates:
  - A top-down, risk-based evaluation that considers materiality and significance in determining effective and efficient audit procedures (the auditor determines which IS control techniques are relevant to the audit objectives and which are necessary to achieve the control activities; generally, all control activities are relevant unless the related control category is not relevant, the audit scope is limited, or the auditor determines that, due to significant IS control weaknesses, it is not necessary to test all relevant IS controls).
  - An evaluation of entitywide IS controls and their effect on audit risk, and therefore on the extent of audit testing (effective entitywide IS controls can reduce audit risk, while ineffective entitywide IS controls result in increased audit risk and generally are a contributory cause of IS control weaknesses at the system and business process application levels).
  - An evaluation of general controls and their pervasive impact on business process application controls (effective general controls support the effectiveness of business process application controls, while ineffective general controls generally render business process application controls ineffective).
  - An evaluation of security management at all levels of control —entitywide, system (includes networks, operating systems, and infrastructure applications), and business process application levels.
  - A control hierarchy (control categories, critical elements, and control activities) to assist in evaluating the significance of identified IS control weaknesses (if a critical element is not achieved, the respective control category is not likely to be achieved; if one of the nine control categories are not effectively achieved, IS controls are ineffective, unless other factors sufficiently reduce the risk).

- Groupings of control categories consistent with the nature of the risk.

- Change from "installation level" general controls to "system level" general controls to reflect the logically networked structure of today's systems

- IS controls audit documentation guidance for each audit phase

- Additional audit considerations that may affect an IS audit, including:
  - information security risk factors
  - automated audit tools
  - sampling techniques

Chapter 3

- Reorganized general control categories, consistent with GAGAS:
  - Security management - broadened to consider statutory requirements and best practices
  - Access controls - restructured to incorporate system software, eliminate redundancies, and facilitate IS auditing in a networked environment:
    - System boundaries
    - Identification and authentication
    - User authorization
    - Sensitive system resources
    - Audit and monitoring
    - Physical security
  - Configuration management - broadened to include network components and applications
  - Segregation of Duties - relatively unchanged
  - Contingency Planning - updated for new terminology

- Updated general control activities that (1) are consistent with current NIST and OMB information security guidance (including all NIST SP 800-53 controls) including references/mapping of each critical element to such guidance, and (2) consider new IS risks and audit experience

Chapter 4

- Audit methodology and IS controls for business process applications that (1) are consistent with GAGAS and current NIST and OMB information security guidance (including all NIST Special Publication 800-53 controls) including references/mapping to such guidance, and (2) consider new IS risks and audit experience:
  - Application security (formerly general controls at the application level)
  - Business process controls related to the validity, completeness, accuracy, and confidentiality of transactions and data during application processing
    - Transaction data input
    - Transaction data processing
    - Transaction data output
    - Master file data setup and maintenance
  - Interface controls
  - Data management systems controls

Appendices

- Expanded appendices to support IS audits
  - Updated information system controls audit planning checklist
  - Tables for summarizing the results of the IS audit
  - Mapping of FISCAM to NIST Special Publication 800-53 and other related NIST publications
  - Knowledge, skills, and abilities needed to perform IS audits
  - Scope of an IS audit in support of a financial audit
  - Entity's use of service organizations
  - Application of FISCAM to Single Audits
  - Application of FISCAM to FISMA
  - Information System Controls Audit Documentation
  - Updated Glossary

INFORMATION SYSTEM CONTROLS OBJECTIVES

GENERAL CONTROLS

Security Management

Controls provide reasonable assurance that security management is effective, including effective:

- security management program
- periodic assessments and validation of risk,
- security control policies and procedures,
- security awareness training and other security-related personnel issues,
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices,
- remediation of information security weaknesses, and
- security over activities performed by external third parties.

Access Controls

Controls provide reasonable assurance that access to computer resources (data, equipment, and facilities) is reasonable and restricted to authorized individuals, including effective

- protection of information system boundaries,
- identification and authentication mechanisms,
- authorization controls,
- protection of sensitive system resources,
- audit and monitoring capability, including incident handling, and
- physical security controls.

Configuration Management

Controls provide reasonable assurance that changes to information system resources are authorized and systems are configured and operated securely and as intended, including effective

- configuration management policies, plans, and procedures,
- current configuration identification information,
- proper authorization, testing, approval, and tracking of all configuration changes,
- routine monitoring of the configuration,
- updating software on a timely basis to protect against known vulnerabilities, and
- documentation and approval of emergency changes to the configuration.

Segregation of Duties

Controls provide reasonable assurance that incompatible duties are effectively segregated, including effective

- segregation of incompatible duties and responsibilities and related policies, and
- control of personnel activities through formal operating procedures, supervision, and review.

Contingency Planning

Controls provide reasonable assurance that contingency planning (1) protects information resources and minimizes the risk of unplanned interruptions and (2) provides for recovery of critical operations should interruptions occur, including effective

- assessment of the criticality and sensitivity of computerized operations and identification of supporting resources,
- steps taken to prevent and minimize potential damage and interruption,
- comprehensive contingency plan, and
- periodic testing of the contingency plan, with appropriate adjustments to the plan based on the testing.

BUSINESS PROCESS APPLICATION CONTROLS

Completeness – controls provide reasonable assurance that all transactions that occurred are input into the system, accepted for processing, processed once and only once by the system, and properly included in output.

Accuracy – controls provide reasonable assurance that transactions are properly recorded, with correct amount/data, and on a timely basis (in the proper period); key data elements input for transactions are accurate; data elements are processed accurately by applications that produce reliable results; and output is accurate.

Validity – controls provide reasonable assurance (1) that all recorded transactions and actually occurred (are real), relate to the organization, are authentic, and were properly approved in accordance with management's authorization; and (2) that output contains only valid data.

Confidentiality – controls provide reasonable assurance that application data and reports and other output are protected against unauthorized access.

Availability – controls provide reasonable assurance that application data and reports and other relevant business information are readily available to users when needed.[5]

[5]Availability controls are principally addressed in application security controls (especially contingency planning) and therefore, are not included as specific controls in the business process controls (BP), interface controls (IN), and data management system controls (DA) categories in Chapter 4.

IS AUDIT METHODOLOGY STEPS

Plan the Information System Controls Audit

- Understand the Overall Audit Objectives and Related Scope of the Information System Controls Audit
- Understand the Entity's Operations and Key Business Processes.
- Obtain a General Understanding of the Structure of the Entity's Networks
- Identify Key Areas of Audit Interest
- Assess Information System Risk on a Preliminary Basis
- Identify Critical Control Points
- Obtain a Preliminary Understanding of Information System Controls
- Perform Other Audit Planning Procedures
  - Relevant Laws and Regulations
  - Consideration of the Risk of Fraud
  - Previous Audits and Attestation Engagements
  - Audit Resources
  - Multiyear Testing Plans
  - Communication with Entity Management and Those Charged with Governance
  - Service Organizations
  - Using the Work of Others
  - Audit Plan

Perform Information System Controls Audit Tests

- Understand Information Systems Relevant to the Audit Objectives
- Determine which IS Control Techniques are Relevant to the Audit Objectives
- For each Relevant IS Control Technique Determine Whether it is Suitably Designed to Achieve the Critical Activity and has been Implemented

- Perform Tests to Determine Whether such Control Techniques are Operating Effectively
- Identify Potential Weaknesses in IS Controls and Consider Compensating Controls

Report Audit Results

- Evaluate the Effects of Identified IS Control Weaknesses
  - Financial Audits, Attestation Engagements, and Performance Audits
- Consider Other Audit Reporting Requirements and Related Reporting Responsibilities

KEY GAO CONTRIBUTORS

GAO staff who made key contributions to the FISCAM include: Lon C. Chin, Debra M. Conner, David B. Hayes, Jeffrey L. Knott, David F. Plocher, John A. Spence, and Charles M. Vrabel.

Contents

Appendices

Figures

Tables

Chapter 1. Introduction

1.0 Chapter 1 Overview

This manual provides a methodology for performing information system (IS) control audits in accordance with "generally accepted government auditing standards" (GAGAS), as presented in *Government Auditing Standards* (also known as the "Yellow Book").[6] However, at the discretion of the auditor, this manual may be applied on other than GAGAS audits. As defined in GAGAS, IS controls consist of those internal controls that are dependent on information systems processing and include general controls and application controls. This manual focuses on such general and application controls.

As computer technology has advanced, federal agencies and other government entities have become dependent on computerized information systems to carry out their operations and to process, maintain, and report essential information. Virtually all federal operations are supported by automated systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Hence, ineffective IS controls can result in significant risk to a broad array of government operations and assets. For example,

- resources, such as payments and collections, could be lost or stolen;
- computer resources could be used for unauthorized purposes, including the launching of attacks on others;
- sensitive information, such as taxpayer data, Social Security records, medical records, other personally identifiable information, and proprietary business information, could be inappropriately added, deleted, read, copied, disclosed, or

[6]GAO, *Government Auditing Standards*, GAO-07-162G (Washington, D.C.: July 2007).

modified for purposes such as espionage, identity theft, or other types of crime;

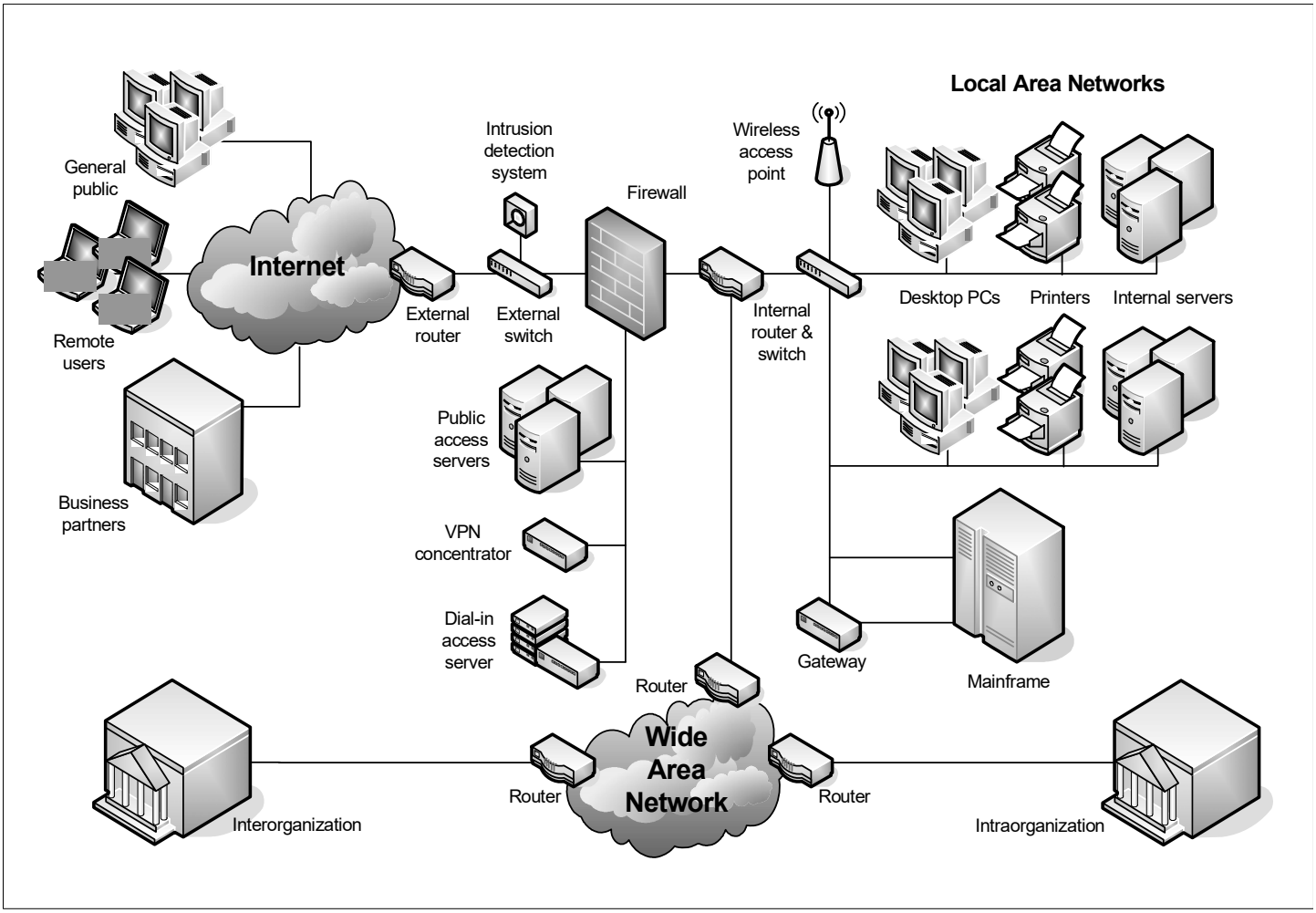
- critical operations, such as those supporting national defense and emergency services, could be disrupted;
- data could be modified or destroyed for purposes of fraud or disruption; and
- entity missions could be undermined by embarrassing incidents that result in diminished confidence in an entity's ability to conduct operations and fulfill its responsibilities.

The nature of IS risks continues to evolve. Protecting government computer systems has never been more important because of the complexity and interconnectivity of systems (including Internet and wireless), the ease of obtaining and using hacking tools, the steady advances in the sophistication and effectiveness of attack technology, and the emergence of new and more destructive attacks.

As a result, the reliability of computerized data and of the systems that process, maintain, and report these data is a major concern to managements of government entities and their auditors. Auditors may need to evaluate the effectiveness of information system controls over data supporting financial statements or data used to analyze specific program costs and outcomes. In addition, auditors may be called on to evaluate the effectiveness of IS controls to help reduce the risk due to errors, fraud, and other illegal acts and disasters or other incidents that cause the systems to be unavailable.

Figure 1 illustrates the potential complexity of a typical networked infrastructure. Such infrastructures are built upon multiple hosts, including desktop personal computers (PCs), servers, and mainframes. Data communications links and network devices such as routers, hubs, and switches enable the hosts to communicate with one another through local area networks (LANs) within entities. Wide area networks (WANs) connect LANs at different geographical locations. Moreover, entities are typically connected to the Internet.

Figure 1. An Example of Typical Networked Systems



Sources: GAO analysis and Visio.

1.1 Purpose and Anticipated Users of the Manual

This manual describes (1) an audit methodology for assessing the effectiveness of IS controls, and (2) the IS controls that auditors evaluate when assessing the confidentiality, integrity, and availability of information and information systems. The Federal Information System Controls Audit Manual (FISCAM) is designed to be used primarily on financial and performance audits and attestation engagements performed in accordance with "generally accepted government auditing standards" (GAGAS), as presented in *Government Auditing Standards* (also known as the "Yellow Book"). However, at the discretion of the auditor, this manual may be applied on other than GAGAS audits. This manual is intended for both (1) auditors performing financial and performance audits and attestation engagements to assist them in understanding the work done by IS controls specialists, and (2) IS controls specialists to plan and perform the IS controls audit. Federal and other government auditors may use this manual. It is not an auditing standard and it would be incorrect to refer to it as a standard. Its purposes are to

- provide guidance for performing effective and efficient IS controls audits, either alone or as part of a performance audit, a financial audit, or an attestation engagement, including communication of any identified IS control weaknesses; and
- inform financial, performance, and attestation auditors about IS controls and related audit issues, so that they can (1) plan their work in accordance with GAGAS and (2) integrate the work of IS controls specialists with other aspects of the financial or performance audit or attestation engagement.

The auditor should determine whether IS controls are relevant to the audit objectives. IS controls generally are relevant to a financial audit, as financial information is usually processed by information systems. For financial audits, the GAO/PCIE Financial Audit Manual

(FAM)[7] provides a framework for evaluating IS controls as part of a financial audit. The scope of an information system controls audit in support of a financial audit is summarized in Appendix VI. For performance audits, GAGAS 7.27 states that auditors should determine which audit procedures related to information system controls are needed to obtain sufficient, appropriate evidence to support the audit findings and conclusions.[8] This GAGAS paragraph provides factors that may assist auditors in making this determination.

This manual lists specific control activities and techniques and related suggested audit procedures. These are described at a high level and assume some level of expertise for an auditor to perform these audit procedures effectively. Accordingly, the auditor, applying judgment, should develop more detailed audit steps and tailor control activities based on the specific software and control techniques employed by the entity, the audit objectives, and significant areas of audit interest. Further, the auditor is responsible for identifying any necessary changes to IS control-related criteria, including changes to control activities and techniques, based on publications issued after December 2008. Future updates to the FISCAM, including any implementation tools and related materials, will be posted to the FISCAM website at http://www.gao.gov/special.pubs/fiscam.html.

As used in the FISCAM, "federal entities" refers to those entities that are subject to the specific law or regulation cited in the related discussion (e.g., Federal Information Security Management Act, Federal Financial Management Improvement Act, Federal Managers' Financial Integrity Act).

[7]The GAO/PCIE Financial Audit Manual (FAM) provides a framework for performing IS control audits performed as part of a financial audit. This framework is summarized in Appendix VI. The FAM is a joint effort between GAO and the President's Council on Integrity and Efficiency (PCIE) to provide a methodology for performing financial audits that meets professional standards. It can be viewed or downloaded at http://www.gao.gov/special.pubs/gaopcie/.

[8]In addition, GAO guidance, "Assessing the Reliability of Computer-Processed Data" (Washington, DC; October 2002) can be used to assist the auditor in determining the use of IS control audits in assessing data reliability in a performance audit.

In addition, the FISCAM includes narrative that is designed to provide a basic understanding of the methodology (Chapter 2), general controls (Chapter 3) and business process application controls (Chapter 4) addressed by the FISCAM. The narrative may also be used as a reference source by the auditor and the IS control specialist. More experienced auditors and IS control specialists may find it unnecessary to routinely refer to such narrative in performing IS control audits. For example, a more experienced auditor may have sufficient knowledge, skills, and abilities to directly use the control tables in Chapters 2 and 3 (which are summarized in Appendices II and III).

Further, many of the suggested audit procedures start with the word "review." The intent of such language is for the auditor to do more than simply look at the subject to be reviewed. Rather, a critical evaluation is envisioned, in which the auditor uses professional judgment and experience and undertakes the task with a certain level of skepticism, critical thinking, and creativity.

Although IS controls audit work, especially control testing, is generally performed by an IS controls specialist, financial or performance auditors with appropriate training, expertise, and supervision may undertake specific tasks in this area of the audit. Throughout this manual, the term "auditor" means either (1) an IS controls specialist or (2) a financial or performance auditor working in consultation with or under the supervision of an IS controls specialist. The FISCAM may be used by other staff that possess adequate IT competence. GAGAS requires that staff assigned to conduct an audit must collectively possess the technical knowledge, skills, and experience necessary to be competent for the type of work being performed. See Appendix V for additional information on the knowledge, skills, and abilities needed to perform information system control audits.

The following terms are used in the FISCAM to describe the degree of responsibility they impose on auditors and audit organizations:

- **must** - Auditors and audit organizations are required to comply with this unconditional requirement in all cases in which the circumstances exist to which the unconditional requirement applies. The term "must" is used only in FISCAM when the related requirement is specified as a "must" in GAGAS.

- **should** – Auditors and audit organizations are also required to comply with this presumptively mandatory requirement in all cases in which the circumstances exist to which the presumptively mandatory requirement applies; however, in rare circumstances, auditors and audit organizations may depart from a presumptively mandatory requirement provided they document their justification for the departure and how the alternative procedures performed in the circumstances were sufficient to achieve the objectives of the presumptively mandatory requirement. The term "should" is used when (1) the related requirement is specified as a "should" in GAGAS, or (2) performance is deemed necessary to meet GAGAS evidence requirements for an IS controls audit.

- **generally should** – Although optional, compliance with this policy is strongly encouraged

- **may** – Compliance with this procedure or action is optional. It is descriptive rather than required. It is explanatory material that provides further explanation and guidance on the professional requirements or identifies and describes other procedures or actions relating to auditors' or audit organizations' activities.

When these or similar terms are used to describe management or entity actions (rather than actions of the auditor or audit organization), the general meaning of the terms is intended. If the entity does not comply with a "must" or "should", the auditor should assess the impact of the noncompliance on the effectiveness of related IS controls.

1.2 Nature of Information System Controls

An evaluation of IS controls generally includes both general and business process application controls (also called application controls). The entity must have effective general and business process application controls to achieve the appropriate confidentiality, integrity, and availability of critical information and information systems.

Information system (IS) controls consist of those internal controls that are dependent on information systems processing and include general controls (entitywide, system, and business process application levels), business process application controls (input, processing, output, master file, interface, and data management system controls), and user controls[9] (controls performed by people interacting with information systems). General and business process application controls are always IS controls. A user control is an IS control if its effectiveness depends on information systems processing or the reliability (accuracy, completeness, and validity) of information processed by information systems. Conversely, a user control is not an IS control if its effectiveness does not depend on information systems processing or the reliability of information processed by information systems.

General controls are the policies and procedures that apply to all or a large segment of an entity's information systems and help ensure their proper operation. Examples of primary objectives for general controls are to safeguard data, protect business process application programs, and ensure continued computer operations in case of unexpected interruptions. General controls are applied at the entitywide, system, and business process application levels. The effectiveness of general controls is a significant factor in determining the effectiveness of business process application controls, which are applied at the business process application level.

[9]User controls are portions of controls that are performed by people interacting with IS controls. The effectiveness of user controls typically depend on information systems processing or the reliability of information processed by IS controls.

Without effective general controls, business process application controls can generally be rendered ineffective by circumvention or modification. For example, automated edits designed to preclude users from entering unreasonably large dollar amounts in a payment processing system can be an effective application control. However, this control is not effective (cannot be relied on) if the general controls permit unauthorized program modifications that might allow some payments to be exempted from the edits or unauthorized changes to be made to data files after the edit is performed. GAGAS paragraph 7.23 discusses the following types of general controls: security management, logical and physical access, configuration management, segregation of duties, and contingency planning. Chapter 3 discusses the general controls in an IS controls audit and provides more detail on the critical elements of each type of general control.

Business process application controls are directly related to individual computerized applications. They help ensure that transactions are complete, accurate, valid, confidential, and available[10]. Business process application controls include (1) programmed control techniques, such as automated edits, and (2) manual follow-up of computer-generated reports, such as reviews of reports identifying rejected or unusual items. GAGAS paragraph 7.23 defines application controls, or business controls, as those controls that help ensure the validity, completeness, accuracy, and confidentiality of transactions and data during application processing. Chapter 4 discusses the business process application level controls in an IS controls audit and provides more detail on the critical elements of each type of business process application control.

The overall framework of IS control objectives presented in the FISCAM can be viewed in different ways. One way to summarize the objectives is presented below.

[10]Availability controls are principally addressed in application security controls (especially contingency planning) and therefore, are not included as specific business process controls in Chapter 4.

GENERAL CONTROLS

Security Management

Controls provide reasonable assurance that security management is effective, including effective:

- security management program,
- periodic assessments and validation of risk,
- security control policies and procedures,
- security awareness training and other security-related personnel issues,
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices,
- remediation of information security weaknesses, and
- security over activities performed by external third parties.

Access Controls

Controls provide reasonable assurance that access to computer resources (data, equipment, and facilities) is reasonable and restricted to authorized individuals, including effective:

- protection of information system boundaries,
- identification and authentication mechanisms,
- authorization controls,
- protection of sensitive system resources,
- audit and monitoring capability, including incident handling, and
- physical security controls.

Configuration Management

Controls provide reasonable assurance that changes to information system resources are authorized and systems are configured and operated securely and as intended, including effective:

- configuration management policies, plans, and procedures,
- current configuration identification information,

- proper authorization, testing, approval, and tracking of all configuration changes,
- routine monitoring of the configuration,
- updating software on a timely basis to protect against known vulnerabilities, and
- documentation and approval of emergency changes to the configuration.

Segregation of Duties

Controls provide reasonable assurance that incompatible duties are effectively segregated, including effective:

- segregation of incompatible duties and responsibilities and related policies, and
- control of personnel activities through formal operating procedures, supervision, and review.

Contingency Planning

Controls provide reasonable assurance that contingency planning (1) protects information resources and minimizes the risk of unplanned interruptions and (2) provides for recovery of critical operations should interruptions occur, including effective:

- assessment of the criticality and sensitivity of computerized operations and identification of supporting resources,
- steps taken to prevent and minimize potential damage and interruption,
- comprehensive contingency plan, and
- periodic testing of the contingency plan, with appropriate adjustments to the plan based on the testing.

BUSINESS PROCESS APPLICATION CONTROLS

Completeness – controls provide reasonable assurance that all transactions that occurred are input into the system, accepted for processing, processed once and only once by the system, and properly included in output.

Accuracy – controls provide reasonable assurance that transactions are properly recorded, with correct amount/data, and on a timely basis (in the proper period); key data elements input for transactions are accurate; data elements are processed accurately by applications that produce reliable results; and output is accurate.

Validity – controls provide reasonable assurance (1) that all recorded transactions and actually occurred (are real), relate to the organization, are authentic, and were properly approved in accordance with management's authorization; and (2) that output contains only valid data.

Confidentiality – controls provide reasonable assurance that application data and reports and other output are protected against unauthorized access.

Availability – controls provide reasonable assurance that application data and reports and other relevant business information are readily available to users when needed.[11]

[11]Availability controls are principally addressed in application security controls (especially contingency planning) and therefore, are not included as specific controls in the business process controls (BP), interface controls (IN), and data management system controls (DA) categories in Chapter 4.

1.3 Determining the Nature and Extent of Audit Procedures

The nature, timing, and extent of audit procedures performed to assess IS controls vary, depending on the audit objectives, the nature and extent of IS control risks and other factors. Factors that can affect the nature, timing, and extent of audit procedures include the nature and complexity of the entity's information systems, the entity's control environment, and particular data and applications that are significant to the financial statements or operations of the entity. As appropriate, the IS controls specialist, and the financial, performance, or attestation auditor generally should work cooperatively to determine the nature, timing, and extent of IS controls audit procedures.

Inadequate coordination can result in ineffective auditing, for example, incomplete IS controls audits or improper consideration of the work performed by the IS controls specialist. When performed as part of a financial statement audit, an assessment of IS controls is part of a comprehensive effort to evaluate both the controls over and reliability of financial reporting. In performance audits and attestation engagements, the nature and extent of IS controls audit procedures vary depending on the objectives of the audit.

1.4 Organization of This Manual

This manual is organized as follows:

- Chapter 2 describes the methodology for performing the IS controls audit.
- Chapter 3 provides information concerning the five general control categories, supporting critical elements, critical activities, potential control techniques, and suggested audit procedures.
- Chapter 4 provides information concerning the four business process application control level categories, supporting critical elements, critical activities, potential control techniques, and suggested audit procedures.

- Appendices provide supplemental information to assist the auditor in applying the FISCAM methodology.

This manual provides a risk-based approach for performing the information system controls audit that is consistent with government auditing standards and the GAO/PCIE *Financial Audit Manual* (FAM).[12] The FISCAM is consistent with GAGAS and, where appropriate, the FISCAM discusses the applicable GAGAS requirements. Each of the nine control categories (five general control categories and four business process level control categories) represents a grouping of related controls having similar types of risk. For each category, this manual discusses the key underlying concepts, associated risks if the controls in the category are ineffective, and the critical elements that should be achieved for IS controls to be effective.

This organization structure facilitates the following:

- Audit planning: Related audit steps can be grouped and broken down into three primary levels: the entitywide level, the system level, and the application level.
- Evaluation of findings: The effectiveness of IS controls can be evaluated by control technique, control activity, critical element, and control category.
- Audit report drafting: Findings can be summarized by control category and critical element.

To evaluate IS controls, the auditor should use appropriate criteria that are relevant to the audit objectives. For audits of federal entities, criteria are provided by the Federal Information Security Management Act (FISMA), OMB policies and guidance, and standards and guidance issued by the National Institute of Standards and Technology (NIST). NIST has developed a risk management framework of standards and guidelines for agencies to follow in

[12]The Financial Audit Manual is a joint effort between GAO and the President's Council on Integrity and Efficiency (PCIE) to provide a methodology for performing financial audits that meets professional standards. It can be viewed or downloaded at http://www.gao.gov/special.pubs/gaopcie/.

developing information security programs. This includes, for non-national security systems, Federal Information Processing Standards Publication (FIPS Pub) 199 *Standards for Security Categorization of Federal Information and Information Systems*, FIPS Pub 200, *Minimum Security Requirements for Federal Information and Information Systems*, and NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems* and other NIST guidance[13]. The Office of Management and Budget (OMB) requires federal entities to apply NIST guidance to non-national security systems. Also, other sources, such as vendor recommended IS practices and other generally accepted IS resources, may provide criteria.[14] In addition, NIST is responsible for developing minimum security standards and guidelines that are complementary with standards and guidelines employed for the protection of national security systems and information contained in such systems. The auditor is responsible for identifying relevant IS control-related criteria issued after December 2008 and, where appropriate, criteria beyond that referred to in the FISCAM. Future updates to the FISCAM, including any implementation tools and related materials, will be posted to the FISCAM website at http://www.gao.gov/special.pubs/fiscam.html.

The critical elements and control activities are designed to be able to be applied to systems with varying level of risk. Consequently, critical elements and control activities are not differentiated by risk level. As discussed in Chapter 2, the auditor assesses IS risk based on a number of factors, including but not limited to consideration of the security categorizations assigned by management. In assessing whether the entity's control techniques are sufficient to achieve a particular control activity, the auditor considers several factors,

[13]NIST SP 800-100, *Information Security Handbook: A Guide for Managers*, provides guidance on establishing and implementing an information security program and includes certain entitywide program level controls.

[14]The Security Content Automation Program (SCAP) is a joint program of the National Security Agency (NSA), Defense Information Systems Agency (DISA), and NIST. SCAP is designed as a free, public repository of tools to be used for automating technical control compliance activities, vulnerability checking, and security measurement. Such tools can provide additional criteria. See http://nvd.nist.gov/scap/scap.cfm.

including but not limited to the level of IS risk, materiality or significance, and the audit objectives.

FISMA states that standards and guidelines for national security systems shall be developed, prescribed, enforced, and overseen as otherwise authorized by law and as directed by the President. Also, FISMA states that the head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency:

- provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system;
- implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President; and
- complies with the requirements of FISMA.

GAO has consulted with NIST, as provided for in FISMA, and all controls in NIST SP 800-53[15] are mapped to FISCAM[16]. Appendix IV provides a mapping of the FISCAM critical elements to NIST SP 800-53 and other related NIST publications. In addition, each critical element includes references to related NIST SP 800-53 controls. NIST SP 800-53 includes a table of the mapping. Also, to assist auditors, individual FISCAM control activities reference related NIST SP 800-53 controls. This manual provides additional narrative to assist the auditor in evaluating IS controls. In addition, FISCAM incorporates other NIST guidance, including, for example, NIST SP 800-100, *Information Security Handbook: A Guide for Managers*, which includes coverage of programmatic areas such as information security governance, capital planning and investment control, and system development life cycle.

[15]NIST has stated that it plans to update SP 800-53 annually.

[16]Audit procedures in FISCAM are designed to enable the auditor to determine if related control techniques are achieved.

FISCAM, which is consistent with NIST and other criteria, is organized to facilitate effective and efficient IS controls audits. Specifically, the methodology in the FISCAM incorporates:

- A top-down, risk-based evaluation that considers materiality and significance in determining effective and efficient audit procedures (the auditor determines which IS control techniques are relevant to the audit objectives and which are necessary to achieve the control activities; generally, all control activities are relevant unless the related control category is not relevant, the audit scope is limited, or the auditor determines that, due to significant IS control weaknesses, it is not necessary to test all relevant IS controls).
- An evaluation of entitywide IS controls and their effect on audit risk, and therefore on the extent of audit testing (effective entitywide IS controls can reduce audit risk, while ineffective entitywide IS controls result in increased audit risk and generally are a contributory cause of IS control weaknesses at the system and business process application levels)—NIST SP 800-53 principally relates to controls at the system and application level.
- An evaluation of general controls and their pervasive impact on business process application controls (effective general controls support the effectiveness of business process application controls, while ineffective general controls generally render business process application controls ineffective).
- An evaluation of security management at all levels of control (entitywide, system, and business process application levels).
- A control hierarchy (control categories, critical elements, and control activities) to assist in evaluating the significance of identified IS control weaknesses (if a critical element is not achieved, the respective control category is not likely to be achieved; if one of the nine control categories are not effectively achieved, IS controls are ineffective, unless other factors sufficiently reduce the risk).
- Groupings of control categories consistent with the nature of the risk.
- Experience gained in GAO's performance and review of IS control audits, including field testing the concepts in this revised FISCAM.

As discussed above, this manual is organized in a hierarchical structure to assist the auditor in performing the IS controls audit. Chapter 3 (general controls) and Chapter 4 (business process application level controls) contain several control categories, which are groupings of related controls pertaining to similar types of risk. For each control category, the manual identifies critical elements—tasks that are essential for establishing adequate controls within the category. For each critical element, there is a discussion of the associated objectives, risks, and control activities, as well as related potential control techniques and suggested audit procedures. This hierarchical structure facilitates the auditor's audit planning and analysis of identified control weaknesses.

Because control activities are generally necessary to achieve the critical elements, they are generally relevant to a GAGAS audit unless the related control category is not relevant, the audit scope is limited, or the auditor determines that, due to significant IS control weaknesses, it is not necessary to assess the effectiveness of all relevant IS controls. Within each relevant control activity, the auditor should identify control techniques implemented by the entity and determine whether the control techniques, as designed, are sufficient to achieve the control activity, considering IS risk and the audit objectives. The auditor may be able to determine whether control techniques are sufficient to achieve a particular control activity without evaluating and testing all of the control techniques. Also, depending on IS risk and the audit objectives, the nature and extent of control techniques necessary to achieve a particular control objective will vary.

If sufficient, the auditor should determine whether the control techniques are implemented (placed in operation) and are operating effectively. Also, the auditor should evaluate the nature and extent of testing performed by the entity. Such information can assist in identifying key controls and in assessing risk, but the auditor should not rely on testing performed by the entity in lieu of appropriate auditor testing. As discussed later in this section, if the control techniques implemented by the entity, as designed, are not sufficient to address the control activity, or the control techniques are not effectively implemented as designed, the auditor should determine the effect on IS controls and the audit objectives.

The entity's management is responsible for implementing an appropriate system of cost-effective IS controls, including an effective monitoring program to provide management with reasonable assurance that IS controls are properly designed and effectively operating. The auditor's responsibility is to perform tests of the IS controls and provide conclusions on the results of such tests to support the audit objectives.

Future updates to the FISCAM, including implementation tools and materials, will be posted to the FISCAM website at http://www.gao.gov/special.pubs/fiscam.html.

1.4.1 Appendices

The appendices to the FISCAM, summarized below, provide additional information to assist the auditor in performing the IS controls audit.

List of Appendices

Appendix	Description	Purpose
Appendix I	Information System Controls Audit Planning Checklist	To assist the auditor in requesting relevant background information.
Appendix II	Tables for Summarizing Work Performed in Evaluating and Testing General and Business Process Application Controls	To assist the auditor in summarizing work performed.
Appendix III	Tables for Assessing the Effectiveness of General and Business Process Application Controls	To assist the auditor in assessing and reporting on IS controls.
Appendix IV	Mapping of FISCAM to NIST SP 800-53 and Other Related NIST Publications	To show correlation of FISCAM critical elements to NIST SP 800-53 and related NIST publications.
Appendix V	Knowledge, Skills, and Abilities Needed to Perform Information System Controls Audits	Skill sets necessary to perform the IS controls audit.
Appendix VI	Scope of an Information System Controls Audit in Support of a Financial Audit	To show relation of FISCAM to relevant FAM sections.
Appendix VII	Entity's Use of Service Organizations	Audit issues related to an entity's use of a service organization and use of FISCAM as a basis for performing a SAS 70 audit.

Appendix	Description	Purpose
Appendix VIII	Application of FISCAM to Single Audits	Use of FISCAM to assess IS controls over compliance requirements and financial reporting in connection with a Single Audit.
Appendix IX	Application of FISCAM to FISMA	Use of FISCAM for the independent evaluation of a federal agency's information security program required by FISMA.
Appendix X	Information System Controls Audit Documentation	Summarizes IS controls audit documentation
Appendix XI	Glossary	Key terms used in the FISCAM.
Appendix XII	Bibliography	List of information sources.

Chapter 2. Performing the Information System Controls Audit

2.0 Introduction

The information system (IS) controls audit involves the following three phases:

- Planning: The auditor determines an effective and efficient way to obtain the evidential matter necessary to achieve the objectives of the IS controls audit and the audit report. For financial audits, the auditor develops an audit strategy and an audit plan. For performance audits, the auditor develops an audit plan.
- Testing: The auditor tests the effectiveness of IS controls that are relevant to the audit objectives.
- Reporting: The auditor concludes on the effect of any identified IS control weaknesses on the audit objectives and reports the results of the audit, including any material weaknesses and other significant deficiencies.

Appendix VI provides the scope of an IS controls audit in support of a financial statement audit.

For each of the three phases, the auditor prepares appropriate audit documentation.

In addition to the GAGAS field work and reporting standards (Chapters 4 through 8), which are generally addressed by the FISCAM, the auditor performing a GAGAS audit also should meet the requirements in Chapters 1, 2, and 3 of *Government Auditing Standards*.

2.1 Plan the Information System Controls Audit

2.1.1 Overview

In planning the IS controls audit, the auditor uses the equivalent concepts of materiality (in financial audits and attestation engagements) and significance[17] (in performance audits) to plan both effective and efficient audit procedures. Materiality and significance are concepts the auditor uses to determine the planned nature, timing, and extent of audit procedures. The underlying principle is that the auditor is not required to spend resources on items of little importance; that is, those that would not affect the judgment or conduct of a reasonable user of the audit report, in light of surrounding circumstances. On the basis of this principle, the auditor may determine that some areas of the IS controls audit (e.g., specific systems) are not material or significant, and therefore warrant little or no audit attention.

Materiality and significance include both quantitative and qualitative factors in relation to the subject matter of the audit. Even though a system may process transactions that are quantitatively immaterial or insignificant, the system may contain sensitive information or provide an access path to other systems that contain information that is sensitive or otherwise material or significant. For example, an application that provides public information via a website, if improperly configured, may expose internal network resources, including sensitive systems, to unauthorized access. Materiality is

[17] GAGAS paragraph 7.04 states that "the concept of significance assists auditors throughout a performance audit, including when deciding the type and extent of audit work to perform, when evaluating results of audit work, and when developing the report and related findings and conclusions. Significance is defined as the relative importance of a matter within the context in which it is being considered, including quantitative and qualitative factors. Such factors include the magnitude of the matter in relation to the subject matter of the audit, the nature and effect of the matter, the relevance of the matter, the needs and interests of an objective third party with knowledge of the relevant information, and the impact of the matter to the audited program or activity. Professional judgment assists auditors when evaluating the significance of matters within the context of the audit objectives."

more fully discussed in the FAM in section 230 (Determine Planning, Design, and Test Materiality), and both materiality and significance are discussed further in GAGAS.

Planning occurs throughout the audit as an iterative process. (For example, based on findings from the testing phase, the auditor may change the planned audit approach, including the design of specific tests.) However, planning activities are concentrated in the planning phase, during which the objectives are to obtain an understanding of the entity and its operations, including its internal control, identify significant issues, assess risk, and design the nature, extent, and timing of audit procedures. To accomplish this, the methodology presented in this chapter includes guidance to help the auditor do the following:

- Understand the overall audit objectives and related scope of the IS controls audit
- Obtain an understanding of an entity and its operations and key business processes
- Obtain a general understanding of the structure of the entity's networks
- Identify key areas of audit interest (files, applications, systems, locations)
- Assess IS risk on a preliminary basis
- Identify critical control points (for example, external access points to networks)
- Obtain a preliminary understanding of IS controls
- Perform other audit planning procedures

Although each of these areas is discussed separately in this chapter, they are not generally performed as discrete, sequential steps. For example, the IS controls specialist may gather information related to several steps concurrently, such as through interviews with key information technology (IT) staff or through data requests, or may perform steps in a different sequence. The auditor performs planning to determine an effective and efficient way to obtain the evidential matter necessary to support the objectives of the IS controls audit and the audit report. The nature and extent of audit

planning procedures varies for each audit depending on several factors, including the entity's size and complexity, the auditor's experience with the entity, and the auditor's knowledge of the entity's operations.

A key to a high-quality audit, the senior members of the audit team should be involved in planning. The auditor should coordinate with the entity being audited and, if the IS controls audit is part of another audit, with senior members of the overall audit team. In addition, auditors generally should determine the needs of other auditors who plan to use the work being performed and consult with them in a timely manner, especially when making decisions involving significant judgment.

If the IS controls audit is performed as part of a financial audit, GAGAS require the auditor to obtain an understanding of internal control over financial reporting sufficient to assess the risk of material misstatement of the financial statements whether due to error or fraud, and to design the nature, timing, and extent of further audit procedures based on that assessment. This includes performing risk assessment procedures to evaluate the design of controls relevant to an audit of financial statements and to determine whether they have been implemented. In obtaining this understanding, the auditor considers how an entity's use of information technology (IT) and manual procedures affect controls relevant to the audit. The auditor's responsibilities for considering internal control in a financial audit are described in more detail in the FAM.

If the IS controls audit is performed as part of an examination-level attestation engagement, the auditor should obtain a sufficient understanding of internal control that is material to the subject matter in order to plan the engagement and design procedures to achieve the objectives of the attestation engagement.

If the IS controls audit is performed as part of a performance audit, GAGAS[18] (para. 7.24) states that when information systems controls

[18]There is a section of GAGAS entitled "Information Systems Controls" (paras. 7.23-7.27)

are determined to be significant to the audit objectives, auditors should then evaluate the design and operating effectiveness of such controls. This evaluation would include other information systems controls that impact the effectiveness of the significant controls or the reliability of information used in performing the significant controls. Auditors should obtain a sufficient understanding of information systems controls necessary to assess audit risk and plan the audit within the context of the audit objectives.

Additionally, GAGAS (para. 7.27) states that auditors should determine which audit procedures related to information systems controls are needed to obtain sufficient, appropriate evidence to support the audit findings and conclusions. It also provides the following factors to assist the auditor in making this determination:

a. The extent to which internal controls that are significant to the audit depend on the reliability of information processed or generated by information systems.

b. The availability of evidence outside the information system to support the findings and conclusions: It may not be possible for auditors to obtain sufficient, appropriate evidence without assessing the effectiveness of relevant information systems controls. For example, if information supporting the findings and conclusions is generated by information systems or its reliability is dependent on information systems controls, there may not be sufficient supporting or corroborating information or documentary evidence that is available other than that produced by the information systems.

c. The relationship of information systems controls to data reliability: To obtain evidence about the reliability of computer-generated information, auditors may decide to assess the effectiveness of information systems controls as part of obtaining evidence about the reliability of the data. If the auditor concludes that information systems controls are effective, the auditor may reduce the extent of direct testing of data.

d. Assessing the effectiveness of information systems controls as an audit objective: When assessing the effectiveness of information systems controls that is directly a part of an audit objective, auditors

should test information systems controls necessary to address the audit objectives. For example, the audit may involve the effectiveness of information systems controls related to certain systems, facilities, or organizations.

2.1.2 Understand the Overall Audit Objectives and Related Scope of the Information System Controls Audit

The nature, timing, and extent of IS controls audit procedures vary depending upon the audit objectives. For example, the IS controls audit

- may be performed as part of a financial or performance audit, or may be performed as a separate engagement;
- may comprehensively address an entire entity, a component, or a network, or may narrowly target an application, specific technology (e.g., wireless, operating system, etc.), or location; and/or
- may include all control objectives or only a subset of control objectives (e.g., general controls, business process controls, or selected components of them, such as focusing on an entity's security management program).

If achieving the audit objectives does not require an overall conclusion on the effectiveness of the entity's IS controls or relates only to certain components of the entity or a subset of controls, the auditor's assessment would not necessarily identify all significant IS control weaknesses that may exist. For example, a limited review of controls over a type of operating system may not identify any significant weaknesses, although there may be very significant weaknesses in other areas that the auditor is unaware of because the scope of the audit is limited. Consequently, the auditor should evaluate the potential limitations of the auditor's work on the auditor's report and the needs and expectations of users. The auditor may determine that, because the limitations are so significant, the auditor will (1) communicate the limitations to the management of the audited entity, those charged with governance, and/or those requesting the audit, and (2) clearly report such limitations on the conclusions in the audit report. For example, in

reporting on an audit of an operating system, the auditor may determine that it is appropriate to clearly report that the scope of the assessment was limited to the operating system and that, consequently, additional IS control weaknesses may exist that could impact the effectiveness of IS controls related to the operating system and to the entity as a whole.

Based on the overall engagement objectives, the auditor should develop and document the objectives of the IS controls audit. Typical IS controls audit objectives include the following:

- To support financial statement audits by, for example, assessing the effectiveness of IS controls related to financial reporting. (Note: The assessment of IS controls generally occurs during the internal control phase of a financial statement audit.) This assessment affects the nature, timing, and extent of financial audit procedures to be performed, as well as provide timely recommendations for improvements in IS controls. In addition, it may cover the entire audit year or relate only to controls at a point in time, such as at the end of the fiscal year. The scope of an IS controls audit in support of a financial audit is described further in the FAM and in Appendix VI.
- To supplement IT performance audits by assessing the effectiveness of security within the context of a broader systems review.
- To support other performance audits, such as assessing data reliability or how well an information system protects the confidentiality, integrity, and availability of data and the effect of this level of protection on program performance.
- To determine the effectiveness of IS controls, not in support of another audit, so that any risks are identified. Such audits may be designed to provide a conclusion on the effectiveness of IS controls and describe any material weaknesses and other significant deficiencies, or merely describe any IS control weaknesses without an overall conclusion as to the effectiveness of IS controls.
- To support an evaluation of IS controls as required by FISMA.
- To support Single Audits.

The auditor should also determine and document (such as in an audit strategy and audit plan) the appropriate scope of the IS controls audit, including

- the organizational entities to be addressed (e.g., entitywide, selected component(s), etc.);
- the breadth of the audit (e.g., overall conclusion on IS control effectiveness, review of a specific application or technology area, such as wireless or UNIX, etc.);
- the types of IS controls to be tested:
- general and/or business process application level controls to be tested, or selected components; or
- all levels of the entity's information systems, or selected levels (e.g., entitywide, system level, or business process application level, or selected components of them—for definitions of each level, see the section below entitled "2.2 Perform Information System Controls Audit Tests.").

If the IS controls audit is performed as part of another audit, the auditor should understand the overall audit objectives and how the IS controls audit will integrate with the audit. The auditor should reach a common understanding of objectives with the audit team responsible for the overall audit.

2.1.3 Understand the Entity's Operations and Key Business Processes

The auditor should obtain and document an understanding of the entity sufficient to plan and perform the audit in accordance with applicable auditing standards and requirements. In planning the audit, the auditor obtains information that will provide an overall understanding of the entity, such as its mission, size and location, organization, business, strategies, risks, and internal control structure. Understanding the entity's operations in the planning process enables the auditor to identify, respond to, and resolve problems early in the audit.

The auditor's understanding of the entity includes:

- entity management and organization,
- external and internal factors affecting the entity's operations, and
- key business processes (defined below).

To plan the audit, the auditor obtains a general understanding of the entity's and the IT function's organizational structure, including key members of entity and IT management. The auditor's main objective is to understand how the entity is managed and how the organization is structured.

The auditor should identify significant external and internal factors that affect the entity's operations, particularly IT. External factors might include (1) IT budget, (2) external systems users, (3) current political climate, and (4) relevant legislation. Internal factors might include (1) size of the entity, (2) number of locations, (3) structure of the entity (centralized or decentralized), (4) complexity of operations, (5) IT management structure, (6) impact of information systems on business operations, (7) qualifications and competence of key IT personnel, and (8) turnover of key IT personnel. The auditor should document any significant factors that could affect the IS controls audit, including the auditor's risk assessment.

The auditor should also obtain a general understanding of the entity's business processes, particularly those processes most closely related to the audit objectives. Business processes are the primary functions that the entity performs in accomplishing its mission. Examples of typical business processes in government entities include

- mission-related processes, typically at the program or subprogram level, such as education, public health, law enforcement, or income security;
- financial management processes, such as collections, disbursements, or payroll; and
- other support processes, such as human resources, property management, or security.

Understanding the entity's operations and business processes includes understanding how business process applications are used to support key business processes, as it tends to vary from entity to entity. The auditor should obtain and review documentation, such as design documents, blueprints, business process procedures, user manuals, etc., and inquire of knowledgeable personnel to obtain a general understanding of each significant business process application that is relevant to the audit objectives. This includes a detailed understanding of

- business rules (e.g. removing all transactions that fail edits or only selected ones based on established criteria),
- transaction flows (detailed study of the entity's internal controls over a particular category of events that identifies all key procedures and controls relating to the processing of transactions), and
- application and software module interaction (transactions leave one system for processing by another, e.g. payroll time card interfaces with pay rate file to determine salary information).

Obtaining this understanding is essential to assessing information system risk, understanding business process application controls, and developing relevant audit procedures. For efficiency, the auditor may combine this step with the steps in FISCAM section 2.2.1 subsection entitled "Understand Information Systems Relevant to the Audit Objectives" to aid in the identification of relevant controls.

The auditor should identify and document the key business processes that are relevant to the audit objectives. For each key business process, the auditor should identify the significant general support systems and major applications that are used to support

each key business process.[19] Also, for each key business process, the auditor should identify the use of contractors and others to process information and/or operate systems for or on behalf of the entity. Throughout the remainder of this manual, references to entity systems and business processes include the use of contractors and others to process information and/or operate systems for or on behalf of the entity. If the IS controls audit is performed as part of a financial audit, as discussed in FAM 320 (Understand Information Systems) and other FAM sections, the auditor should obtain an understanding of the entity's information systems (including methods and records) for processing and reporting accounting (including supplemental information), compliance, and operations data (including performance measures reported in the Management's Discussion and Analysis).

The auditor should document an understanding of the entity's operations and key business processes, including the following items to the extent relevant to the audit objectives:

- the significance and nature of the programs and functions supported by information systems;
- a general understanding of the entity's and the IT function's organizational structure;
- key business processes relevant to the audit objectives, including business rules, transaction flows, and application and software module interaction;
- significant general support systems and major applications that support each key business process;
- background information checklist, if used;
- significant internal and external factors that could affect the IS controls audit objectives;

[19]OMB uses the terms "general support" and "application" systems to describe the two types of entity systems. As defined in OMB Circular A-130, a general support system is an interconnected set of information resources under the same direct management control that share common functionality. It normally includes hardware, software, information, data, applications, communications, and people. The term "application" means the use of information resources (information and information technology) to satisfy a specific set of user requirements.

- a detailed organization chart, particularly the IT and the IS components;
- significant changes in the IT environment or significant applications implemented within the recent past (e.g. 2 years) or planned within the near future (e.g., 2 years); and
- the entity's reliance on third parties to provide IT services (e.g., in-house, remote connectivity, remote processing).

Appendix I includes an Information System Controls Audit Planning Checklist that can be provided to the entity's management to facilitate gathering appropriate information for this audit step.

The auditor generally gathers planning information through different methods (observation, interviews, reading policy and procedure manuals, etc.) and from a variety of sources, including

- previous audits and management reviews (see section 2.1.9.C),
- top-level entity and IT management,
- entity management responsible for relevant significant programs,
- Office of Inspector General (IG) and internal audit management (including any internal control officer),
- other members of the audit organization, concerning relevant completed, planned or in-progress assignments,
- personnel in the Office of General Counsel, and
- personnel in the Special Investigator Unit.

Also, the auditor generally gathers information from relevant reports and articles issued by or about the entity, including

- GAO reports;
- IG, internal audit, or other audit reports (including those for performance audits and other reviews);
- congressional hearings and reports;
- consultant reports; and
- material published about the entity in newspapers, magazines, Internet sites, and other publications.

2.1.4 Obtain a General Understanding of the Structure of the Entity's Networks

The auditor should obtain and document a general understanding of the structure of the entity's networks as a basis for planning the IS controls audit. The auditor's understanding includes a high-level view of the network architecture that the entity uses to implement relevant key business processes. Such an understanding helps the auditor to assess risk, identify potential critical control points on a preliminary basis, understand technologies that may be subject to audit, and identify key locations. The auditor generally should request documentation of such information from the entity, including both high-level and detailed network schematics. The auditor should obtain the following information about the network architecture, generally documented in network schematics:

- Internet presence;
- firewalls, routers, and switches;
- intrusion detection or prevention systems;
- critical systems, such as Web and mail systems, file transfer systems, etc.;
- network management systems;
- connections to inter- and intra-agency sites;
- connections to other external organizations;
- remote access—virtual private network and dial-in; and
- wireless connections.

2.1.5 Identify Key Areas of Audit Interest

The auditor should identify key areas of audit interest, which are those that are critical to achieving the audit objectives (e.g., general support and business process application systems and files (or components thereof)). For a financial audit, this would include key financial applications and data and related feeder systems.[20] For a

[20] A feeder system is a system that provides information or data to support the main application. For example, in a payroll system the time and attendance system is the feeder system for the main application.

performance audit, this would include key systems that are likely to be significant to the audit objectives. For each key area of audit interest, the auditor should document relevant general support systems and major applications and files, including (1) the operational locations of each key system or file, (2) significant components of the associated hardware and software (e.g., firewalls, routers, hosts, operating systems), (3) other significant systems or system level resources that support the key areas of audit interest, and (4) prior audit problems reported. The auditor should also identify all access paths into and out of the key areas of audit interest. By identifying the key systems, files, or locations, the auditor can concentrate efforts on them, and do little or no work associated with other areas. The auditor generally should prioritize important systems, files, or locations in order of importance to the audit objectives. The auditor may characterize these items by the sensitivity or significance of the information processed, dollar value of the transactions processed, or presence or number of key edits or other controls performed by a business process application.

2.1.6 Assess Information System Risk on a Preliminary Basis

Overview

The auditor should assess and document, on a preliminary basis, the nature and extent of IS risk that relates to the key areas of audit interest. IS risk is the likelihood that a loss of confidentiality, integrity, or availability could occur that would materially/significantly affect the audit objectives (e.g., for a financial audit, a material misstatement). Assessing IS risk involves evaluation of both the likelihood that such a loss of confidentiality, integrity, or availability could occur and the materiality or significance of a loss of confidentiality, integrity, or availability to the audit objectives. The auditor should document factors that significantly increase or decrease the level of IS risk and their potential impact on the effectiveness of information system controls.

Assessing IS risk relating to the audit is different from management's risk assessment. In assessing IS risk, the auditor is

not required or expected to reperform management's risk assessment. Rather, the auditor assesses IS risk on a preliminary basis using data that would be collected in the planning of audit (this includes using the entity's risk assessments and performing other audit procedures as outlined below). The auditor's risk assessment should reflect the impact of the effectiveness of IS controls on the audit objectives.

The auditor's assessment of IS risk affects the nature, timing, and extent of IS controls audit procedures. As IS risk increases, the auditor should perform more extensive and/or more effective tests of IS controls. For example, a significant number of Internet access points that are not centrally controlled increases IS risk. In this case, the auditor would expand the auditor's testing, as there are more potential access paths to the key areas of audit interest. Risk assessments prepared by the entity may serve as a useful tool to assist in the identification of IS risk. However, the auditor should not rely on them without performing audit procedures to identify and assess risk.

To develop a framework for analyzing IS risk, the auditor should consider IS risk in the context of the following three security objectives for information and information systems:

- Confidentiality—preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.
- Integrity—guarding against improper information modification or destruction, which includes ensuring information nonrepudiation[21] and authenticity[22]. A loss of integrity is the unauthorized modification or destruction of information.

[21]Nonrepudiation is assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information. Nonrepudiation may not be necessary to evaluate integrity to meet an audit objective.

[22]Authenticity is the property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. Authenticity may not be necessary to evaluate integrity to meet an audit objective.

- Availability—ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

In some instances, one or more of the security objectives may have more significance to the audit objectives than the others.

The auditor should identify factors or conditions that significantly increase or decrease IS risk. These factors are general in nature; the auditor uses judgment in determining (1) the extent of procedures to identify the risks and (2) the impact of such risks on the entity's operations and the audit objectives. Because this risk assessment involves the exercise of significant audit judgment, the auditor should use experienced audit team personnel to perform the risk assessment. Factors considered would include those related to inherent risk[23] as well as those related to the control environment, risk assessment, communication, and monitoring components of internal control[24]. The auditor identifies such factors based on information obtained in the planning phase, primarily from understanding the entity's operations and key business processes, including significant IT processing performed outside the entity.

For each risk identified, the auditor should document the nature and extent of the risk; the conditions that gave rise to that risk; and the specific information or operations affected (if not pervasive). The auditor should also document compensating controls or other considerations that may mitigate the effects of identified risks.

[23]Inherent risk is the likelihood that a loss of confidentiality, integrity, or availability could occur that would materially/significantly affect the audit objectives (e.g., for a financial audit, a material misstatement), assuming that there are no related internal controls.

[24]Standards for Internal Control in the Federal Government (GAO/AIMD-00-21.3.1) describe the five standards of internal control as: control environment, risk assessment, control activities, information and communications, and monitoring. The specific IS controls assessed in an IS controls audit are part of the control activities component.

As noted above, the auditor should assess and document, on a preliminary basis, the nature and extent of IS risks for the information and information systems related to the key areas of audit interest, considering confidentiality, integrity, and availability. The auditor should document the basis for the assessed risk and its potential impact on the audit objectives. For example, in a financial audit, the auditor should evaluate the possibility of a material misstatement as a result of a loss of confidentiality, integrity, or availability. As discussed above, risk assessments prepared by the entity may serve as a useful tool to assist the auditor in the identification of IS risks.

Also, as noted above, IS risk includes the risk of loss of confidentiality, integrity, or availability. Such risk includes the potential impact of a loss to entity operations, assets, and individuals. However, depending on the audit objectives, the impact on the audit objectives could be greater or lesser. Federal agencies are required to use the following three levels to categorize their systems based on the potential impact of a breach of security on organizational operations, organizational assets, or individuals:[25]

- *Low*. The loss of confidentiality, integrity, or availability could be expected to have a **limited adverse effect** on organizational operations, organizational assets, or individuals.[26] A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
- *Moderate*. The loss of confidentiality, integrity, or availability could be expected to have a **serious adverse effect** on

[25]These risk levels are discussed further in National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards Publication (FIPS PUB) 199 (December 2003).

[26]Adverse effects on individuals may include, for example, loss of the privacy to which individuals are entitled under law.

organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.

- *High*. The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic adverse effect** on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

The auditor's assessment of IS risk may change as audit evidence is obtained. To determine whether audit procedures continue to be appropriate, the auditor should periodically reassess the IS risk during the audit. For example, the auditor may reassess the IS risk level at the end of the planning and testing phases, as well as when evidence is obtained that significantly affects the auditor's risk assessment. If IS risk changes during the audit, the auditor should make any necessary changes to the nature, timing, and extent of planned audit procedures.

The risk factors that the auditor considers consist of the following two types, which are discussed further below:

- Inherent risk factors

- Risk factors related to the control environment, risk assessment, communication, and monitoring components of internal control

Inherent Risk Factors

Information systems can introduce additional risk factors not present in a manual system. To properly assess IS risk, the auditor should (1) evaluate each of the following factors and (2) assess the overall impact of information systems on IS risk. The impact of these factors typically will be pervasive in nature.

- The nature of the hardware and software may affect IS risk, as illustrated below.
- The type of processing (online, batch oriented, or distributed) presents different levels of IS risk. Distributed networks enable multiple computer processing units to communicate with each other, increasing the number of potential access points and the risk of unauthorized access to computer resources and possible data alteration. On the other hand, distributed networks may decrease the risk of data inconsistencies at multiple processing units if the units share a common database.
- Peripheral access devices or system interfaces can increase IS risk. For example, Internet or wireless access to a system increases the system's accessibility to additional persons and therefore increases the risk of unauthorized access to computer resources.
- Highly customized application software may have higher IS risk than vendor-supplied software that has been thoroughly tested and is in general commercial use. On the other hand, vendor-supplied software new to commercial use may not have been thoroughly tested or undergone client processing to a degree that would encounter existing flaws.
- Certain hardware and software may have more significant identified weaknesses than others.
- In certain systems (e.g., enterprise resource planning—ERP—systems[27]), the audit trails and supporting information produced

[27]ERP systems consist of functional modules that support business requirements such as human resources, financials, or inventory control. The modules can be used individually or in conjunction with other modules as needed. The individual modules contain the business process necessary to complete their intended function.

by the systems may be limited in their usefulness (1) as a basis for applying certain types of controls or (2) as audit evidence.

- Highly decentralized applications, particularly Web applications, increase IS risk by adding complexity to IS and increasing potential vulnerabilities.
- The application of new technologies generally increases the risk that secure configurations of such technologies may not be well developed or tested, or that IT personnel may not properly implement security over such new technologies.
- The manner in which the entity's networks are configured can affect the related IS risk. For example, factors increasing IS risks include a significant number of Internet access points that are not centrally controlled, networks that are not segmented to protect sensitive systems or information, use of technologies that are no longer supported, or lack of technologies that enhance security.
- The consistency of the entity's enterprise architecture and IT strategy with its business strategies can affect the proper planning and implementation of IT systems and related security.

Also, the following risk factors, discussed in FAM 260 (Identify Risk Factors) are relevant to both financial and performance audits:

- Uniform processing of transactions: Because information systems process groups of identical transactions consistently, any misstatements arising from erroneous computer programming will occur consistently in the same types of transactions. However, the risk of random processing errors is reduced substantially in information systems–based accounting systems.
- Automatic processing: The information system may automatically initiate transactions or perform processing functions. Evidence of these processing steps (and any related controls) may or may not be visible.
- Increased potential for undetected misstatements: Information systems use and store information in electronic form and require less human involvement in processing than manual systems. Without adequate controls, there is increased risk that individuals could gain unauthorized access to sensitive

information and alter data without leaving visible evidence. Because information is in electronic form, changes to computer programs and data are not readily detectible. Also, users may be less likely to challenge the reliability of information systems output than manual reports.

- Existence, completeness, and volume of the audit trail: The audit trail is the evidence that demonstrates how a specific transaction was initiated, processed, and summarized. For example, the audit trail for a purchase could include a purchase order; a receiving report; an invoice; an entry in an invoice register (purchases summarized by day, month, and/or account); and general ledger postings from the invoice register. Some computer systems are designed to maintain the audit trail for only a short period, only in an electronic format, or only in summary form. Also, the information generated may be too voluminous to be analyzed effectively without software. For example, one transaction may result from the automatic summarization of information from hundreds of locations. Without the use of audit or retrieval software, tracing transactions through the processing may be extremely difficult.
- Unusual or nonroutine transactions: As with manual systems, unusual or nonroutine transactions increase IS risk. Programs developed to process such transactions may not be subject to the same procedures as programs developed to process routine transactions. For example, the entity may use a utility program to extract specified information in support of a nonroutine management decision.

In addition, the auditor should evaluate the additional audit risk factors discussed in the "Additional IS Risk Factors" at the end of this chapter.

Risk Factors Related to the Control Environment, Risk Assessment, Communication, and Monitoring Components of Internal Control

Also, the auditor should evaluate the IT system factors discussed below, to the extent relevant to the audit objectives, in making an overall assessment of the control environment, risk assessment, communication, and monitoring components of internal control.

Additional information concerning these internal control components can be found at GAO's *Standards for Internal Control in the Federal Government*[28] ("Green Book") and *Internal Control Management and Evaluation Tool*[29], and at FAM 260, 295A, and 295B.

a. **Management's attitudes and awareness with respect to IT systems:** Management's interest in and awareness of IT system functions (including those performed for the entity by other organizations) is important in establishing an entitywide consciousness of control issues. Management may demonstrate its interest and awareness by

- considering the risks and benefits of computer applications;
- communicating policies regarding IT system functions and responsibilities;
- overseeing policies and procedures for developing, modifying, maintaining, and using computers, and for controlling access to programs and files;
- considering the risk of material misstatement, including fraud risk, related to IT systems;
- responding to previous recommendations or concerns;
- quickly and effectively planning for, and responding to, computerized processing crises; and
- using reliable computer-generated information for key operating decisions.

b. **Organization and structure of the IT system function:** The organizational structure affects the control environment. Centralized structures often have a single computer processing organization and use a single set of system and applications software, enabling tighter management control over IT systems. In decentralized structures, each computer center generally has its own computer processing organization, application programs, and system software, which may result in differences in policies and procedures and various levels of compliance at each location.

[28]GAO, *Standards for Internal Control in the Federal Government,* AIMD-00-21.3.1 (Washington, D.C.:November 1, 1999).

[29]GAO, *Internal Control Management and Evaluation Tool*, GAO-01-1008G (Washington, D.C.:August 2001).

c. **Clearly defined assignment of responsibilities and authority:** Appropriate assignment of responsibility according to typical IT system functional areas can affect the control environment. Factors to consider include

- how the position of the Chief Information Officer (CIO) fits into the organizational structure;
- whether duties are appropriately segregated within the IT systems function, such as operators and programmers, since lack of segregation typically affects all systems;
- the extent to which management external to the IT systems function is involved in major systems development decisions; and
- the extent to which IT system policies, standards, and procedures are documented, understood, followed, and enforced.

d. **Management's ability to identify and to respond to potential risk:** Computer processing, by its nature, introduces additional risk factors. The entity should be aware of these risks and should develop appropriate policies and procedures to respond to any IT system issues that might occur. The auditor may evaluate

- the methods for monitoring incompatible functions and for enforcing segregation of duties and
- management's mechanism for identifying and responding to unusual or exceptional conditions.

Examples of potential IT-related control environment, risk assessment, communication, and monitoring weaknesses include:

- Management and personnel in key areas (such as accounting, IT systems, IG, and internal auditing) have a high turnover.
- Management attitude toward IT systems and accounting functions is that these are necessary "bean counting" functions rather than a vehicle for exercising control over the entity's activities or making better decisions.
- The number of people, particularly in IT systems and accounting, with requisite skill levels relative to the size and complexity of the operations is inadequate.
- Management has not adequately identified risks arising from internal sources, such as human resources (ability to

retain key people) or IT (adequacy of backup systems in the event of systems failure).
- Accounting systems and/or information systems, including IT systems, are not modified in response to changing conditions.

2.1.7 Identify Critical Control Points

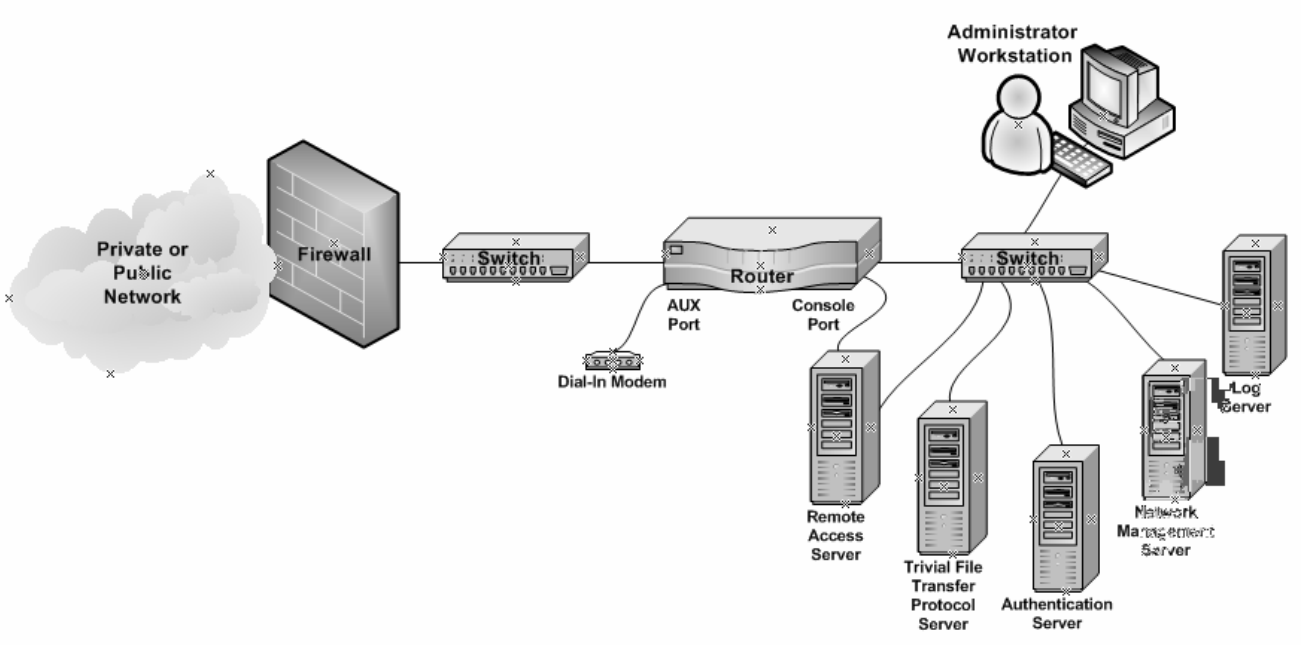
The auditor should identify and document critical control points in the design of the entity's information systems based on the auditor's understanding of such systems, key areas of audit interest, and IS risk. Critical control points are those system control points that, if compromised, could allow an individual to gain unauthorized access to or perform unauthorized or inappropriate activities on entity systems or data, which could lead directly or indirectly to unauthorized access or modifications to the key areas of audit interest. Control points typically include external access points to the entity's networks, interconnections with other external and internal systems, system components controlling the flow of information through the entity's networks or to the key areas of audit interest, critical storage and processing devices, and related operating systems, infrastructure applications, and relevant business process applications. Typical control points also include network components where business process application controls are applied. As the audit testing proceeds and the auditor gains a better understanding of the entity's information systems, of control weaknesses, and of the related risks, the auditor should periodically reassess the critical control points. Based on information obtained during audit planning, the auditor should identify those critical control points in the entity's IT systems that are significant to the effectiveness of security over the key areas of audit interest.

An analysis of critical control points includes consideration of alternate work sites. Since multiple FISCAM control categories are relevant to alternate work sites, it is not addressed as a specific control in this document. For further information on this subject refer to NIST guidance contained in SP 800-53 and SP 800-46.

In identifying critical control points and in planning and performing the assessment of IS controls, auditors apply the concept of control

dependencies. A control dependency exists when the effectiveness of an internal control is dependent on the effectiveness of other internal controls. An assessment of the effectiveness of information system controls over a critical control point includes testing the effectiveness of controls over other control points upon which the security of the critical control point is dependent. Figure 2 illustrates the concept of a control dependency in relation to a router for a typical network.

Figure 2: Example of Router Control Dependencies



Source: GAO and Visio.

The figure illustrates that the effectiveness of controls over the router in this example network are dependent on controls over other control points. In this example, because unauthorized or inappropriate access to the other control points could affect the security of the router, the auditor's tests of IS controls generally should include controls over

- the trivial file transfer protocol (tftp) servers used to maintain a central repository of sensitive configuration files (tftp servers do

not require authentication and are also used as remote boot devices for routers);
- the centralized authentication server that authenticates users to the router and other network devices;
- network switches that could share sensitive data with routers such as passwords and shared keys (also, network switches provide a trusted path to the routers);
- administrative workstations used to manage network devices, such as routers; and
- the log server, which maintains logs containing relevant information about significant network events, such as router access.

In addition, as part of a review of the system level controls over the router, the auditor generally should test controls over

- the network management servers used to manage configuration files that contain sensitive information about network devices such as routers;
- remote access to the router via the auxiliary and console ports that could be used to remotely manage the router;
- the firewalls that provide boundary protection (i.e., limits connectivity to the router);
- unencrypted network traffic that could be "sniffed" to obtain router or other privileged passwords; and
- the PC connected to the router that could facilitate direct connectivity to the router.

Further, the auditor generally should test other controls that may affect the security of the router, based on the auditor's judgment. Note that, in addition to controls over access to the router itself, IS controls include controls over the routing of traffic throughout the network (see AC-1 in Chapter 3).

As the auditor performs the IS controls audit, based on the auditor's assessment of risk and the results of audit tests, the auditor may determine that it is necessary to modify the scope of the audit, including revisions to the critical control points. For example, if

significant IS control weaknesses are identified during the audit, it may not be necessary to perform all planned tests of IS controls. If testing is reduced due to the identification of significant weaknesses, the auditor should document such a decision. Also, testing may result in the identification of additional risks, and critical control points, and /or control dependencies; the auditor should determine whether to adjust the scope for them.

2.1.8 Obtain a Preliminary Understanding of Information System Controls

The auditor should obtain and document a preliminary understanding of the design of the entity's IS controls, including the organization, staffing, responsibilities, authorities, and resources of the entity's security management function. The auditor should document a preliminary understanding of entitywide controls (or componentwide controls if only a component is being audited) related to security management, access controls, configuration management, segregation of duties and, contingency planning.

The auditor should understand the design of each of the three types of IS controls (general, business process application, and user controls) to the extent necessary to tentatively conclude whether these controls are likely to be effective. If they are likely to be effective, the auditor should consider specific IS controls in determining whether relevant IS control objectives are achieved. If IS controls are not likely to be effective, the auditor should obtain a sufficient understanding of control risks arising from IS controls to assess audit risk, design appropriate audit procedures, and develop appropriate findings.

In addition, the auditor should obtain a preliminary understanding of the business process application controls (business process, interface, and data management system controls) over key business process applications identified as or related to key areas of audit interest, determine where those controls are applied, and determine whether the controls are designed effectively and have been implemented (placed in operation). For example, authentication and authorization may be applied in network components that are different from those where key data files or applications reside; (e.g., Web applications that reside on one server may be used to

authenticate and authorize users of legacy systems that run on different servers or systems). The auditor should determine the potential impact of any identified design weaknesses on the completeness, accuracy, validity, and confidentiality of related application data. (See Chapter 4 for a description of completeness, accuracy, validity, and confidentiality.)

Based on this understanding, the auditor should make a preliminary assessment of whether IS controls are likely to be effective to assist in determining the nature, timing, and extent of testing. This assessment is based primarily on discussions with personnel throughout the entity, including program managers, system administrators, information resource managers, and systems security managers; on observations of IT operations and controls; on reviewing examples of evidence of control performance; on prior audits or the work of others; and on reading written policies and procedures. This preliminary assessment for financial audits is discussed further at FAM 270 (Determine Likelihood of Effective Information System Controls). Based on the preliminary assessment, the auditor should make any adjustments, as necessary, to the IS risk level, critical control points, and planned scope of the audit work.

Control activities for critical elements in each general control and business process control category are described in Chapters 3 and 4, respectively, and summarized in Appendix II. The auditor may use the summary tables in Appendix II, which are also available in electronic form from the FISCAM website at http://www.gao.gov/special.pubs/fiscam.html, to document preliminary findings and to assist in making the preliminary assessment of controls. As the audit progresses through testing of internal controls, the auditor may continue to use the electronic version of the tables to document controls evaluated and tested, test procedures performed, conclusions, and supporting documentation references.

The auditor should include the following information in the documentation of their preliminary understanding of the design of IS controls, to the extent relevant to the audit objectives:

- An identification of relevant entitywide, system, and business process application level controls designed to achieve the control activities for each critical element within each general control area and a determination of whether they are designed effectively and implemented (placed in operation), including identification of control activities for which there are no or ineffective controls at the entitywide level and the related risks
- Identification of business process controls for key applications identified as key areas of audit interest, determination of where those controls are implemented within the entity's systems, and the auditor's conclusion about whether the controls are designed effectively and implemented (placed in operation), including identification of control activities for which there are no or ineffective controls and the related risks and the potential impact of any identified design weaknesses on the completeness, accuracy, validity, and confidentiality of application data
- Any internal or third-party information systems reviews, audits, or specialized systems testing (e.g., penetration tests, disaster recovery tests, and application-specific tests) performed during the last year and the auditor's evaluation of the other auditor's objectivity, competence and conclusions (see section 2.1.9.C)
- Management's plans of action and milestones, or their equivalent, that identify corrective actions planned to address known IS control weaknesses (see section 2.1.9.C)
- Status of the prior years' audit findings (see section 2.1.9.C)
- Documentation for any significant computer security related incidents identified and reported for the last year
- Documented security plans
- Documented risk assessments for relevant systems (e.g., general support systems and major applications)
- System certification and accreditation documentation or equivalent for relevant systems
- Documented business continuity of operations plans and disaster recovery plans
- A description of the entity's use of third-party IT services

The auditor should obtain information from relevant reports and other documents concerning IS that are issued by or about the entity, including

- the entity's prior FISMA or equivalent reports on IS;
- the entity's annual performance and accountability report or equivalent reports on performance including reports filed to comply with the Federal Financial Management Improvement Act of 1996[30] (FFMIA) and Federal Managers' Financial Integrity Act of 1982[31] (FMFIA);
- other reports by management or the auditor about IS;
- other reports that contain information concerning IS that are relevant to the audit objectives;
- GAO reports;
- IG and internal audit reports (including those for performance audits and other reviews); and
- consultant reports.

2.1.9 Perform Other Audit Planning Procedures

The auditor should address the following areas during the planning phase, even though related audit procedures may be applied during the other phases. More specifically, the auditor should address any other issues, not identified in the previous steps, that could affect the objectives, scope, or methodology of the IS controls audit, including

- relevant laws and regulations;
- consideration of the risk of fraud;
- previous audits and attestation engagements;
- audit resources;
- multiyear testing plans;

[30]Federal Financial Management Improvement Act of 1996, 31 U.S.C. 3512 note.
[31]Federal Managers' Financial Integrity Act of 1982 (FMFIA), 31 U.S.C. 3512 (c), (d).

- communication with entity management and those charged with governance;
- service organizations;
- using the work of others; and
- audit plan (and an audit strategy for financial statement audits).

2.1.9.A Relevant Laws and Regulations

The auditor should identify applicable laws and regulations that are relevant to IS at the entity. Such laws and regulations may establish general or specific IS control requirements or criteria. Laws and regulations generally relevant to audits of federal agencies include FISMA, FMFIA, FFMIA, Appendix III of OMB Circular A-130[32], OMB Circulars A-123[33] and A-127[34], and FISMA implementing guidance. Federal laws and regulations that may affect the entity include, but are not limited to:

- Health Insurance Portability and Accountability Act of 1996 (HIPAA),[35]
- Gramm-Leach-Bliley Act,[36]
- Requirements for information security for Medicare Administrative Contractors,[37]
- Chief Privacy Officer statutory requirements,[38]

[32]OMB, *Management of Federal Information Resources*, Circular A-130 (Washington, D.C.: November 28, 2000).

[33]OMB, *Management's Responsibility for Internal Control*, Circular A-123 (Washington, D.C.: December 21, 2004).

[34]OMB, *Financial Management Systems*, Circular A-127, (Washington, D.C.: January 9, 2009).

[35]Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191 (Aug. 21, 1996). For provisions relating to health information and systems, see 42 U.S.C. 1320d, et seq. For HHS HIPAA Security and Privacy Standards, see 45 C.F.R. Part 164.

[36]Gramm-Leach-Bliley Act, Pub. L. 106-102 (Nov. 12, 1999), see, e.g., Title V, Privacy.

[37]Requirements for information security for Medicare Administrative Contractors, Sec. 912, Medicare Prescription Drug, Improvement, and Modernization Act of 2003, Pub. L. 108-173 (Dec. 8, 2003), 117 Stat. 2387.

- OMB Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy*, [39]
- OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information*, and[40]
- OMB Memorandum M 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information.*[41]

In IS controls audits of state and local governments, the auditor should identify applicable legal and reporting requirements and issues. Further information specifically related to audits of state and local government entities can be obtained from the National Association of State Auditors, Comptrollers and Treasurers (NASACT).[42]

Under GAGAS, the auditor should design and perform procedures to provide reasonable assurance of detecting instances of violations of legal and regulatory requirements that are significant within the context of the audit objectives. Consequently, if one of the objectives of the audit is to determine whether the entity violated specific laws or regulations, the auditor should plan the audit to detect significant violations of such laws or regulations. In financial audits, the auditor should test those laws and regulations that could have a direct and material effect on the financial statements.

[38]For example, sec. 522, Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005, Div. H, Consolidated Appropriations Act, 2005, Pub. L. 108-447 (Dec. 8, 2004).5 USC 552a note.

[39]OMB, *Designation of Senior Agency Officials for Privacy*, M-05-08 (Washington, D.C.: Feb. 11, 2005).

[40]OMB, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, M-06-19 (Washington, DC: July 12, 2006).

[41]OMB, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, M 07-16 (Washington, D.C.: May 22, 2007).

[42]Intergovernmental Information security Audit Forum, *Information Systems Security Auditing: Legal and Reporting Considerations* (Sept. 11, 2003) www.nasact.org/IISAF/legal.html

As part of an IS controls audit, the auditor's findings will typically be reported in terms of whether IS controls are effective. While laws and regulations such as FISMA, FMFIA, FFMIA, and OMB and NIST guidance provide requirements and criteria for assessing IS, IS controls audit objectives generally are not focused on detecting violations of such laws and regulations, but rather on assessing controls and identifying any control weaknesses. Consequently, such laws and regulations generally would not be considered significant to the audit objectives for the purposes of designing compliance tests to meet GAGAS. However, audit objectives may sometimes include specific objectives to determine compliance with such laws, in which case such laws and regulations would be significant. Also, other laws such as HIPAA, which provide for potential penalties, may be significant to the audit objectives.

2.1.9.B Consideration of the Risk of Fraud

In audits performed under GAGAS, the auditor should gather and assess the risks of fraud[43] occurring that is significant within the context of the audit objectives (for financial audits, a material misstatement) or that could affect the findings or conclusions. When auditors identify factors or risks related to fraud that has occurred or is likely to have occurred that they believe are significant within the context of the audit objectives, they should design procedures to provide reasonable assurance of detecting such fraud. In financial audits, GAGAS indicates that auditors should assess the risk of material misstatements of financial statement amounts or other financial data significant to the audit objectives due to fraud and to consider that assessment in designing the audit procedures to be performed.[44]

[43]Fraud is a type of illegal act involving the obtaining of something of value through willful misrepresentation.

[44]The terms "material" and "significant" are synonymous under generally accepted government auditing standards. In the AICPA standards, "material" is used in relation to audits of financial statements. "Significant" is used in relation to performance audits performed under GAGAS.

The auditor's responsibilities with respect to the risk of fraud in financial statement audits are discussed further in the GAGAS and in the AICPA's Auditing Standards Board Statement on Auditing Standards No. 99, titled *Consideration of Fraud in a Financial Statement Audit*, as amended (AU section 316). The risk of fraud is also a relevant consideration in performance audits. For example, an area of concern for fraud in a performance audit would be the adequate protection of personally identifiable information where individual social security numbers could be stolen and used for fraudulent activities.

If the IS controls audit is performed as part of a broader financial or performance audit, the auditor should coordinate with the audit team in the identification of and response to the risk of fraud. The auditor should be aware of fraud risks identified by the overall audit team and communicate any fraud risks or suspected fraud associated with IT to the overall audit team. Also, the overall audit team may identify audit procedures to be performed by the IS controls specialist to detect fraud significant to the audit.

The audit team should hold a brainstorming session at the start of the audit to discuss potential fraud risks, fraud factors such as individuals' incentives or pressures to commit fraud, the opportunity for fraud to occur, and rationalizations or attitudes that could allow individuals to commit fraud. For example, the following factors related to IS may indicate a risk of fraud:

- failure to provide an adequate security management program, including inadequate monitoring of control effectiveness;
- weaknesses in access and other IS controls that could allow overrides of internal controls or access to systems susceptible to fraud (e.g., payment systems);
- lack of adequate segregation of duties;[45] and
- pervasive or long-standing IS control weaknesses.

[45]Separation of duties so that no one individual controls all critical stages of a work process. Also see section 3.4 and the definition in the glossary.

The auditor should gather and assess information necessary to identify fraud risks that could be relevant to the audit objectives or affect the results of their audit. For example, the auditor may obtain information through discussion with officials of the audited entity or through other means to determine the susceptibility of the program to fraud, the status of internal controls the entity has established to detect and prevent fraud or the risk that officials of the audited entity could override internal controls. The auditor should exercise professional skepticism in assessing these risks to determine which factors or risks could significantly affect the results of their work if fraud has occurred or is likely to have occurred.

When the auditor identifies factors or risks related to fraud that they believe are significant within the context of the audit objectives or the results of the audit, they should design procedures to provide reasonable assurance of detecting such fraud. The auditor should prepare audit documentation related to their identification and assessment of and response to fraud risks.

Assessing the risk of fraud is an ongoing process throughout the audit and relates not only to planning the audit but also to evaluating evidence obtained during the audit. When testing general and business process application level controls, the auditor should be alert for information or other conditions that indicate fraud that is significant within the context of the audit objectives may have occurred.

A specific area of concern for fraud is override of controls, particularly in ERP applications. Because ERP applications are by their nature highly integrated, the potential risk of management override of controls is heightened. The audit generally should include procedures to identify system-based overrides. These procedures might include testing for instances of users performing inappropriate combinations of transactions (i.e., transactions that should have been segregated) and other similar procedures. Some examples of antifraud controls to consider include: workflow approvals, restricting access to sensitive files, segregation of duties, review of audit trails, and review of key management reports. Access controls, segregation of duties, and audit trails are discussed in Chapter 3.

The auditor should also evaluate situations or transactions that could be indicative of fraud. When information comes to the auditors' attention (through audit procedures, allegations received through fraud hotlines, or other means) indicating that fraud may have occurred, the auditor should evaluate whether the possible fraud could significantly affect the audit results. If the fraud could significantly affect the audit results, auditors should modify the audit steps and procedures, as necessary, to (1) determine if fraud likely has occurred and (2) if so, determine its effect on the audit results.

The auditor's training, experience, and understanding of the program being audited may provide a basis for recognizing that some acts coming to his or her attention may be indicative of fraud. Whether an act is, in fact, fraud is a determination to be made through the judicial or other adjudicative system and is beyond auditors' professional expertise and responsibility. However, the auditor is responsible for being aware of vulnerabilities to fraud associated with the area being audited to identify indications that fraud may have occurred.

2.1.9.C Previous Audits and Attestation Engagements

Under GAGAS, auditors should evaluate whether the audited entity has taken appropriate corrective action to address findings and recommendations from previous engagements that are significant within the context of the audit objectives (for financial audits, those that could have a material effect on the financial statements). When planning the audit, auditors should ask entity management to identify previous audits, attestation engagements, performance audits, or other studies that directly relate to the objectives of the audit, including whether related recommendations have been implemented. For IS control audits, this would include weaknesses identified by management through its monitoring controls (e.g., for federal entities, Plans of Action and Milestones) that are relevant to the audit objectives. Auditors should use this information in assessing risk and determining the nature, timing, and extent of current audit work, including determining the extent to which

testing the implementation of the corrective actions is applicable to the current audit objectives.

2.1.9.D Audit Resources

As with other types of audits, the staff assigned to perform the IS controls audit must collectively possess adequate professional competence. Therefore, it is important to carefully plan IS controls audits to ensure that adequate and appropriate resources are available to perform the audit. IS controls audits need a broad range of technical skills. In addition to skills necessary to assess each control category, IS controls audits generally use technical specialists with skills in such areas as networks, Windows/Novell, Unix, data management systems, and mainframe system and access control software. See Appendix V for a discussion of typical skill sets for IS controls specialists. Based on the knowledge obtained during audit planning, the auditor should identify resource requirements and determine whether internal resources are available or whether contractors will be necessary to complete the audit. The auditor should then schedule the resources for the appropriate periods of time.

Regardless of the size of the entity, the auditor must still perform the necessary planning to ensure that audit requirements are fully satisfied. This includes small/independent agencies which generally have a less complex, less risky IS control environment, which requires inherently fewer IS controls audit resources. The Committee of Sponsoring Organizations (COSO)[46] publication "Internal Controls over Financial Reporting – Guidance for Smaller Public Companies" includes guidance that could be used by smaller agencies to assist in planning their audits.

The auditor may determine that it is necessary to contract for audit services for all or a portion of the IS controls audit. For example, the auditor may determine that it is necessary to contract only for certain technical skills needed to perform the audit. Contracting for

[46]Is a voluntary private sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls, and corporate governance.

audit services offers two significant benefits to an entity's audit organization—it allows audit coverage beyond that possible with the existing audit staff level, and it allows the audit activity to address technical and other issues in which the in-house staff is not skilled. Engagements that employ contractors in this way may help train in-house staff for future audits. However, when contracting for audit services, some in-house audit personnel generally should be actively involved. For example, the audit organization should be instrumental in determining the scope of the contracted services, and in developing the task order or request for proposal for the work. The FISCAM may be required to be used as a basis for the work to be performed.

Also, an auditor generally should be designated to monitor the contract for the entity. The contract monitor should have sufficient knowledge of IS controls to monitor and to assess the quality and adequacy of the work performed by the contractor, including the adequacy of the audit documentation. The contract monitor should discuss the contract with the contractor, including the product deliverables, the established time frames for deliverables, and documentation standards to adhere to. The auditor generally should hold this meeting before the contractor begins work. In addition, the contract monitor should attend critical meetings the contractor has with entity representatives, including the opening and close-out meetings.

The contract monitor should conduct a technical review of the work performed and may use this manual as guidance to determine whether the work addressed relevant issues and the audit procedures were adequate. For financial audits, the contract monitor or audit team may reperform some tests in accordance with FAM 650, "Using the Reports and Work of Others." Also, the contract monitor should review the audit report and supporting audit documentation to determine whether the audit report is adequately supported.

2.1.9.E Multiyear Testing Plans

In circumstances where the auditor regularly performs IS controls audits of the entity (as is done, for example, by an IG or for annual

financial audits), the auditor may determine that a multiyear plan for performing IS controls audits is appropriate. Such a plan will cover relevant key entity applications, systems, and processing centers. These strategic plans should cover no more than a 3-year period and include the schedule and scope of assessments to be performed during the period and the rationale for the planned approach. The auditor typically evaluates these plans annually and adjusts them for the results of prior and current audits and significant changes in the IT environment, such as implementation of new systems.

Multiyear testing plans can help to assure that all entity systems and locations are considered in the IS control evaluation process, to consider relative audit risk and prioritization of systems, and to provide sufficient evidence to support an assessment of IS control effectiveness, while helping to reduce annual audit resources under certain conditions. When appropriate, this concept allows the auditor to test computer-related general and business process application controls on a risk basis rather than testing every control every year. Under a multiyear testing plan, different controls are comprehensively tested each year, so that each significant general and business process control is selected for testing at least once during the multiyear period, which should not be more than 3 years. For example, a multiyear testing plan for an entity with five significant business process applications might include comprehensive tests of two or three applications annually, covering all applications in a 2 or 3 year period. For systems with high IS risk, the auditor generally should perform annual testing.

Such multiyear testing plans are not appropriate in all situations. For example, they are not appropriate for first-time audits, for audits where some significant business process applications or general controls have not been tested within a sufficiently recent period (no more than 3 years), or for audits of entities that do not have strong entitywide controls. Also, using this concept, the auditor should perform some limited tests and other activities annually for general and business process controls not selected for full testing; examples of such activities include updating the auditor's understanding of the control environment, inquiring about control changes, and conducting walk-throughs. For example, because of the importance of system level critical control points, the

auditor generally updates the understanding of these yearly through limited tests. Multiyear testing is discussed in greater detail in FAM section 395 G: "Multiyear Testing of Controls."

2.1.9.F Communication with Entity Management and Those Charged with Governance

The auditor should communicate information about the audit to appropriate entity management and those charged with governance. The auditor should document this communication, usually with an engagement letter. This step is particularly important in an IS controls audit because of the sensitivity of entity information systems and the nature of tests performed. Multiple meetings may be necessary with various levels of management so that they are adequately aware of the audit process. GAGAS requires that to help the various parties involved in the audit understand the audit objectives, time frames, and any data needs, the auditor should provide them with information about the specific nature of the audit, as well as general information concerning the planning and conduct of the audit and reporting. If the IS audit is performed as part of a broader financial or performance audit or attestation engagement, the auditor should coordinate this step with the audit team.

As part of this communication, it may be useful to provide general protocols for conducting the IS controls audit. Such protocols might include the following:

- Define the scope of the engagement. This might include an overview of the audit objectives, information about what is to be tested, when testing will occur, where and from what locations testing will be performed, who will be performing and monitoring the testing, and how the testing will be performed (for example, the methodology and tools that will be employed). However, it is important to not disclose detailed audit procedures so that the tests become ineffective.
- Communicate risks and steps taken by management to manage such risks. While risks cannot be eliminated entirely, they can be managed to an acceptable level to avoid, or at least minimize, service degradation or interruption. Auditors can communicate actions they have taken to minimize risks such as (a) not

performing denial-of-service testing, (b) coordinating testing with the audited site, (c) having knowledgeable personnel from the audited site monitoring all testing, (d) testing the tools that will be used and gaining expertise in their use, (e) logging test parameters, (f) logging testing and results, (g) using network analyzers to monitor loads placed on the network during testing, and (h) performing testing during nonpeak hours, if possible.

- Identify roles and responsibilities. Address the roles and responsibilities of each participant. Participants will likely include the test team, the auditors, the system owners, the systems security officer, the systems administrators, and contractors, if applicable.
- Address logistical requirements. Logistical requirements would include information about such items as the organization's range of Internet Protocol addresses and telephone numbers (particularly sensitive numbers that should be excluded from testing), analog telephone lines, wireless connections, Internet access paths, policies governing user accounts and passwords, etc. On-site workspace arrangements and entity points of contact might also be addressed.

GAGAS requires certain communications with management, those charged with governance, and others. For financial audits, see AU 380 and GAGAS 4.06. For attestation engagements, see GAGAS 6.06-6.08. For performance audits, see GAGAS 7.46-7.48. In situations in which those charged with governance are not clearly evident, auditors should document the process followed and conclusions reached for identifying those charged with governance.

2.1.9.G Service Organizations

When IS controls that are significant to a GAGAS audit are performed by a service organization external to the audited entity, the auditor should determine how to obtain sufficient, appropriate evidence about the operating effectiveness of such controls. The auditor should coordinate these procedures with the audit procedures performed in support of critical element SM-7 "Ensure That Activities Performed by External Third Parties are Adequately Secure". For example, the auditor should determine how

management of the audited entity monitors the effectiveness of IS controls at the service organization, such as through the receipt and analysis of a service auditor (SAS 70[47]) report. SAS 70 reports are discussed in more detail in Appendix VII. If the auditor uses a SAS 70 report, the auditor is responsible for determining whether SAS 70 report provides sufficient evidence about the operating effectiveness of IS controls performed by the service organization that are significant to the audit. Also, see section 2.1.9.H below. If IS controls are performed by service organizations, the auditor should document conclusions whether such controls are significant to the audit objectives and any audit procedures performed with respect to such controls (e.g., review of service auditor reports).

The auditor should integrate evidence obtained about the operating effectiveness of service auditor controls into the IS controls audit. For example, the auditor should evaluate the effectiveness of IS controls for the combination of IS controls at the audited entity and at the service organization collectively. The preparation and use of service auditor reports are discussed further in Appendix VII, including how to determine whether the service auditor report contains sufficient, appropriate evidence.

If the user auditor plans to use a service auditor's report as audit evidence about the design and implementation and/or operating effectiveness of controls at the service organization, the user auditor should:

- evaluate whether the description of the service organization's system and, for type 2 reports, the service auditor's description of tests of controls and results thereof, is as of a date or for a period that is appropriate for the user auditor's purposes;
- evaluate the sufficiency and appropriateness of the evidence provided for the understanding of internal control relevant to the audit;
- evaluate whether the specific tests of controls performed by the service auditor and the results thereof as described in the type 2

[47]The Auditing Standards Board of the American Institute of Certified Public Accountants is currently deliberating on possible changes to SAS 70 requirements. Users of the FISCAM should determine whether such changes have been made before applying this section.

report are relevant to assertions in the user entity's financial statements; and

- determine whether complementary user entity controls identified by the service organization are relevant to the user entity and, if so, obtain an understanding of whether the user entity has designed and implemented such controls and test such controls.

2.1.9.H Using the Work of Others

The auditor may be able to use the work of the other auditors to support findings or conclusions for the current audit. If auditors use the work of other auditors, they should perform procedures that provide a sufficient basis for using that work. For financial audits, further information on using the work of other auditors is discussed in FAM 650 and AU 336. For performance audits, as discussed in GAGAS 7.41-.43, auditors should obtain evidence concerning the other auditors' qualifications and independence and should determine whether the scope, quality, and timing of the audit work performed by the other auditors is adequate for reliance in the context of the current audit objectives. Procedures that auditors may perform in making this determination include reviewing the other auditors' report, audit plan, or audit documentation, and/or performing tests of the other auditors' work. The nature and extent of evidence needed will depend on the significance of the other auditors' work to the current audit objectives and the extent to which the auditors will use that work.

As discussed in GAGAS 7.43, some performance audits may necessitate the use of specialized techniques or methods that require the skills of a specialist. If auditors intend to use the work of specialists, they should obtain an understanding of the qualifications and independence of the specialists. (See GAGAS paragraph 3.05 for independence considerations when using the work of others.) Evaluating the professional qualifications of the specialist involves the following:

a. the professional certification, license, or other recognition of the competence of the specialist in his or her field, as appropriate;

b. the reputation and standing of the specialist in the views of peers and others familiar with the specialist's capability or performance;
c. the specialist's experience and previous work in the subject matter; and
d. the auditors' prior experience in using the specialist's work.

If the auditor plans to use the work of others, the auditor should document conclusions concerning the planned use of the work of others and any audit procedures performed with respect to using the work of others.

2.1.9.I Audit Plan

The auditor should prepare a written audit plan for each audit. The auditor should describe the objectives, scope, and methodology for the IS controls audit. The auditor should include planning information, discussed in the preceding sections of this chapter. If the IS controls audit is a component of a performance audit or attestation engagement, the auditor should integrate such information, as appropriate, into the overall audit plan. If the IS controls audit is a component of a financial audit, the auditor should integrate such information, as appropriate, with the overall audit strategy and audit plan for the financial audit. Additionally, the auditor generally should use the IS controls audit plan as a tool to communicate with the audit team. If the auditor believes that another auditor will use his or her work, the auditor may use the plan to coordinate with the other auditor.

In planning the audit, the auditor generally will first assess the effectiveness of entitywide and system level general controls prior to testing business process application level controls, unless the purpose of the audit is to identify control weaknesses in the application area. Without effective entitywide and system level general controls, business process application level controls may be rendered ineffective by circumvention or modification. Consequently, if general controls are not designed or operating effectively, the auditor may conclude that assessing business process application level controls is not efficient or necessary to achieve the audit objectives. In such cases, the auditor should

develop appropriate findings and consider the nature and extent of risks and their effect on the audit objectives and the nature, timing, and extent of audit procedures. However, if an audit objective is to identify control weaknesses within a business process application, an assessment of the business process application level controls would be appropriate. Also, testing of business process application level controls may be warranted when the auditor finds general control weaknesses mainly in areas with a relatively insignificant impact on business process controls and the key areas of audit interest, but not in more significant areas.

GAGAS require that a written audit plan be prepared for each performance audit. The form and content of the written audit plan may vary among audits and may include an audit strategy, audit program, project plan, audit planning paper, or other appropriate documentation of key decisions about the audit objectives, scope, and methodology and of the auditor's basis for these decisions. The auditor should update the plan, as necessary, to reflect any significant changes to the plan made during the audit. GAGAS include financial audit planning documentation standards.

2.1.10 Documentation of Planning Phase

The auditor should document the following information developed in the planning phase:

- Objectives of the IS controls audit and, if it is part of a broader audit, a description of how such objectives support the overall audit objectives.
- The scope of the IS controls audit.
- The auditor's understanding of the entity's operations and key business processes, including, to the extent relevant to the audit objectives, the following:
  - The significance and nature of the programs and functions supported by information systems;
  - Key business processes relevant to the audit objectives, including business rules, transaction flows, and application and software module interaction;

    - Significant general support systems and major applications that support each key process;
    - Background information request, if used;
    - Significant internal and external factors that could affect the IS controls audit objectives;
    - Detailed organization chart, particularly the IT and the IS components;
    - Significant changes in the IT environment/architecture or significant applications implemented within the past 2 years or planned within the next 2 years; and
    - The entity's reliance on third parties to provide IT services (e.g., in-house, remote connectivity, remote processing).
- A general understanding of the structure of the entity's or component's networks as a basis for planning the IS controls audit, including high-level and detailed network schematics relevant to the audit objectives.
- Key areas of audit interest, including relevant general support systems and major applications and files. This includes (1) the operational locations of each key system or file, (2) significant components of the associated hardware and software (e.g., firewalls, routers, hosts, operating systems), (3) other significant systems or system-level resources that support the key areas of audit interest, and (4) prior audit problems reported. Also, the auditor should document all access paths in and out of the key areas of audit interest.
- Factors that significantly increase or decrease IS risk and their potential impact on the effectiveness of information system controls. For each risk identified, the auditor should document the nature and extent of the risk; the conditions that gave rise to that risk; and the specific information or operations affected (if not pervasive).
- Preliminary assessment of IS risks related to the key areas of audit interest and the basis for the assessed risk. For each risk identified, the auditor should document the nature and extent of the risk; the conditions that gave rise to that risk; and the specific information or operations affected (if not pervasive). The auditor should also document other considerations that may mitigate the effects of identified risks.

- Critical control points.
- A preliminary understanding of the entity's IS controls, including the organization, staffing, responsibilities, authorities, and resources of the entity's security management function. The auditor should include the following information in the documentation of their preliminary understanding of the design of IS controls, to the extent relevant to the audit objectives:
  - Identification of entitywide level controls (and appropriate system level controls) designed to achieve the control activities for each critical element within each general control area and a determination of whether they are designed effectively and implemented (placed in operation), including identification of control activities for which there are no or ineffective controls at the entitywide level and the related risks;
  - Identification of business process level controls for key applications identified as key areas of audit interest, determination of where those controls are implemented (placed in operation) within the entity's systems, and the auditor's conclusion about whether the controls are designed effectively, including identification of control activities for which there are no or ineffective controls and the related risks and the potential impact of any identified design weaknesses on the completeness, accuracy, validity, and confidentiality of application data;
  - Any internal or third-party information systems reviews, audits, or specialized systems testing (e.g., penetration tests, disaster recovery tests, and application-specific tests) performed during the last year;
  - Management's plans of action and milestones, or their equivalent, that identify corrective actions planned to address known IS control weaknesses;
  - Status of the prior years' audit findings;
  - Documentation for any significant computer security related incidents identified and reported for the last year;
  - Documented security plans;
  - Documented risk assessments for relevant systems (e.g., general support systems and major applications);

- System certification and accreditation documentation or equivalent for relevant systems;
- Documented business continuity of operations plans and disaster recovery plans; and
- A description of the entity's use of third-party IT services

- Relevant laws and regulations and their relation to the audit objectives.
- Description of the auditor's procedures to consider the risk of fraud, any fraud risk factors that the auditor believes could affect the audit objectives, and planned audit procedures to detect any fraud significant to the audit objectives.
- Audit resources planned.
- Current multiyear testing plans.
- Documentation of communications with entity management.
- If IS controls are performed by service organizations, conclusions whether such controls are significant to the audit objectives and any audit procedures performed with respect to such controls (e.g., review of service auditor reports)
- If the auditor plans to use the work of others, conclusions concerning the planned use of the work of others and any audit procedures performed with respect to using the work of others.
- Audit plan (and for financial audits, audit strategy) that adequately describes the objectives, scope, and methodology of the audit.
- Any decision to reduce testing of IS controls due to the identification of significant IS control weaknesses.

2.2 Perform Information System Controls Audit Tests

2.2.1 Overview

In the testing phase of the IS controls audit, the auditor uses information obtained in the planning phase to test the effectiveness of IS controls that are relevant to the audit objectives. As audit evidence is obtained through performing control testing, the auditor should reassess the audit plan and consider whether changes are appropriate.

While determining whether IS controls are appropriately designed and implemented and while performing tests of IS controls, the auditor should periodically assess the cumulative audit evidence obtained to identify any revisions needed to the audit plan. For example, if significant weaknesses have been identified, the auditor may decide to perform less testing in remaining areas if audit objectives have been achieved. Conversely, the performance of tests may uncover additional areas to be tested.

For those IS controls that the auditor determines are properly/suitably designed and implemented, the auditor determines whether to perform tests of the operating effectiveness of such controls. In determining whether to test the operating effectiveness of IS controls, the auditor should determine whether it is possible and practicable to obtain sufficient, appropriate audit evidence without testing IS controls. For federal financial statement audits and for Single Audits (compliance requirements), the auditor is required to test controls that are suitably designed and implemented to achieve a low assessed level of control risk.

As discussed in Chapter 1, this manual is organized in a hierarchical structure to assist the auditor in performing the IS controls audit. Chapter 3 provides information concerning the general controls, and Chapter 4 provides information concerning four business process application level controls. Each of the chapters contains several control categories, which are groupings of related controls pertaining to similar types of risk. For each control category, this manual discusses the key underlying concepts and associated risks if the controls in the category are ineffective.

Chapter 3 is organized by five general control categories:

- security management,
- access controls,
- configuration management,
- segregation of duties, and
- contingency planning.

Chapter 4 is organized into four business process application level control categories:

- business process application level general controls[48] (also referred to as application security),
- business process controls,
- interface and conversion controls, and
- data management systems controls.

The last three business process application level control categories are collectively referred to herein as "business process application controls."

For each control category, the manual identifies critical elements—tasks that are essential for establishing adequate controls within the category. For each critical element, there is a discussion of the associated objectives, risks, and control activities, as well as related potential control techniques and suggested audit procedures. This hierarchical structure facilitates the auditor's analysis of identified control weaknesses.

Because control activities are generally necessary to achieve the critical elements, they are generally relevant to a GAGAS audit unless the related control category is not relevant, the audit scope is limited, or the auditor determines that, due to significant IS control weaknesses, it is not necessary to assess the effectiveness of all

[48]The first category of business process controls is defined as general controls operating at the business process application level.

relevant IS controls. Within each relevant control activity, the auditor should identify control techniques implemented by the entity and determine whether the control techniques, as designed, are sufficient to achieve the control activity, considering IS risk and the audit objectives. The auditor may be able to determine whether control techniques are sufficient to achieve a particular control activity without evaluating and testing all of the control techniques. Also, depending on IS risk and the audit objectives, the nature and extent of control techniques necessary to achieve a particular control objective will vary.

As discussed in Chapter 1, the FISCAM lists specific control activities and techniques and related suggested audit procedures. These are described at a high level and assume some level of expertise for an auditor to perform these audit procedures effectively. Accordingly, the auditor, applying judgment, should develop more detailed audit steps and tailor control activities based on the specific software and control techniques employed by the entity, the audit objectives, and significant areas of audit interest. Further, the auditor is responsible for identifying any necessary changes to IS control-related criteria, including changes to control activities and techniques, based on publications issued after December 2008. Future updates to the FISCAM, including any implementation tools and related materials, will be posted to the FISCAM website at http://www.gao.gov/special.pubs/fiscam.html.

Also, the auditor should evaluate the nature and extent of testing performed by the entity. Such information can assist in identifying key controls and in assessing risk, but the auditor should not rely on testing performed by the entity in lieu of appropriate auditor testing.

As discussed later in this section, if the control techniques implemented by the entity, as designed, are not sufficient to address the control activity, or the control techniques are not effectively implemented as designed, the auditor should determine the effect on IS controls and the audit objectives.

The auditor identifies control techniques and determines the effectiveness of controls at each of the following levels:

- Entitywide or component level (general controls) Controls at the entity or component level consist of the entitywide or componentwide processes designed to achieve the control activities. They are focused on how the entity or component manages IS related to each general control activity in Chapter 3. For example, the entity or component may have an entitywide process for configuration management, including establishment of accountability and responsibility for configuration management, broad policies and procedures, development and implementation of monitoring programs, and possibly centralized configuration management tools. The absence of entitywide processes may be a root cause of weak or inconsistent controls; for example, by increasing the risk that IS controls are not applied consistently across the organization.

- System level (general controls). Controls at the system level consist of processes for managing specific system resources related to either a general support system or major application. These controls are more specific than those at the entity or component level and generally relate to a single type of technology. Within the system level are three further levels that the auditor should assess: network, operating system, and infrastructure application. The three sublevels can be defined as follows:
  - *Network*. A network is an interconnected or intersecting configuration or system of components. For example, a computer network allows applications operating on various computers to communicate.
  - *Operating system*. An operating system is software that controls the execution of computer programs and may provide various services. For example, an operating system may provide services such as resource allocation, scheduling, input/output control, and data management.
  - *Infrastructure applications*. Infrastructure applications are software that is used to assist in performing systems operations, including management of network devices. These applications include databases, e-mail, browsers, plug-ins,

utilities, and applications not directly related to business processes. For example, infrastructure applications allow multiple processes running on one or more machines to interact across a network.

For an example of the identification of system level controls, take configuration management. The auditor who is evaluating configuration management at the system level should determine whether the entity has applied appropriate configuration management practices for each significant type of technology (e.g., firewalls, routers) in each of the three sublevels (e.g., specific infrastructure applications). Such configuration management practices typically include standard configuration guidelines for the technology and tools to effectively determine whether the configuration guidelines are effectively implemented.

- Business process application level. Controls at the business process application level consist of policies and procedures for controlling specific business processes. For example, the entity's configuration management should reasonably ensure that all changes to application systems are fully tested and authorized.

Chapter 3 includes general control activities that are applicable to the entitywide and system levels, and Chapter 4 includes the general controls applied at the business process application level (also referred to as application security) as well as the three categories of business process application controls. The control techniques for achieving the control activities and the related audit tests vary according to the level to which they are being applied. However, they are described at a high level in this manual, and these descriptions assume some expertise about the subject to be effectively performed. Thus, the auditor should develop more detailed audit steps based on the entity's specific software and control techniques, after consulting with the financial or performance auditor about audit objectives and significant areas of audit interest. This manual lists specific control activities and techniques and related suggested audit procedures. Table 1 shows the control categories applicable at each level.

Table 1: Control Categories Applicable at Different Levels of Audit

	Control Categories	Entitywide/ Component Level	System Level			Business Process Application Level
			Network	Operating Systems	Infrastructure Applications	
General Controls	Security Management	→	→	→	→	→
	Access Controls	→	→	→	→	→
	Configuration Management	→	→	→	→	→
	Segregation of Duties	→	→	→	→	→
	Contingency Planning	→	→	→	→	→
Business Process Application Controls	Business Process Controls					→
	Interfaces					→
	Data Management Systems					→

Source: GAO.

The auditor should evaluate the effectiveness of IS controls including system and/or application level controls related to each critical control point. The auditor should evaluate all potential ways in which the critical control point could be accessed. Generally, for each critical control point, this would include assessing controls

related to the network, operating system, and infrastructure application components. For example, if a particular router was deemed to be a critical control point, the auditor generally should test controls related to the router itself (a network component), its operating system, and the infrastructure application that is used to manage the router. Access to any of these could lead to access to the control point. See the discussion of control dependencies in the above section entitled “Identify Critical Control Points”.

As discussed in audit planning (section 2.1.2), the auditor determines the appropriate scope of the IS controls audit, including

- the organizational entities to be addressed (e.g., entitywide, selected component(s), etc.);
- the breadth of the audit (e.g., overall conclusion on IS control effectiveness, review of a specific application or technology area, such as wireless or UNIX, etc.);
- the types of IS controls to be tested:
- general and/or business process application level controls to be tested, or selected components; or
- all levels of the entity’s information systems, or selected levels (e.g., entitywide, system level, or business process application level, or selected components of them.

The auditor should perform the following procedures as part of testing the effectiveness of information system controls:

- Understand information systems relevant to the audit objectives, building on identification of key areas of audit interest and critical control points.
- Determine which IS control techniques are relevant to the audit objectives. The control categories, critical elements, and control activities in Chapters 3 and 4 are generally relevant to all audits. However, if the auditor is not performing a comprehensive audit, for example, an application review, then there may be no need to assess controls in Chapter 3.
- For each relevant IS control technique, determine whether it is suitably designed to achieve the critical activity and has been implemented — placed in operation (if not done earlier).

- Perform tests to determine whether such control techniques are operating effectively.
- Identify potential weaknesses in IS controls. For each potential weakness, consider the impact of compensating controls or other factors that mitigate or reduce the risks related to potential weaknesses.

Understand Information Systems Relevant to the Audit Objectives

The auditor should obtain and document an understanding of the information processing steps performed in information systems that are significant to the audit objectives, including:

- The manner in which transactions are initiated;
- The nature and type of records and source documents;
- The processing involved from the initiation of transactions to their final processing, including the nature of computer files and the manner in which they are accessed, updated, and deleted; and
- For financial audits, the process used to prepare the entity's financial statements and budget information, including significant accounting estimates, disclosures, and computerized processing.

This understanding builds on information obtained in audit planning (e.g., identification of key areas of audit interest and critical control points). For efficiency, the auditor may combine this step with audit planning to aid in the identification of relevant controls. The auditor should perform and document walk-throughs for all business process applications that are significant to the audit objectives. Walk-throughs are important for understanding the information processing and for determining appropriate audit procedures.

Identify IS Control Techniques That Are Relevant to the Audit Objectives

Based on the results of audit planning and other procedures performed, the auditor should identify the control categories, critical elements, control activities, and control techniques that are relevant to the IS audit. In doing this, the auditor considers the audit

objectives and audit scope, the extent of IS risk and the preliminary understanding of IS controls. The process for identifying relevant control techniques is summarized below.

For IS audits that are stand alone GAGAS audits, generally all of the control categories, critical elements, and control activities are relevant to the audit objectives, unless specifically not part of the audit objectives. For example, in an evaluation of the effectiveness of business process controls in a specific application, the general controls in Chapter 3 may or may not be part of the audit objectives.

At the entitywide level and for each critical control point (including control dependencies) at the system and business process application levels, the auditor should identify and document the control techniques used by the entity to achieve each relevant control activity. For purposes of illustration, using the example of the router that is a critical control point (as discussed in section 2.1.7), the auditor would identify and document the control techniques used by the entity to achieve the control activities related to each relevant control category and critical element for the router and for the related control dependencies.

If the IS audit is part of a broader financial audit, performance audit, or attestation engagement, the auditor should obtain, from the overall audit team, audit documentation that identifies internal controls that are significant to the audit objectives. For financial audits performed under the FAM, such controls are identified in the SCE form. For each internal control technique that is identified as significant to the audit objectives (significant control technique) , the audit team should determine whether it is an IS control. An IS controls specialist generally should review and concur with the audit team's identification of IS controls, particularly with respect to whether all IS controls were properly identified as such.

The auditor should identify and document the other entitywide, system, and business process level IS controls upon which the effectiveness of each significant IS control technique depends. These other IS controls will principally relate to the entitywide level controls and to controls over each of the critical control points (including control dependencies) at the system and business process application levels. For example, if the IS control is the

review of an exception report, the auditor should identify and test the business process application controls directly related to the production of the exception report, as well as the general and other business process application controls upon which the reliability of the information in the exception report depends, including the proper functioning of the business process application that generated the exception report and the reliability of the data used to generate the exception report. In addition, the auditor should test the effectiveness of the user control (i.e., management review and followup on the items in the exception report).

For each relevant IS control technique, the auditor should determine whether it is (1) designed effectively to achieve the related control activity, considering IS risk and the audit objectives, and (2) implemented (placed in operation). The auditor may be able to determine whether control techniques are sufficient to achieve a particular control activity without evaluating and testing all of the control techniques. Also, depending on IS risk and the audit objectives, the nature and extent of control techniques necessary to achieve a particular control objective will vary.

The auditor generally should evaluate the design effectiveness and test only the control techniques necessary to achieve the relevant audit activities. For example, if there are two control techniques, each of which individually would achieve the control activity, the auditor generally would evaluate and test only one control technique. However, if the auditor determines that the control technique evaluated and tested was not effective, the auditor would consider the effectiveness of the other control technique.

Also, the auditor should evaluate the nature and extent of testing performed by the entity. Such information can assist in identifying key controls and in assessing risk, but the auditor should not rely on testing performed by the entity in lieu of appropriate auditor testing. If the control techniques implemented by the entity, as designed, are not sufficient to address the control activity, or the control techniques are not effectively implemented as designed, the auditor should determine the effect on IS controls and the audit objectives.

For efficiency, the auditor may implement a tiered approach to the identification and evaluation of the design effectiveness of relevant

IS control techniques, as discussed later in this session, beginning with entitywide level controls, followed by system level controls, then by business process application level controls.

Appendices II and III may be used to identify and summarize relevant IS controls at the entitywide, system, and business process application levels.

Test Information System Controls

The auditor should design and conduct tests of relevant control techniques that are effective in design to determine their effectiveness in operation.

It is generally more efficient for the auditor to test IS controls on a tiered basis, starting with the general controls at the entitywide and system levels, followed by the general controls at the business process application level, and concluding with tests of business process application, interface, and data management system controls at the business process application level. Such a testing strategy may be used because ineffective IS controls at each tier generally preclude effective controls at the subsequent tier.

If the auditor identifies IS controls for testing, the auditor should evaluate the effectiveness of

- general controls at the entitywide and system level;
- general controls at the business process application level; and
- specific business process application controls (business process controls, interface controls, data management system controls), and/or user controls, unless the IS controls that achieve the control objectives are general controls.

The auditor should determine whether entitywide and system level general controls are effectively designed, implemented, and operating effectively by

- identifying applicable general controls;
- determining how those controls function, and whether they have been placed in operation; and
- evaluating and testing the effectiveness of the identified controls.

The auditor should document the understanding of general controls and should conclude whether such controls are effectively designed, placed in operation, and, for those controls tested, operating as intended.

Based on the results of the IS controls audit tests, the auditor should determine whether the control techniques are operating effectively to achieve the control activities. Controls that are not properly designed to achieve the control activities or that are not operating effectively are potential IS control weaknesses. For each potential weakness, the auditor should determine whether there are specific compensating controls or other factors that could mitigate the potential weakness. If the auditor believes that the compensating controls or other factors could adequately mitigate the potential weakness and achieve the control activity, the auditor should obtain evidence that the compensating or other control is effectively operating and actually mitigates the potential weakness. If it effectively mitigates the potential weakness, the auditor can conclude that the control activity is achieved; however, the auditor may communicate such weaknesses to the entity. If the potential weakness is not effectively mitigated, the potential weakness is an actual weakness. The auditor evaluates its effects on IS controls in combination with other identified weaknesses in the reporting phase.

Tests of General Controls at the Entitywide and System Levels

The auditor may test general controls through a combination of procedures, including observation, inquiry, inspection (which includes a review of documentation on systems and procedures), and reperformance using appropriate test software. Although sampling is generally not used to test general controls, the auditor may use sampling to test certain controls, such as those involving approvals.

If general controls at the entitywide and system levels are not effectively designed and operating as intended, the auditor will generally be unable to obtain satisfaction that business process application-level controls are effective. In such instances, the

auditor should (1) determine and document the nature and extent of risks resulting from ineffective general controls and (2) identify and test any manual controls that achieve the control objectives that the IS controls were to achieve.

However, if manual controls do not achieve the control objectives, the auditor should determine whether any specific IS controls are designed to achieve the objectives. If not, the auditor should develop appropriate findings principally to provide recommendations to improve internal control. If specific IS controls are designed to achieve the objectives, but are in fact ineffective because of poor general controls, testing would typically not be necessary, except to support findings.

Tests of General Controls at the Business Process Application Level

If the auditor reaches a favorable conclusion on general controls at the entitywide and system levels, the auditor should evaluate and test the effectiveness of general controls for those applications within which business process application controls or user controls are to be tested. These business process application level general controls are referred to as Application Security (AS) controls in Chapter 4.

If general controls are not operating effectively within the business process application, business process application controls and user controls generally will be ineffective. If the IS controls audit is part of a financial or performance audit, the IS controls specialist should discuss the nature and extent of risks resulting from ineffective general controls with the audit team. The auditor should determine whether to proceed with the evaluation of business process application controls and user controls.

Tests of Business Process Application Controls and User Controls

The auditor generally should perform tests of those business process application controls (business process, interface, data management), and user controls necessary to achieve the control objectives where the entitywide, system, and application-level general controls were determined to be effective.

If IS controls are not likely to be effective, the auditor should obtain a sufficient understanding of control risks arising from information systems to

- identify the impact on the audit objectives,
- design audit procedures, and
- develop appropriate findings.

Also, in such circumstances, the auditor considers whether manual controls achieve the control objectives, including manual controls that may mitigate weaknesses in IS controls. If IS controls are not likely to be effective and if manual controls do not achieve the control objectives, the auditor should identify and evaluate any specific IS controls that are designed to achieve the control objectives to develop recommendations for improving internal controls.

IS controls that are not effective in design do not need to be tested. If the auditor determined in a prior year that controls in a particular accounting application were ineffective and if management indicates that controls have not significantly improved, the auditor need not test them.

2.2.2 Nature, Timing, and Extent of Control Tests

To assess the operating effectiveness of IS controls, auditors should perform an appropriate mix of audit procedures to obtain sufficient, appropriate evidence to support their conclusions. Such procedures could include the following:

- Inquiries of IT and management personnel can enable the auditor to gather a wide variety of information about the operating effectiveness of control techniques. The auditor should corroborate responses to inquiries with other techniques.
- Questionnaires can be used to obtain information on controls and how they are designed.
- Observation of the operation of controls can be a reliable source of evidence. For example, the auditor may observe the verification of edit checks and password controls. However, observation provides evidence about controls only when the

auditor was present. The auditor needs other evidence to be satisfied controls functioned the same way throughout the period.

- The auditor may review documentation of control polices and procedures. For example, the entity may have written policies regarding confidentiality or logical access. Review of documents will allow the auditors to understand and assess the design of controls.
- Inspection of approvals/reviews provides the auditor with evidence that management is performing appropriate control checks. The auditor may combine these tests with discussions and observations.
- Analysis of system information (e.g., configuration settings, access control lists, etc.) obtained through system or specialized software provides the auditor with evidence about actual system configuration.
- Data review and analysis of the output of the application processing may provide evidence about the accuracy of processing. For example, a detailed review of the data elements or analytical procedures of the data as a whole may reveal the existence of errors. Computer-assisted audit techniques (CAAT) may be used to test data files to determine whether invalid transactions were identified and corrected by programmed controls. However, the absence of invalid transactions alone is insufficient evidence that the controls effectively operated.
- Reperformance of the control could be used to test the effectiveness of some programmed controls by reapplying the control through the use of test data. For example, the auditor could prepare a file of transactions that contains known errors and determine if the application successfully captures and reports the known errors.

In assessing the operating effectiveness of IS controls, the auditor may determine that it is appropriate to attempt to gain access to identified key systems (e.g., vulnerability assessments or penetration tests). Consideration should be given to performing this type of tests when (1) a new system is developed or major system upgrade occurs, (2) major changes are made to the environment the system operates, and (3) serious weaknesses are identified that may

impact the system. See NIST SP 800-53A, Appendix G for further guidance on penetration testing. In performing this testing, it is important that the auditor and entity management have a common understanding of the type of tests to be performed, scope of the tests, and the risks involved in performing this testing. See SM-5 for further discussion of vulnerability assessments and section 2.1.9.F. concerning communication with entity management.

In determining the appropriate timing for tests of IS controls, the auditor should consider appropriate factors, including, among other things, whether the audit objectives relate to a specific point in time or to a period of time, the nature of the evidential matter that is available (evidence of the proper operation of many IS controls is available only at the time of the test), the extent of information system risk, the significance or criticality of the IS control to the audit objectives, and the effectiveness of entitywide and security management controls in reasonably assuring that IS controls operated consistently during the relevant period.

Audit procedures may include a selection of specific items (e.g., access forms). In addition, the auditor may need to determine, among multiple instances of a type of network component, which specific components to test. For example, the entity may have many internet access points or multiple instances of a data base. The auditor should exercise judgment in determining the number of items to select and the method used to select them. Generally, such judgment would include consideration of the related information system risk, the significance or criticality of the specific items in achieving the related control objectives, the location of the network component in relation to the key areas of audit interest, and the extent of consistency in the configuration of the components.

2.2.3 Documentation of Control Testing Phase

Information developed in the testing phase that the auditor should document includes the following:

- An understanding of the information systems that are relevant to the audit objectives
- IS Control activities relevant to the audit objectives
- By level (e.g., entitywide, system, business process application) and system sublevel (e.g., network, operating system, infrastructure applications), a description of control techniques used by the entity to achieve the relevant IS control objectives and activities
- By level and sublevel, specific tests performed, including
  - related documentation that describes the nature, timing, and extent of the tests;
  - evidence of the effective operation of the control techniques or lack thereof (e.g., memos describing procedures and results, output of tools and related analysis);
  - if a control is not achieved, any compensating controls or other factors and the basis for determining whether they are effective;
  - the auditor's conclusions about the effectiveness of the entity's IS controls in achieving the control objective; and
  - for each weakness, whether the weakness is a material weakness, significant deficiency or just a deficiency, as well as the criteria, condition, cause, and effect if necessary to achieve the audit objectives. The aggregate effect of all weaknesses is evaluated in the next section (2.3).

Appendices II and III may be used to summarize the results of testing.

2.3 Report Audit Results

After completing the testing phase, the auditor summarizes the results of the audit, draws conclusions on the individual and aggregate effect of all identified IS control weaknesses on audit risk and audit objectives and reports the results of the audit. Such evaluation includes consideration of (1) the effect of weaknesses identified by the auditor's current testing, (2) followup on weaknesses reported in previous audits or evaluations that are relevant to the audit objectives, and (3) other uncorrected weaknesses that have been identified and/or reported by management or others that are relevant to the audit objectives. The auditor evaluates the effect of any weaknesses on the entity's ability to achieve each of the critical elements in Chapters 3 and 4 and on the risk of unauthorized access to key systems or files. Also, the auditor evaluates potential control dependencies.

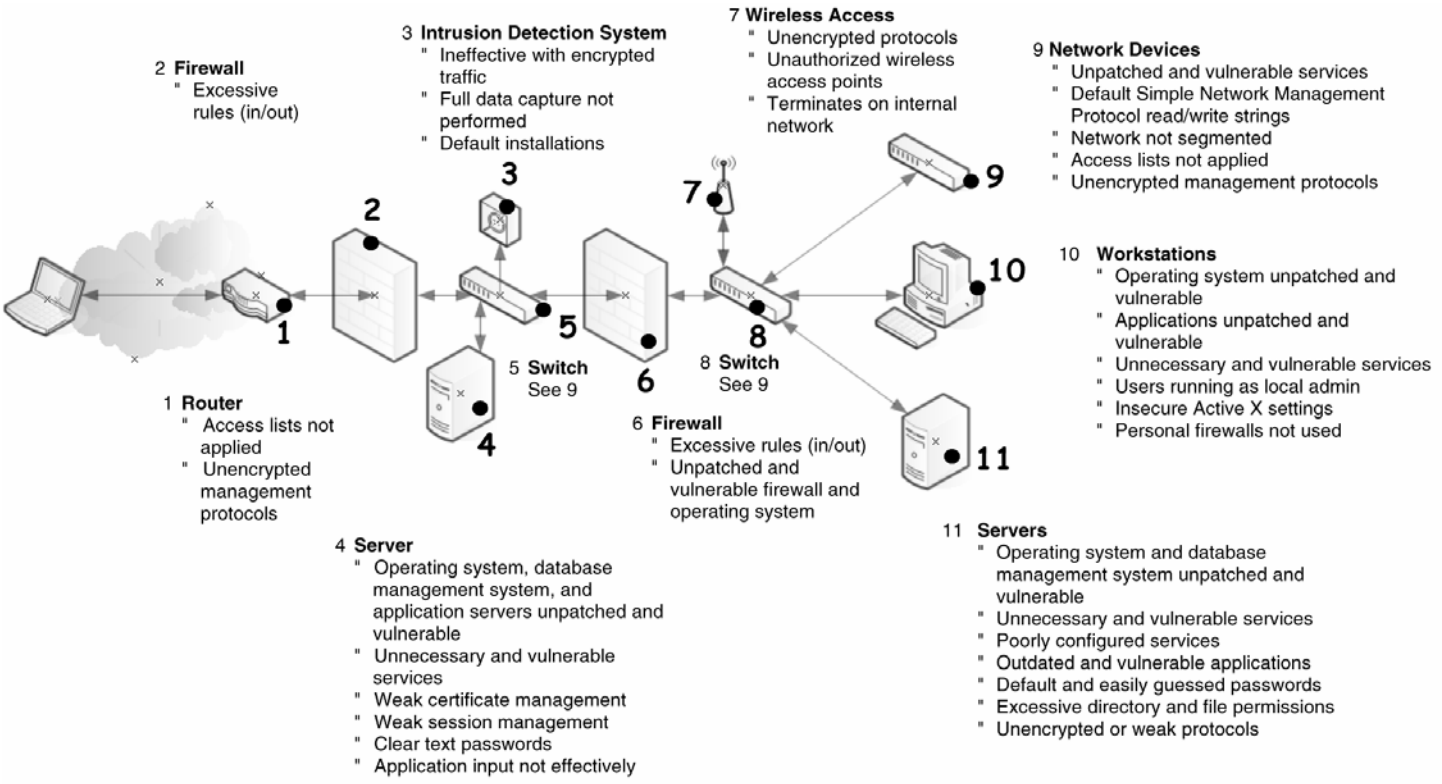
For each critical element, the auditor should make a summary determination as to whether the critical element is achieved, considering entitywide, system, and business process application levels collectively. The auditor should evaluate the effect of related underlying control activities that are not achieved. In addition, based on identified weaknesses, the auditor should determine the effectiveness of IS controls for each of the five categories of general controls or the four categories of application-level controls. If a critical element is not achieved, then (1) the respective control category is not likely to be achieved and (2) in the absence of strong compensating controls, overall IS controls are unlikely to be effective. If one or more of the nine control categories are not effectively achieved, IS controls are ineffective, unless other factors sufficiently reduce the risk. The auditor uses professional judgment in making such determinations. Also, the auditor should determine whether IS control weaknesses identified by the audit were identified in the entity's Plans of Action and Milestones (POA&Ms) or equivalent document. If not, the auditor generally should attempt to determine why they were not identified by the entity as appropriate and report weaknesses in the reporting process.

Also, the auditor should evaluate whether the aggregate combination of weaknesses could result in unauthorized access to

systems or files supporting key areas of audit interest, resulting in a significant internal control deficiency. Guidance for evaluating IS controls and determining the appropriate reporting are discussed separately for financial audits and attestation engagements and for performance audits in the following sections.

For example, a series of weaknesses might result in individuals having the ability to gain unauthorized external access to entity systems, escalate their privileges to obtain a significant level of access to critical control points, and consequently achieve access to key areas of audit interest. The auditor can use simplified network schematics annotated with weaknesses related to key system components to document the impact of a series of weaknesses. Such documentation may be developed as the audit progresses, allowing the auditor to demonstrate on the system that the weaknesses in fact exist and can be exploited to achieve the expected result. Also, such documentation can assist in communicating the related risks to entity management. Figure 3 is an example of a simplified network schematic annotated with weaknesses related to key system components.

Figure 3. Example of Network Schematic Describing System Weaknesses



Source: GAO and Visio.

Further, the auditor should evaluate the potential impact of any identified weaknesses on the completeness, accuracy, validity, and confidentiality of application data relevant to the audit objectives. (See Chapter 4 for a description of completeness, accuracy, validity, and confidentiality.)

When IS controls audits are performed as part of a broader financial or performance audit or attestation engagement, the auditor should coordinate with the audit team to determine whether significant controls are dependent on IT processing. In very rare circumstances, the auditor may determine that IS controls, in the aggregate, are ineffective, but that the entity has overall compensating controls not dependent on IT processing or that other factors mitigate or reduce the risks arising from IS control weaknesses. For example, manual reviews of support for all disbursements could mitigate certain IS risks related to a

disbursement system. If compensating controls or other factors are present, the auditor should document such controls or factors, test them appropriately to determine whether they effectively mitigate the identified IS control weaknesses, and draw conclusions about the nature and extent of the risks that remain after considering such controls or factors.

As noted earlier in the section entitled "Understand the Overall Audit Objectives and Related Scope of the Information System Controls Audit," if achieving the audit objectives does not require an overall conclusion on IS controls or only relates to certain components of the entity or a subset of controls, the auditor's assessment would not necessarily identify all significant IS control weaknesses. For example, a limited review of controls over a type of operating system may not identify any significant weaknesses, although there may be very significant weaknesses in other areas that the auditor may not be aware of because of the limited scope of the audit. Consequently, the auditor should evaluate the potential limitations of the auditor's work on the auditor's report and the needs and expectations of users. The auditor may determine that, because the limitations are so significant, the auditor (1) will communicate the limitations to the audited entity, those charged with governance, and those requesting the audit and (2) clearly report such limitations on the conclusions in the audit report. For example, in reporting on an audit of an operating system, the auditor may determine that it is appropriate to clearly report that the scope of the assessment was limited to the operating system and that, consequently, additional IS control weaknesses may exist that could impact the effectiveness of IS controls related to the operating system and to the entity as a whole.

The auditor should express the effect of identified IS control weaknesses in terms of the audit objectives. The following sections provide guidelines for assessing IS controls in financial and performance audits. For financial audits and attestation engagements, GAGAS states that auditors should report material weaknesses and other significant deficiencies.

2.3.1 Financial Audits and Attestation Engagements

The auditor should conclude whether IS control weaknesses, individually or in the aggregate, constitute a significant deficiency or material weakness in financial reporting. The auditor should coordinate these procedures with the overall audit team. For financial audits, GAGAS and OMB Circular A-123 state that a control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. A deficiency in design exists when (*a*) a control necessary to achieve the control activity is missing or (*b*) an existing control is not properly designed so that even if the control operates as designed, the control activity is not always achieved. A deficiency in operation exists when a properly designed control does not operate as designed or when the person performing the control does not possess the necessary authority or qualifications to perform the control effectively. In addition, in financial audits of federal entities, the auditor should evaluate the effect of IS control weaknesses on FFMIA and FMFIA reporting.

GAGAS uses the following definitions and guidelines for classifying internal control weaknesses for financial audits and attestation engagements:

A **significant deficiency** is a deficiency in internal control, or combination of deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles (or in accordance with the applicable criteria or framework for attestation engagements) such that there is more than a remote likelihood[49] that a misstatement of the entity's financial statements (or misstatement of the subject matter for attestation engagements)

[49]The term "more than remote" used in the definitions for significant deficiency and material weakness means "at least reasonably possible." The following definitions apply: (1) Remote—The chance of the future events occurring is slight. (2) Reasonably possible—The chance of the future events or their occurrence is more than remote but less than likely. (3) Probable—The future events are likely to occur.

that is more than inconsequential[50] will not be prevented or detected.

A **material weakness** is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements (or misstatement of the subject matter for attestation engagements) will not be prevented or detected.

OMB Circular A-123 uses the same definition for significant deficiency, but continues to refer to it as a reportable condition.

In determining whether IS control deficiencies, individually or in the aggregate, constitute a significant deficiency or material weakness, the auditor should evaluate several factors, including the following:

- The likelihood that an individual could obtain unauthorized access to or perform unauthorized or inappropriate activities on key entity systems or files that could affect information recorded in the financial statements. This might include (1) the ability to obtain root access to systems that house key financial systems (including feeder systems), thereby enabling unauthorized users to read, add, delete, modify, or exfiltrate financial data either directly or through the introduction of unauthorized software; (2) the ability to directly access and modify files containing financial information; or (3) the ability to assign unauthorized application user rights, thereby entering unauthorized transactions.
- The nature of unauthorized access that could be obtained (e.g., limited to system or application programmers or system administrators; all authorized system users; or anyone through

[50]The phrase "more than inconsequential" as used in the definition of significant deficiency describes the magnitude of potential misstatement that could occur as a result of a significant deficiency and serves as a threshold for evaluating whether a control deficiency or combination of control deficiencies is a significant deficiency. A misstatement is "inconsequential" if a reasonable person would conclude, after considering the possibility of further undetected misstatements, that the misstatement, either individually or when aggregated with other misstatements, would clearly be immaterial to the financial statements. If a reasonable person would not reach such a conclusion regarding a particular misstatement, that misstatement is more than inconsequential.

unauthorized external access through the Internet) or the nature of unauthorized or inappropriate activity that could be performed.

- The likelihood that financial statement amounts could be materially affected.
- The likelihood that other controls including business process application controls would prevent or detect such unauthorized access. Generally, if the effectiveness of such other controls depends on computer processed information, it is unlikely that they could effectively prevent or detect such access; unless the identified IS control weaknesses could not reasonably result in the ability to compromise such other controls.
- The risk that management could override controls (such as through excessive access rights).

Based upon these considerations, the auditor should determine whether IS control deficiencies, individually or in the aggregate, are a material weakness or significant deficiency. Also, the auditor should evaluate whether significant deficiencies, in combination, result in material weaknesses. If so, the auditor should determine them to be material weaknesses in drawing conclusions as to the effectiveness of internal control and reporting findings, as discussed in FAM paragraphs 580.42–.48 and 580.51–.58. If the control deficiencies constitute a material weakness, the auditor should conclude that internal controls are not effective.

Financial auditors may take one of two different approaches to reporting on internal control: (1) express an opinion on internal control (see FAM paragraphs 580.38-.48) or (2) report weaknesses found, categorized as material weaknesses or other significant deficiencies, but do not give an opinion (see FAM paragraphs 580.49-.50). GAO auditors generally express an opinion on internal control. In either case, the auditor considers whether internal control is sufficient to meet the following control objectives insofar as those objectives pertain to preventing or detecting misstatements, losses, or noncompliance that would be material in relation to the financial statements:

- Reliability of financial reporting—transactions are properly recorded, processed, and summarized to permit the preparation of the financial statements and supplemental information in accordance with Generally Accepted Accounting Principles (GAAP), and assets are safeguarded against loss from unauthorized acquisition, use, or disposition.
- Compliance with applicable laws and regulations—transactions are executed in accordance with laws governing the use of budget authority; other laws and regulations that could have a direct and material effect on the financial statements or required supplementary information (RSI); and any other laws, regulations, and governmentwide policies identified by OMB in its audit guidance.

The auditor may report weaknesses that do not meet the criteria for significant deficiencies in a letter to management or orally to an appropriate level of the entity. The auditor may include suggestions for corrective action for these less significant weaknesses if enough is understood about their cause. (More detailed information on how and where to report control weaknesses for financial statement audits is presented in sections 580.48 through 580.52 of the FAM.)

Note that SAS 115, issued in October 2008, which is incorporated into GAGAS, revised the definitions of material weakness and significant deficiency for financial audits. The SAS is effective for audits of financial statements for periods ending on or after December 15, 2009. The revised definitions are as follows:

- A material weakness is a deficiency, or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis.
- A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Check the FISCAM website for any updates at http://www.gao.gov/special.pubs/fiscam.html.

2.3.2 Performance Audits

The auditor should draw conclusions on the effectiveness of IS controls relevant to the audit objectives. Depending on the audit objectives, the auditor's report will vary. For example, the auditor's report may

- provide an overall conclusion (e.g., the entity's IS controls are or are not effective in achieving the IS control objectives relevant to the audit) and communicate identified weaknesses;
- limit reporting to identified weaknesses without providing an overall conclusion (e.g., "based on our work, we identified the following IS control weaknesses"); or
- if in support of a broader performance audit, report findings in the context of the audit objectives, such as how they relate to the assessment of the reliability of computer-processed data.

GAGAS state that auditors should include in their audit reports the scope of their work on internal control (which includes IS controls) and any deficiencies in internal control that are significant within the context of the audit objectives and based upon the audit work performed. Determining whether and how to communicate to officials of the audited entity internal control deficiencies that have an inconsequential effect on the financial statement or subject matter is a matter of professional judgment. Auditors should document such communications. The auditor may report such inconsequential weaknesses orally to officials of the entity or in a separate written communication.

In determining the significance of the IS control weaknesses, the auditor should evaluate several factors, including the following:

- The likelihood that an individual could obtain unauthorized access to or perform unauthorized or inappropriate activities on key entity systems or files that could affect key areas of audit interest. This might include (1) the ability to obtain root access to systems that house key areas of audit interest (including supporting systems), thereby enabling an intruder to read, add, delete, modify, or exfiltrate data either directly or through the introduction of unauthorized software; (2) the ability to directly

access and modify files related to key areas of audit interest; or (3) the ability to assign unauthorized application user rights, thereby enabling an intruder to enter unauthorized transactions or perform unauthorized activities.

- The nature of unauthorized access that could be obtained (e.g., limited to system or application programmers or system administrators; authorized system users; or anyone through unauthorized external access through the Internet)
- The likelihood that the achievement of the audit objectives would be significantly affected.
- The likelihood that other controls including business process application controls would prevent or detect such unauthorized access. Generally, if the effectiveness of such other controls depends on computer processed information, it is unlikely that they could effectively prevent or detect such access, unless the identified IS control weaknesses could not reasonably result in the ability to compromise such other controls.
- The risk that management could override controls (such as through excessive access rights).

Under GAGAS (Section 8.03), the auditor must issue audit reports communicating the results of each completed performance audit, including GAGAS audits performed to meet FISMA requirements. GAGAS also states that auditors should include in the audit report (1) the scope of their work on internal control and (2) any deficiencies in internal control that are significant within the context of the audit objectives and based upon the work performed. Such deficiencies would include any identified significant internal control deficiencies.

2.3.3 Other Audit Reporting Considerations

It is important to report IS control weaknesses in terms that are understandable to individuals who may have limited expertise regarding information systems issues. In this regard, the auditor generally should define technical terms and avoid jargon and undefined abbreviations and acronyms.

Auditors should develop the elements of the findings to the extent necessary to achieve the audit objectives. The extent to which the auditor should develop the elements for a finding (criteria, condition, cause, and effect) depends on the audit objectives. If auditors are able to sufficiently develop the findings, they should provide recommendations for corrective action if they are significant within the context of the audit objectives.

Criteria describe the required or desired state, or what is expected from the program or operation. Condition is the actual situation. Cause is the factor or factors responsible for the difference between condition and criteria. Effect is the impact of the difference between the condition and the criteria. This information helps senior management understand the significance of the weakness and develop appropriate corrective actions. For most types of IS control weaknesses, this manual includes a discussion of risks and potential negative effects that can be adapted for audit reports. GAO has issued numerous reports that can be used as models for reporting computer-related weaknesses. Current IS reports can be obtained from GAO's report database on GAO's Web site (http://www.gao.gov).

In many cases, auditors will have detailed information on control weaknesses that is too technical to be meaningful to most senior managers and other users of the audit report, but may be valuable to the entity's technical staff to aid in understanding the precise cause of the weaknesses and in developing corrective actions. The auditors generally should provide this information to the entity's technical staff in briefings. The auditor should provide information to technical staff that is in substance the same as that reported to senior management.

The auditor should effectively communicate the results of an IS controls audit to the appropriate persons through appropriate reports. This serves several purposes, including

- informing the audited entity and those charged with governance of control weaknesses; issues of noncompliance with laws, regulations, and provisions of contracts or grant agreements; and instances of fraud, illegal acts, or abuse;

- providing the audited entity with recommendations to correct such control weaknesses;
- providing the financial or performance auditor an understanding of the information systems control environment and the effects of IT on the processing of transactions;
- complying with legal reporting requirements; and
- complying with auditing standards, including generally accepted government auditing standards.

However, the auditor should avoid the disclosure of sensitive IS data. An individual could potentially compromise a system from any location in the world, as long as they have access to a computer and a telephone line or Internet connection. Technical information discussed in an audit report could potentially assist individuals by reducing the time and effort to obtain unauthorized access and compromise a system. Also, to avoid disclosure of sensitive information, the auditor should provide draft IS reports to the entity for a sensitivity review. The auditor should evaluate entity sensitivity concerns and make appropriate report revisions, considering legal or regulatory requirements, including the exercise of information classification authority.

Generally, in the federal environment, either one report with limited distribution or two reports, one of which has limited distribution, are issued. Information systems security audit reports may or may not be put on entity Web sites or released under FOIA, generally depending on the degree or extensiveness of sensitive data. Even though these reports may not be posted on entity Web sites, they are still typically issued to entity management. Also, state laws and regulations may affect the form of reporting. For further information, see *Information Systems Security Auditing: Legal and Reporting Considerations*.[51]

[51]Intergovernmental Information Security Audit Forum (Sept. 11, 2003); see www.nasact.org

2.3.4 Related Reporting Responsibilities

In addition to reporting the results of the audit, the auditor may have other related reporting responsibilities established by law, regulation, or policy. The auditor should identify any other reporting requirements and respond appropriately.

In financial audits of federal entities, the auditor should determine whether the IS control weaknesses, individually or in the aggregate, constitute a material weakness for FMFIA reporting or a lack of substantial compliance of the entity's systems with FFMIA. See FAM 260.53-57 for further information. Also, further information about reporting IS control weaknesses in relation to a financial audit are discussed in FAM 580 (Draft Reports).

OMB Circular A-123 provides requirements for complying with FMFIA. The Circular requires management to assess controls and provide an annual assurance statement on the overall adequacy and effectiveness of internal control within the agency. In addition, management is required to provide a separate assurance statement on the effectiveness of internal control over financial reporting, which includes safeguarding of assets and compliance with applicable laws and regulations. Also, OMB audit guidance requires management to include representations about internal control in its management representation letter to the auditor.

FMFIA requires agencies to evaluate and report on the adequacy of the systems of internal accounting and administrative control. For the *overall assessment* of internal control, OMB Circular A-123 defines a **material weakness** as a reportable condition which the agency head determines to be significant enough to report outside of the agency. It defines a **reportable condition** as a control deficiency, or combination of control deficiencies, that in management's judgment, should be communicated because they represent significant weaknesses in the design or operation of internal control that could adversely affect the organization's ability to meet its internal control objectives. For the *assessment of internal control over financial reporting*, Circular A-123 uses the same definitions for material weakness and significant deficiency described above for financial audits, except that OMB uses the term

reportable condition rather than the term significant deficiency. Also, FMFIA and OMB Circular A-123 require management to report nonconformances with system requirements. The Circular defines nonconformances as instances in which financial management systems do not substantially conform to financial systems requirements. Financial management systems include both financial and financially-related (or mixed) systems.

The auditor should evaluate the material weaknesses reported under FMFIA to determine whether they meet the definitions of material weakness and reportable condition for reporting as part of management's assertion about the effectiveness of internal control.

In addition, the auditor should consider if there are any issues that should be reported under OMB Circular A-127 "Financial Management Systems". This circular prescribes policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems.

FISMA requires federal agencies to report significant deficiencies in information security as material weaknesses under FMFIA and, if relating to financial management systems, as an instance of a lack of substantial compliance of systems with FFMIA. The term "significant deficiency" used in FISMA differs from the same term used in GAGAS. OMB defines a FISMA significant deficiency as "a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken."

FFMIA requires agencies to implement and maintain financial management systems that comply substantially with federal financial management systems requirements, applicable federal accounting standards, and the U.S. Government Standard General

Ledger[52] at the transaction level. FFMIA requires auditors to assess whether an agency's financial management systems substantially comply with system requirements. IS control weaknesses are a major concern for federal agencies and the general public and are one of the frequently cited reasons for noncompliance with FFMIA.

2.3.5 Documentation of Reporting Phase

The auditor should document appropriate IS information developed in the reporting phase, including:

- The auditor's conclusion about the effectiveness of IS controls (in relation to the IS controls audit objectives) in achieving the control categories, critical elements, and the relevant control activities and the basis for the conclusion, including the factors that the auditor considered in making the determination;
- If part of a broader audit, the impact of any identified IS control weaknesses on the overall audit objectives;
- Copies of any reports or written communications issued in connection with the audit, including the draft the entity commented on and entity management comments related to such reports and communications;
- For financial audits and attestation engagements, the auditor's determination of whether identified weaknesses represent material weaknesses or significant deficiencies, and the basis for the auditor's conclusions;
- Other documentation required by the audit organization's policies and procedures, including quality assurance processes;
- Results of procedures to detect any fraud significant to the audit objectives and the impact on the audit;
- Results of audit follow-up procedures to determine whether entity corrective actions have been implemented, to sufficiently remediate previously reported IS control weaknesses; and

[52]The *U.S. Government Standard General Ledger* (SGL) provides a uniform chart of accounts and pro forma transactions used to standardize federal agencies' financial information accumulation and processing throughout the year, enhance financial control, and support budget and external reporting, including financial statement preparation.

- As appropriate, the auditor's considerations and determinations concerning FMFIA, FFMIA, and other reporting responsibilities.

2.4 Documentation

The auditor should adequately document the IS controls audit. GAGAS has general documentation requirements for financial and performance audits and attestation engagements. In summary, they are as follows:

Financial Audits - Auditors must prepare audit documentation in connection with each engagement in sufficient detail to provide a clear understanding of the work performed (including the nature, timing, extent, and results of audit procedures performed), the audit evidence obtained and its source, and the conclusions reached. Auditors should prepare audit documentation that enables an experienced auditor, having no previous connection to the audit, to understand **a.** the nature, timing, and extent of auditing procedures performed to comply with GAGAS and other applicable standards and requirements; **b.** the results of the audit procedures performed and the audit evidence obtained; **c.** the conclusions reached on significant matters; and **d**. that the accounting records agree or reconcile with the audited financial statements or other audited information.

Attestation Engagements - Auditors must prepare attest documentation in connection with each engagement in sufficient detail to provide a clear understanding of the work performed (including the nature, timing, extent, and results of attest procedures performed); the evidence obtained and its source; and the conclusions reached. Auditors should prepare attest documentation in sufficient detail to enable an experienced auditor, having no previous connection to the attestation engagement, to understand from the documentation the nature, timing, extent, and results of procedures performed and the evidence obtained and its source and the conclusions reached, including evidence that supports the auditors' significant judgments and conclusions. Auditors should prepare documentation that contains support for

findings, conclusions, and recommendations before they issue their report.

Auditors also should document the following for attestation engagements performed under GAGAS: **a.** the objectives, scope, and methodology of the attestation engagement; **b.** the work performed to support significant judgments and conclusions, including descriptions of transactions and records examined; **c.** evidence of supervisory review, before the attest report is issued, of the work performed that supports findings, conclusions, and recommendations contained in the attest report; and **d.** the auditors' consideration that the planned procedures are designed to achieve objectives of the attestation engagement when (1) evidence obtained is dependent on computerized information systems, (2) such evidence is material to the objective of the engagement, and (3) the auditors are not relying on the effectiveness of internal control over those computerized systems that produced the evidence. Auditors should document (1) the rationale for determining the nature, timing, and extent of planned procedures; (2) the kinds and competence of available evidence produced outside a computerized information system, or plans for direct testing of data produced from a computerized information system; and (3) the effect on the attestation engagement report if evidence to be gathered does not afford a reasonable basis for achieving the objectives of the engagement.

Performance Audits – Auditors must prepare audit documentation related to planning, conducting, and reporting for each audit. Auditors should prepare audit documentation in sufficient detail to enable an experienced auditor, having no previous connection to the audit, to understand from the audit documentation the nature, timing, extent, and results of audit procedures performed, the audit evidence obtained and its source and the conclusions reached, including evidence that supports the auditors' significant judgments and conclusions. Auditors should prepare audit documentation that contains support for findings, conclusions, and recommendations before they issue their report. Auditors should document the following: **a.** the objectives, scope, and methodology of the audit; **b.** the work performed to support significant judgments and conclusions, including descriptions of transactions and records

examined; and **c.** evidence of supervisory review, before the audit report is issued, of the work performed that supports findings, conclusions, and recommendations contained in the audit report.

In addition to meeting these general requirements, the auditor should include, in IS controls audit documentation, the specific information discussed throughout this chapter, and summarized in Appendix X.

2.5 Other Information System Controls Audit Considerations

In addition to the above, the auditor should apply the following topics and techniques to the extent they are relevant to the entity, the audit objectives, and the audit procedures.

- Additional IS risk factors
- Automated audit tools
- Sampling techniques

Also, guidance is provided to the auditor in the evaluation of IS controls associated with service organizations, Single Audits, and FISMA independent evaluations in Appendix VII, VIII, and IX, respectively.

2.5.1 Additional IS Risk Factors

As part of the risk assessment, the auditor should also evaluate the following additional IS risk factors to the extent that they are relevant to the entity and the audit objectives. The auditor's risk assessment also includes other risk factors not listed here (e.g., Voice over Internet Protocol – VoIP)

2.5.1.A Defense-In-Depth Strategy

Defense-in-Depth is a commonly accepted "best practice" for implementing computer security controls in today's networked environments. In some agencies, the auditor may encounter this strategy as part of the agency's security management program.

Where an effective Defense-in-Depth strategy has been implemented by the entity, the auditor's assessment of IS risk would generally be lower. Conversely, where this strategy is not used, the auditor's assessment of IS risk would generally be higher. The auditor's IS control testing generally provides evidence about the effectiveness of a Defense-in-Depth strategy. See Chapter 3 (AC-1 and CM-5) for additional information on Defense-in-Depth strategy.

According to the National Security Agency, Defense-in-Depth integrates people, operations, and technology capabilities to protect information systems across multiple layers and dimensions. For example, successive layers of defense will cause an adversary who penetrates or breaks down one barrier to promptly encounter successive barriers until the attack ends. The strategy recommends a balance between protection capabilities and cost, performance, and operational considerations.

The people component of Defense-in-Depth begins with a senior-level management commitment (normally at the chief information officer level) that is based on a clear understanding of the perceived threat. This component must be implemented with effective information security policies and procedures, assignment of roles and responsibilities, commitment of resources, training and awareness programs (for both users and system administrators), and personnel accountability, which includes the establishment of physical and personnel security measures to control and monitor access to facilities and critical elements of the information technology environment.

The operations component focuses on all activities required to sustain an entity's security posture on a day-to-day basis. These activities include

- maintaining up-to-date system security policies,
- establishing certification and accreditation programs,
- managing information system security (for example, installing patches and virus updates, maintaining access control lists),
- performing system security assessments (for example, vulnerability assessments),

- auditing and monitoring system activity and responding to threats, and
- implementing recovery and reconstitution procedures in the event of a security breach.

The technology component includes defense in multiple places and layered defense mechanisms that provide intrusion prevention, detection, and response to security incidents. Since attackers may target multiple points in an information system, an entity needs to deploy protection mechanisms at multiple locations including the protection of local and wide area communication networks (for example, from denial of service attacks), protection for data transmitted over the networks (for example, use of encryption and traffic flow security measures), defense of enclave boundaries (for example, deploy firewalls and intrusion detection systems), and defense of the computing environment (for example, access control on hosts and servers). Even the best security products have inherent weaknesses, so it is only a matter of time before an attacker finds an exploitable vulnerability. Therefore, it is important to deploy layered defense mechanisms such as nested firewalls coupled with intrusion detection at outer and inner network boundaries, between the adversary and the target.

2.5.1.B Web Applications

Web applications, which use a web browser as part of the application, present significant additional IS risks because, if not properly controlled, they can expose the application and the entity's systems to unauthorized access. In some instances, the risk related to the application itself may be low because it is not critical or it does not contain sensitive information. However, if not properly controlled, it could be used to obtain unauthorized access to other entity system resources. Therefore, due to the heightened risk, even if a web application itself is not part of the scope of the audit, the auditor should assess the effectiveness of web application security and, as appropriate, general controls to determine whether the information system controls over the application could allow unauthorized access through the application to other system resources.

2.5.1.C ERP Systems

ERP systems present additional IS risks. While IS control objectives contained in the FISCAM, if properly achieved, should address such risks, it is important for the auditor to properly consider how the control objectives are achieved in ERP systems. This section provides some considerations in auditing ERP systems. The auditor should supplement the FISCAM with audit considerations and techniques that are specific to the particular ERP system(s) being audited. Although ERP systems share some similar functionality, the way they are implemented and the audit techniques (e.g., specific system queries, analysis of superuser capabilities) applied will vary with the particular vendor.

Factors affecting the overall risk related to ERP systems include the following:

- ERP systems are highly integrated (e.g., common databases, common security administration) and cover/include/address a broad range of entity activities, which leads to increased risks related to several control areas. For example, an ERP application generally includes a broader cross-section of users in the entity, increasing the need for access (particularly least privilege) and segregation of duties controls. Also, because loss of an ERP system/application can have devastating consequences to an entity, the entity needs effective controls over (1) system development/configuration management controls to provide reasonable assurance that the system will operate as intended, (2) service continuity/contingency planning to recover the more comprehensive ERP systems, and (3) access and other general controls to prevent unauthorized access to entity system resources that could lead to denial of service. Further, general controls over the ERP system and supporting databases and operating systems are important to adequately protect access to the underlying data and processing.
- Because ERP systems are on-line-real-time systems, data validation controls are critical to reasonably assure that only valid data is processed by the ERP systems. Controls in ERP systems tend to be preventive rather than detective, as subsequent detection and correction of errors may be costly or

impossible. Also, fewer controls may be in place as the data is generally entered and validated once.

- The network architectures for ERP systems are typically more distributed, resulting in increased access controls and other risks than for more centralized systems.
- Because security administration is generally centralized and powerful access is provided to system administrators, access controls over security administration and segregation of duties controls are important. In addition, ERP systems have powerful default user IDs that need to be adequately controlled.
- The broader number of users may also lead to an increase in external access (wireless or other remote access), from both a broader range of internal users as well as external users (e.g., vendors, customers), increasing the number of access points to the entity's systems.
- ERP systems typically have limited, if any, paper audit trails. Consequently, controls over audit logs and other general controls are important for the reliability of data in the ERP systems. Also, auditing access to ERP systems is typically performed online.
- In many instances, interfaces are developed between the ERP system and legacy applications. As a result, the adequacy of interface controls and configuration management controls are important to ensure that data from legacy systems is reliable, valid, complete, and properly converted from the legacy application into the ERP system.
- ERP systems may have a program change control module that allows for direct changes to production code. Therefore, controls related to segregation of development, test and production facilities and functions may not be present. Consequently, IS risks related to configuration management and monitoring are increased, and the entity should secure and monitor such modules.

ERP systems contain certain controls that are not changeable by the entity. It is important to understand these controls and how they may help to achieve the IS control objectives.

In addition, due to the increased risks discussed above, there are a number of other controls that are of increased significance in ERP systems, including controls relating to:

- user access to sensitive application capabilities (e.g., pages, screens, transactions, menus, queries), including related segregation of duties
- powerful user roles/profiles, including defaults
- default user IDs and default passwords
- default system configurations
- access to critical tables/databases
- access to log files
- the effectiveness of the settings of configurable controls
- sensitive reports/outputs

2.5.1.D Interface Controls

Interface controls are particularly important when applications rely on input from legacy systems. Such legacy systems are sometimes referred to as feeder systems. In certain instances, such legacy applications may not have been designed to fully achieve the objectives of the application they support. Consequently, the auditor evaluates the adequacy of interface controls and of application controls related to such legacy applications to provide reasonable assurance that data from legacy systems is reliable, valid, complete, and properly converted from the legacy applications into the applications they support. In addition, the auditor should assess the effectiveness of application controls over the legacy applications, if the reliability of input is relevant to the audit objectives. Interface controls are discussed further at section 4.3.

2.5.1.E Data Management Systems

Operational characteristics of various system architectures that include data management systems such as Database Management Systems (DBMS) software introduce several potential vulnerabilities to the data/application the DBMS directly supports and the general controls environment, itself. The degree to which these potential vulnerabilities increase risk is determined by the characteristics of the networks and host system(s) involved. One area of risk exists when the DBMS architecture involves multiple installations of the DBMS, which may be located on more than one host system.

System and/or application architectures that utilize multiple DBMS installations are commonly used to support functionally or geographically distributed operations, high performance requirements, high availability requirements or some combination of these factors. When multiple DBMSs exist, the mechanisms that allow them to communicate with each other need to be implemented and controlled to prevent unintended data and/or system access. Additionally, modern DBMS software contains powerful capabilities to access the host's operating system and other operating systems and other DBMSs across networks. The ability to use these capabilities needs to be carefully controlled for each DBMS installation. Finally, some administrator accounts in DBMS software provide privileged levels of access to the host's operating system. So, users with system administration privileges in DBMS software may also have significant privileges in host operating systems and those systems and network devices accessible from the DBMS's host. Data management systems are discussed further at section 4.4.

2.5.1.F Network-based Access Control Systems

Implementations of network-based access control systems (such as LDAPs, including the Microsoft Active Directory™) introduce the potential for specific vulnerabilities. Network-based access control systems are typically hosted on one or more server-class systems. The appropriate configuration of the operating systems and all factors that can effect the functioning of the operating systems for these hosts needs to be carefully controlled. A flaw in operating system-level controls on these hosts potentially jeopardizes the reliability of the control functions provided by the network-based access control system and/or the sensitive access control data contained in that system. Network-based access control systems are designed to support high performance and simplify network administration and maintenance. To facilitate these design considerations, the systems provide flexible methods to connect to and transfer information with other systems. Due to these characteristics, it is essential that effective controls be in place to prevent unintended system functions or data access that could compromise access controls. The nature of networks and

application architectures that employ network-based access control systems involves a shared or common reliance on them for critical controls. Therefore, a compromise of a network-based access control system has the potential of contributing to the compromise of other systems.

2.5.1.G Workstations

In modern systems best described as networks of networks, the effect of workstation controls can be much more significant than control over the functions nominally identified as associated with a specific workstation. Workstations can become critical components of a network's perimeter as a result of the manner in which they are configured in the network, the types of sessions they can create with other devices, the access privileges allowed to workstation users, software running on those workstations, and controls over both inbound and outbound network traffic to and from the workstation. An understanding of the configuration of controls on workstations and network-based controls over workstations in the context of network perimeter controls is necessary to assess risk for any network,

2.5.2 Automated Audit Tools

Various automated audit tools can be used to improve the effectiveness and efficiency of the IS controls audit. Sometimes referred to as CAATs, or computer-assisted audit techniques, such tools may be used by the auditor to gather, or assist in gathering, audit evidence. If the auditor plans to use automated audit tools, the auditor should understand

- when they could be used,
- how they can be used, and
- the associated risks.

In addition, the auditor should be adequately trained in the use/operation of these tools and in the interpretation of the results. Because some tools generate a significant volume of information, the auditor should understand how to analyze such information.

Also, the auditor should obtain reasonable assurance that the tools and their use/application produce reliable results and present a reasonably low risk of disrupting the entity's systems. Organizations should develop a process to select, evaluate, and revise software security tools. The following are some typical steps:

- Research available security tools, listing several in each category.
- Discuss with other members of your audit organization which tools could be most useful in-house and at sites to be audited. Discuss with other audit organizations as appropriate.
- Determine the degree of platform-specific security software needed.
- Determine a methodology to evaluate and select software.
- Develop a procedure to train personnel in its use.
- Develop a review process to determine whether the software tool has produced results commensurate with its cost.

There are many different types of automated audit tools:

- Commercial software, such as Microsoft Excel™, etc., may be used by the auditor for analyzing data imported from client files, writing audit programs, etc.
- Generalized audit software may be used by the auditor to query and extract information from the entity's information system. For example, data extraction tools and reporting facilities for access control software can identify users with excess privileges that circumvent segregation of duties. IDEA is the generalized software package available to GAO auditors.
- An embedded audit module is a CAAT in which code prepared by the auditor is embedded in the client's software to replicate a specific aspect of a control procedure, or to record details of certain transactions in a file accessible only to the auditor.
- An integrated test facility is testing software that is integrated into the client's software and enables the auditor's test data to be integrated and processed with the client's live input. Using an integrated test facility allows the auditor to be satisfied that test data are processed in the same way that live data are processed and to verify that the results are correct. Parallel simulation is a technique in which actual client data are processed by a copy of

the client's software that is under separate control of the auditor and has undergone program code analysis to ensure that the processing is identical to that of the client's operational software.

- Program code analysis is the analysis of the client's program code to ensure that the instructions given to the computer are the same instructions that the auditor has previously identified when reviewing the systems documentation. Control over program code, including review, testing and implementation into production is often supported by special purpose software. Auditors may evaluate the effectiveness of the controls implemented through the use of automated configuration management tools. Additionally, auditors may utilize a client's tools to independently verify that version control is effective.
- A test data CAAT is a technique in which test data prepared by the auditor are processed on the current production version of the client's software, but separately from the client's normal input data. Using the current production software provides evidence that the transactions were processed in the manner expected.
- Specialized audit software is software designed to perform specific tasks in specific circumstances, such as comparison of source and object code, the analysis of unexecuted code, and the generation of test data.
- Other specialized tools can be used to test IS controls. For example:
  - Password crackers can identify the use of vendor-default or easily guessed passwords.
  - Network "sniffers" (software that can intercept and log traffic passing over a network) can identify the transmission of passwords or sensitive information in clear text.
  - Network scanners, along with standard operating system commands, can help identify an organization's network security profile and determine whether dangerous services are active in components.
  - Modem locators ("war dialing" software) can help identify unsecured dial-in modems.
  - "War driving" software used to detect unauthorized wireless access points.

CAATs can also be used in testing the effectiveness of controls, as a companion to other controls testing. This would typically involve making a small selection of transactions and walking them through the system, or developing an integrated test facility and processing test transactions through the system. The advantage of using CAATs in controls testing is that it is possible to test every transaction (either in a master file or transaction file), to determine whether there were any control failures.

Any analysis performed using CAATS should be adequately documented. In addition, a technical review should be performed by audit staff independent of the preparer to determine that the implementation of CAATS and the analysis of results is complete and accurate and that any conclusions are supported by the analysis.

2.5.3 Use of Sampling Techniques

Suggested audit procedures may include a selection of specific items (e.g., access forms). In addition, the auditor may need to determine, among multiple instances of a type of network component, which specific components to test. For example, the entity may have many internet access points or multiple instances of a data base. The auditor should exercise judgment in determining the number of items to select and the method used to select them. Generally, such judgment would include consideration of the related IS risk, the significance or criticality of the specific items in achieving the related control objectives, the location of the network component in relation to the key areas of audit interest, and the extent of consistency in the configuration of the components.

Controls that leave documented evidence of their existence and application (such as logs) may be tested by inspecting such evidence. If sufficient evidence cannot be obtained through walkthroughs in combination with observation, inquiry, and other non-sampling tests, the auditor generally should obtain more evidence by using sampling procedures to select individual items for inspection. The auditor may use multipurpose testing to use the same sample to test controls, compliance, and/or substantive results

(such as balances in financial statements). Multipurpose testing is usually more efficient than separately designed samples. Alternatively, the auditor may design a sample to test controls alone. In this case, the auditor generally should use random attribute sampling. FAM section 450 (Sampling Control Tests) provides additional information on the use of this sampling technique, including those that can be applied to performance audits.

Chapter 3. Evaluating and Testing General Controls

3.0 Introduction

General controls are the policies and procedures that apply to all or a large segment of an entity's information systems and help ensure their proper operation. Examples of primary objectives for general controls are to safeguard data, protect application programs, and ensure continued computer operations in case of unexpected interruptions. General controls are applied at the entitywide, system, and business process application levels. The effectiveness of general controls at the entitywide and system levels is a significant factor in determining the effectiveness of business process controls at the application level. Without effective general controls at the entitywide and system levels, business process controls generally can be rendered ineffective by circumvention or modification. For example, edits[53] designed to preclude users from entering unreasonably large dollar amounts in a payment processing system can be an effective application control. However, this control cannot be relied on if the general controls permit unauthorized program modifications that might allow some payments to be exempt from the edit. Consequently, the auditor may decide that it is efficient to evaluate the effectiveness of general controls separately from and before evaluating business process controls.

In planning the evaluation of IS controls, the auditor identifies areas of audit interest and critical control points. In identifying these areas, the auditor considers business process applications that are relevant to the audit objectives. Also, the auditor considers the network components that are most significant to the effectiveness of IS controls over the areas of audit interest. In planning the

[53]Editing in this context is inspecting a data field or element to verify the accuracy of its content.

evaluation of general controls, the auditor considers the most effective and efficient manner to gather evidence to determine the effectiveness of general controls over these critical control points. For example, if a business process application for benefit payments is a key area of audit interest, the auditor's testing of general controls is designed, to the extent possible, to focus on those general controls that most directly affect the application.

The evaluation of general controls includes the following five general control categories:

- security management, which provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls;
- access controls, which limit or detect access to computer resources (data, programs, equipment, and facilities), thereby protecting them against unauthorized modification, loss, and disclosure;
- configuration management, which prevents unauthorized changes to information system resources (for example, software programs and hardware configurations) and provides reasonable assurance that systems are configured and operating securely and as intended;
- segregation of duties, which includes policies, procedures, and an organizational structure to manage who can control key aspects of computer-related operations; and
- contingency planning, so that when unexpected events occur, critical operations continue without disruption or are promptly resumed, and critical and sensitive data are protected.

For each of these five general control categories, this manual identifies several critical elements that are essential for establishing adequate controls over the related control category. For each critical element, the FISCAM provides a description of risks, control activities, and suggested audit procedures. The auditor can use this information to evaluate entity practices. For each critical element, the auditor should make a summary determination as to the effectiveness of the entity's related controls at the entitywide,

system, and application levels. If a critical element is not achieved, the respective control category is not likely to be achieved. The auditor should use professional judgment in making such determinations.

To evaluate the effectiveness of general controls, the auditor identifies control techniques implemented by the entity to achieve each of the control activities for general controls and determine whether these control techniques, as designed, are sufficient to achieve the control activities. If sufficient, the auditor determines whether they are implemented (placed in operation) and operating effectively. As discussed later in this section, if the control techniques are not sufficient or are not implemented as designed, the auditor should determine the effect on IS controls and the audit objectives.

As discussed in more detail in Chapter 2, general controls are applicable at the entitywide, system, and application levels, and so the auditor should consider general controls at each of these levels. The control techniques and the related audit tests vary according to the level to which they are being applied. However, in this manual they are described at a high level in order to be applicable to many computer environments; they may require some technical expertise about the subject to be effectively performed at an entity. More detailed audit steps generally should be developed by the auditor based on the specific software and control techniques employed by the entity. Table 2 shows the relationship between the general control areas and the levels.

Table 2. General Control Categories Applicable at Different Levels of Audit

	Control Categories	Entitywide/ Component Level	System Level			Business Process Application Level
			Network	Operating Systems	Infrastructure Applications	
General Controls	Security Management	→				
	Access Controls	→				
	Configuration Management	→				
	Segregation of Duties	→				
	Contingency Planning	→				

Source: GAO.

The auditor's evaluation of the effectiveness of IS controls should include system level controls related to each critical control point. Assessing the effectiveness of controls over critical control points should include consideration of all potential ways in which the critical control point could be accessed. Generally, for each critical control point, this would include assessing controls related to the network, operating system, and infrastructure application components. For example, if a particular router was deemed to be a critical control point, the auditor would test controls related to the router itself (a network component), as well as its operating system, and the infrastructure applications used to manage the router. Access to any of these could lead to access to the control point.

To facilitate the auditor's evaluation, tables identifying commonly used control techniques and related audit procedures are included after the discussion of each critical element and also in Appendix II.

These tables can be used for both the preliminary evaluation and the more detailed evaluation and testing of controls. For the preliminary evaluation, the auditor can use the tables to guide and document initial inquiries and observations; for the more detailed evaluation and testing, the auditor can use the suggested procedures in developing and carrying out a testing plan. Such a plan would include more extensive inquiries; inspections of facilities, systems, and written procedures; and tests of key control techniques, which may include using audit or system software and vulnerability analysis tools. To help document these evaluations and allow steps to be tailored to individual audits, electronic versions of the tables are available on our FISCAM website at http://www.gao.gov/special.pubs/fiscam.html.

When evaluating general controls, auditors may want to supplement the control techniques and audit procedures contained in this document with other guidance, including

- National Institute of Standards and Technology (NIST) information security standards and guidelines;
- Applicable OMB policy and guidance;
- international security standards published by the International Organization for Standardization and the International Electrotechnical Commission;
- Information Systems Audit and Control Association (ISACA) auditing standards, guidelines, and procedures; and
- requirements unique to the environment and entity being audited.

3.1. Security Management (SM)

An entitywide information security management program is the foundation of a security control structure and a reflection of senior management's commitment to addressing security risks. The security management program should establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Overall policies and plans are developed at the entitywide level. System and application-specific

procedures and controls implement the entitywide policy. Without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, or improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources. Through FISMA, Congress requires each federal agency to establish an agencywide information security program to provide security to the information and information systems that support the operations and assets of the agency, including those managed by a contractor or other agency.

Security Program Guidance

General guidance on planning and managing an information security program is contained in (1) NIST SP 800-12,[54] which provides guidance on security-related management, operational, and technical controls and (2) our executive guide describing risk management principles found at leading organizations (discussed in the next section).[55] NIST has published a series of information security standards and guidelines for agencies to effectively manage risk to entity operations and entity assets. Key publications are:

- FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*
- FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*
- NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*[56].

[54]NIST, *An Introduction to Computer Security: The NIST Handbook*, Special Publication (SP) 800-12, October 1995.

[55]GAO, *Executive Guide: Information security Management, Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

[56]NIST has stated that it plans to update SP 800-53 annually.

FIPS Publication 200 provides

1. a specification for minimum security requirements for federal information and information systems;

2. a standardized approach to security control selection using the security categorization standard, FIPS Publication 199; and

3. links to NIST SP 800-53, containing the security controls needed for compliance with these minimum security requirements.

In applying the provisions of FIPS 200, agencies first categorize their systems as required by FIPS 199 (see Table 5), and then typically select an appropriate set of security controls from NIST SP 800-53 to satisfy their minimum security requirements. NIST reviews and updates the controls in NIST SP 800-53 annually to ensure that the controls represent the current state of practice in safeguards and countermeasures for information systems.

FIPS 200 and its supporting publication NIST SP 800-53 establish conditions to enable organizations to be flexible in tailoring their security control baselines. Agencies, may, for example, apply scoping guidance taking into consideration the issues related to such things as the technologies employed by the entity, size and complexity of the systems, unique circumstances, and risks involved. Agencies may use compensating controls in lieu of those controls prescribed by NIST SP 800-53. Agencies may also supplement the controls in NIST SP 800-53 with additional controls that may be needed.

In addition, NIST SP 800-100 provides a broad overview of information security program elements, including capital planning and investment control, performance measures, and security services, to assist managers in understanding how to establish and implement an information security program. This handbook summarizes and augments a number of existing NIST standards and guidance documents and provides additional information on related topics.

Other guidance supporting implementation of FIPS 199 and FIPS 200 include:

- NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*
- NIST SP 800-30, *Risk Management Guide for Information Technology Systems*
- NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*
- NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*

These and other publications, directives, and policies that support are available from NIST's website (http://csrc.nist.gov).

Security Management Critical Elements

Assessing an entitywide security management program involves evaluating the entity's efforts to perform each of the critical elements shown in table 3.

Table 3. Critical Elements for Security Management

Number	Description
SM-1	Establish a security management program
SM-2	Periodically assess and validate risks
SM-3	Document and implement security control policies and procedures
SM-4	Implement effective security awareness and other security-related personnel policies
SM-5	Monitor the effectiveness of the security program
SM-6	Effectively remediate information security weaknesses
SM-7	Ensure that activities performed by external third parties are adequately secure

Source: GAO.

The following sections discuss each of these critical elements and the control activities that support their achievement. At the end of each critical element, a summary table is presented that associates each control activity with techniques that agencies can use to perform the activity, as well as procedures for auditing the critical elements and control activities.

Critical Element SM-1: Establish a Security Management Program

Entities should have policies, plans, and procedures that clearly describe the entity's security management program. FISMA requires federal agencies to develop, document, and implement an agencywide information security program to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. The security management program should cover all major systems and facilities and outline the duties of those who are responsible for overseeing security and those who own, use, or rely on the entity's computer resources. As part of this entitywide program, the entity should have a security management structure in place at the system and application levels. Thus, in managing a particular operating system or network device, the entity should have a clearly assigned structure and responsibilities for the security of the operating system and device. Similarly, the entity should have a clearly assigned structure and responsibilities related to particular business process applications. The security program policies, plans, and procedures should be kept up-to-date and revised to reflect system and organizational changes, problems identified during plan implementation, and security control assessments or audit reports.

SM-1.1. The security management program is adequately documented, approved, and up-to-date

The entity's security management program should be adequately documented. The nature and extent of the documentation of the program may vary. For federal entities, at a minimum, the program should adequately reflect the agency's consideration of the following eight elements of an agencywide information security program required by FISMA.

1. periodic risk assessments;

2. policies and procedures to ensure cost-effective risk reduction and compliance with applicable standards and guidance and with agency-determined system configuration requirements;

3. subordinate information security plans for networks, facilities, and systems;

4. security awareness training for agency employees and contractors;

5. periodic management testing and evaluation that includes testing of all major systems;

6. a remedial action process to address any deficiencies;

7. security-incident procedures for detecting, reporting, and responding to incidents; and

8. continuity of operations plans and procedures for information systems.

While most of these elements are covered in this section, security incident procedures are covered in section 3.2 on access controls, and continuity of operations is covered in section 3.5 on contingency planning.

The security management program may be documented in the form of a separate written security management program plan or may consist of several documents that collectively constitute the security management program. The documentation should be supported by subordinate (system and application level) plans and procedures; related policies should cover all major systems and facilities and outline the duties of those responsible for overseeing security (the security management function), as well as those who own, use, or rely on the entity's computer resources. An entitywide plan may describe such things as the overall security architecture, applicable procedures, and applicable system and application-level plans. The system-level plans identify the system-level architecture (for example, network configuration, control points, etc.), operational policies and procedures, and any business process (application-level) plans. Similarly, application-level plans should contain structures, procedures, and controls specific to the application.

The security management program should be approved by an appropriate level of management. In some instances, the entity may include the documentation in a policy document issued by management. In addition, for federal agencies, FISMA requires that

the Director of OMB review federal agency security management programs at least annually and approve or disapprove them.

Finally, to be effective, the security program documentation should be maintained to reflect current conditions. It should be periodically reviewed and, if appropriate, updated and reissued to reflect changes in risk due to factors such as changes in entity mission or the types and configuration of computer resources in use. Revisions to policies and plans should be reviewed, approved, and communicated to all employees. Outdated policies and plans not only reflect a lack of adequate top management concern, but also may be ineffective because they may not address current risks.

SM-1.2. A security management structure has been established

Senior management should establish a structure to implement the security management program throughout the entity. The structure generally consists of a core of personnel who are designated as security managers. These personnel play a key role in developing, communicating, and monitoring compliance with security polices and reporting on these activities to senior management. The security management function also serves as a focal point for other personnel who play a role in evaluating the appropriateness and effectiveness of computer-related controls on a day-to-day basis. These personnel include program managers who rely on the entity's computer systems, system administrators, and system users.

As an illustration of the different responsibilities of a security management structure, FISMA establishes responsibilities for certain agency officials as follows:

- The agency head is responsible for (1) providing risk-based information security, (2) complying with FISMA requirements and related NIST standards, (3) ensuring integration of information security management with agency strategic and operational planning, (4) ensuring adequacy of trained information security personnel, and (5) ensuring receipt of annual reporting from the CIO.
- The CIO is to have authority from the agency head to ensure compliance with FISMA, including responsibility for

(1) designating a senior agency information security official, (2) developing and maintaining the agency information security program and related policies and procedures, (3) training and overseeing information security personnel, and (4) assisting senior agency officials with their information security responsibilities.

- Senior agency officials are responsible for information security for operations and assets under their control, including (1) assessing risk, (2) determining levels of appropriate security, (3) implementing policies and procedures to cost-effectively reduce risks to an acceptable level, and (4) periodically testing and evaluating security controls.

Our survey of leading organizations[57] found that a central management focal point is key to ensuring that the various activities associated with managing risk are carried out. Such responsibility is assigned to a central security program office. A central security program office may be supplemented by individual security program managers, designated in units within the entity who assist in the implementation and management of the organization's security program. These individual unit security managers should report to or coordinate with the central security program office.

Responsibilities of the central security program office may include

- facilitating risk assessments,
- coordinating development and distribution of security policies and procedures,
- routinely monitoring compliance with these policies,
- promoting security awareness among system users,
- planning and coordinating security-related activities, including coordination of geographically dispersed security groups,
- ensuring that desktop security plans are integrated with infrastructure and database security plans,

[57] *Executive Guide: Information Security Management, Learning from Leading Organizations* (GAO/AIMD-98-68, May 1998).

- providing reports to senior management on policy and control evaluation results and advice to senior management on security policy issues, and
- representing the entity in the security community.

In assessing the effectiveness of the security management structure for an entitywide, system, or application level, the auditor considers the security function's scope of authority, placement, training and experience, and tools. For example, security management personnel should

- have sufficient authority to obtain data needed to monitor compliance with policies, report results to senior management, and elevate concerns regarding inappropriate risk management decisions or practices;
- have sufficient resources to carry out their responsibilities, including staff and tools (for example, computers, established audit trails, and specialized security software);
- report to a level of management that maximizes the independence and objectivity of the security function;
- not be assigned responsibilities that diminish their objectivity and independence; and
- have sufficient training and knowledge of control concepts, computer hardware, software, telecommunications concepts, physical and logical security, data architecture, database management and data access methods, pertinent legislation, and administration and organizational issues.

SM-1.3. Information security responsibilities are clearly assigned

Security-related responsibilities of offices and individuals throughout the entity that should be clearly defined include those of (1) information resource owners and users, (2) information resources management and data processing personnel, (3) senior management, and (4) security administrators. Further, responsibilities for individual employee accountability regarding the use and disclosure of information resources should be established. Appendix III of OMB Circular A-130 requires that the rules of the system and application "shall clearly delineate responsibilities and

expected behavior of all individuals with access … and shall be clear about the consequences of behavior not consistent with the rules."

Senior management and information resource management have ultimate responsibility for providing direction and ensuring that information security responsibilities are clearly assigned and carried out as intended. Security plans should clearly establish who "owns" the various computer resources, particularly data files, and what the responsibilities of ownership are. Ownership of computer resources should be assigned to persons responsible for their reliability and integrity. For example, owners of data files and application programs are generally the managers of the programs supported by these applications. These managers are primarily responsible for the proper operation of the program and for accurate reporting of related computer data. Similarly, owners of computer facilities and equipment are generally managers who are responsible for the physical protection of these resources. If a resource has multiple owners, policies should clearly describe whether and how ownership responsibilities are to be shared.

Assignment of ownership responsibilities is important because the managers who own the resources are in the best position to (1) determine the sensitivity of the resources, (2) analyze the duties and responsibilities of users, and (3) determine the specific access needs of these users. Once these factors are determined, the resource owner can identify persons authorized to access the resource and the extent of such access. The owners should communicate these authorizations to the security administrators, who are then responsible for implementing access controls in accordance with the owners' authorizations. Section 3.2, Access Controls, further discusses access authorization.

If management and ownership responsibilities are not clearly assigned, access authorizations may be left to personnel who are not in the best position to determine users' access needs. Such personnel are likely to authorize overly broad access in an attempt to ensure that all users can access the resources they need. This defeats the purpose of access controls and, depending on the

sensitivity of the resources involved, can unnecessarily provide opportunities for fraud, sabotage, and inappropriate disclosures.

SM-1.4. Subordinate security plans are documented, approved, and kept up-to-date

Entities should have written security plans at the system and application levels that cover networks, facilities, and systems or groups of systems, as appropriate. The plans and related policies should cover all major systems and facilities and outline the duties of those who are responsible for overseeing security and those who own, use, or rely on the entity's computer resources. In addition, these system-level plans should provide an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. These plans should be kept up-to-date and revised to reflect system and organizational changes, problems identified during plan implementation, and security control assessments or audit reports. NIST SP 800-18 requires that all security plans should be reviewed and updated, if appropriate, at least annually. Further, NIST SP 800-18 and Appendix III of OMB Circular A-130 provide specific guidance on what should be included in federal entity system security plans.

FISMA states that "each agency shall develop, document, and implement…subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate." System-level plans should identify the system-level architecture (for example, network configuration, control points, etc.), operational policies and procedures, and any application-level plans. Application plans should contain similar elements such as procedures and controls specific to the application.

System security plans should be clearly documented and, according to Appendix III of OMB Circular A-130, cover each general support system and each major application. The circular further specifies the topics to include in the plans. Topic names will differ depending on whether the plan is for a general support system or a major application, but the subject matter will be similar. The required topics are shown in table 4.

Table 4. Security Controls to Include in System Security Plans

General support system	Major application
rules of the system [a]	application rules [a]
training	specialized training
personnel controls	personnel security
incident-response capability	NA
continuity of support	contingency planning
technical security	technical controls
system interconnection	information sharing
NA	public access controls

Source: Appendix III of OMB Circular A-130.

[a] These include rules delineating responsibilities and expected behaviors of staff.
Note: In this manual, access controls are addressed in section 3.2 and contingency planning in section 3.5.

To help ensure that the system security plan is complete and supported by the entity as a whole, senior management should obtain agreement from all affected parties to establish policies for a security program. Such agreements will also help ensure that policies and procedures for security developed at lower levels within the agency are consistent with overall organizational policies and procedures. In accordance with Appendix III of OMB Circular A-130, final responsibility for authorization of a system to process information should be granted by a management official. Generally, the manager whose program operations and assets are at risk is the most appropriate management official. However, any disagreements between program managers and security specialists as to the adequacy of policies and controls should be resolved by senior management.

Like the overall security policies and plans, the subordinate security policies and plans should be maintained to reflect current conditions. As described in SM-1.1, they should be periodically reviewed and updated to reflect changes in risk and revisions should be reviewed, approved, and communicated to employees. Outdated policies and plans may be ineffective because they may not address current risks.

SM-1.5. An inventory of systems is developed, documented, and kept up-to-date

To implement an effective security program, entities need to maintain a complete, accurate, and up-to-date inventory of their

systems. Without one, the entity cannot effectively manage IS controls across the entity. For example, effective configuration management requires the entity to know what systems they have and whether the systems are configured as intended. Furthermore, the inventory is necessary for effective monitoring, testing, and evaluation of IS controls, and to support information technology planning, budgeting, acquisition, and management.

FISMA requires that each agency develop, maintain, and annually update an inventory of major information systems operated by the agency or under its control. OMB Circular A-130 defines a major information system as a system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources. The inventory must include identification of the interfaces between the agency systems and all other systems or networks, including interfaces not controlled by the agency. The inventory is needed to effectively track the agency systems for annual testing and evaluation and contingency planning.

Control Techniques and Suggested Audit Procedures for Critical Element SM-1

Table 5 presents control activities for critical element SM-1, techniques that entities may use to perform the activity and procedures for auditing the critical element and control activities.

SM-1 Related NIST SP 800-53 Controls
See the first control for each family (e.g., AC-1, AT-1)
PL-2 System Security Plan
PL-3 System Security Plan Update
PL-6 Security-Related Activity Planning
SA-2 Allocation of Resources

Table 5. Control Techniques and Suggested Audit Procedures for Critical Element SM-1: Establish a security management program

Control activities	Control techniques	Audit procedures

SM-1.1. The security management program is adequately documented, approved, and up-to-date.	SM-1.1.1. An agency/entitywide security management program has been developed, documented, and implemented that
	• covers all major facilities and operations,
	• has been approved by senior management and key affected parties, and
	• covers the key elements of a security management program:
	  • periodic risk assessments,
	  • adequate policies and procedures,
	  • appropriate subordinate information security plans,
	  • security awareness training,
	  • management testing and evaluation,
	  • a remedial action process,
	  • security-incident procedures, and
	  • continuity of operations.
		Review documentation supporting the agency/entitywide security management program and discuss with key information security management and staff.
		
		Determine whether the program
		• adequately covers the key elements of a security management program
		• is adequately documented, and
		• is properly approved.
		
		Determine whether all key elements of the program are implemented. Consider audit evidence obtained during the course of the audit.

	SM-1.1.2. The agency/entitywide security management program is updated to reflect current conditions.	Based on a review of security management program documentation and interviews with key information security management and staff, determine whether the entity has adequate policies and procedures to identify significant changes in its IT environment that would necessitate an update to the program, and whether the program is periodically updated to reflect any changes.
SM-1.2. A security management structure has been established.	SM-1.2.1. Senior management establishes a security management structure for entitywide, system, and application levels that have adequate independence, authority, expertise, and resources.	Review security policies and plans, the entity's organization chart, and budget documentation. Interview security management staff. Evaluate the security structure: independence, authority, expertise, and allocation of resources required to adequately protect the information systems.
	SM-1.2.2. An information systems security manager has been appointed at an agency/entity level and at appropriate subordinate (i.e., system and application) levels and given appropriate authority.	Review pertinent organization charts and job descriptions. Interview the overall security manager and subordinate security managers responsible for specific systems and applications.
SM-1.3. Information security responsibilities are clearly assigned.	SM-1.3.1. The security program documentation clearly identifies owners of computer-related resources and those responsible for managing access to computer resources. Security responsibilities and expected behaviors are clearly defined at the entitywide, system, and application levels for (1) information resource owners and users, (2) information technology management and staff, (3) senior management, and (4) security administrators.	Review security program documentation detailing security responsibilities and rules of behavior for security officials, resource owners, and users at the entitywide, system, and application levels.

Control activities	Control techniques	Audit procedures
SM-1.4. Subordinate security plans are documented, approved, and kept up-to-date.	SM-1.4.1. System and application security plans have been documented and implemented that • cover all major facilities and operations, • have been approved by key affected parties, • cover appropriate topics (for federal agencies, those prescribed by OMB Circular A-130; see table 4).	Review agency/entity policies and procedures for preparing security plans. Review the system and application security plans encompassing key areas of audit interest and critical control points. Determine whether the plans adequately cover appropriate topics (for federal agencies, refer to NIST SP 800-18 for guidance on security plans) and are properly approved. When conducting the audit, determine whether the plans have been implemented and accurately reflect the conditions noted. Determine whether security plans collectively cover all major facilities and operations.
	SM-1.4.2. The subordinate security plans are updated annually or whenever there are significant changes to the agency/entity policies, organization, IT systems, facilities, applications, weaknesses identified, or other conditions that may affect security.	Review relevant security plans and any related documentation indicating whether they have been reviewed and updated and are current.
SM-1.5. An inventory of systems is developed, documented, and kept up-to-date.	SM-1.5.1. A complete, accurate, and up-to-date inventory exists for all major systems that includes the identification of all system interfaces.	Obtain the agency's/entity's systems inventory. Discuss with agency/entity management (1) the methodology and criteria for including or excluding systems from the inventory and (2) procedures and controls for ensuring the completeness, accuracy, and currency of the inventory. Determine whether systems tested during the audit are included in the inventory. Test the inventory for completeness, accuracy, and currency. The objective of this step in an IS controls audit being performed as part of a financial audit or data reliability assessment is generally limited to understanding management's process and controls for ensuring the accuracy of the inventory. Also, in the absence of effective controls over the inventory, the auditor would need to perform additional procedures to reasonably assure that all systems relevant to the audit have been identified.

Source: GAO.

Critical Element SM-2. Periodically assess and validate risks

A comprehensive risk assessment should be the starting point for developing or modifying an entity's security policies and security plans. Such assessments are important because they help make certain that all threats and vulnerabilities are identified and considered, that the greatest risks are addressed, and that appropriate decisions are made regarding which risks to accept and which to mitigate through security controls. Appropriate risk assessment policies and procedures should be documented and based on the security categorizations.

FISMA explicitly emphasizes a risk-based policy for cost-effective security. In support of and reinforcing this legislation, OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, requires executive agencies within the federal government to plan for security; ensure that appropriate officials are assigned security responsibility; review the security controls in their information systems; and authorize system processing prior to operations and periodically thereafter.

Risk assessments should consider threats and vulnerabilities at the entitywide level, system level, and application levels. For example, at the entitywide level, risk assessments should consider personnel policies and procedures, training, and security awareness activities. At the system level, risks related to connectivity issues (for example, Internet, dial-up, wireless) and access controls (for example, both logical and physical) need to be assessed. At the application level, risk assessments need to consider specific business processes and highly-integrated enterprise resource planning (ERP) applications (discussed in Chapter 4).

Risk assessments should consider risks to data confidentiality, integrity, and availability, and the range of risks that an entity's systems and data may be subject to, including those posed by authorized internal and external users, as well as unauthorized outsiders who may try to break into the systems. For example, risk assessments should take into account observed trends in the types and frequency of hacker activity and threats. Such analyses should also draw on reviews of system and network configurations, as well as observations and testing of existing security controls.

Our study of security programs at leading organizations found that the following were key success factors for risk assessments.

- Organizations had a defined process that allowed an entitywide understanding of what a risk assessment was and avoided individual units developing independent definitions.
- Organizations required that risk assessments be performed and designated a central security group to schedule and facilitate them.
- Risk assessments involved a mix of individuals who have knowledge of business operations and technical aspects of the organization's systems and security controls.
- The business managers were required to provide a final sign-off indicating agreement with risk-reduction decisions and acceptance of the residual risk.
- Organizations required that final documentation be forwarded to more senior officials and to internal auditors so that participants could be held accountable for their decisions.
- Leading organizations did not attempt to precisely quantify risk. Although they would have liked to place a dollar value on risks and precisely quantify the costs and benefits of controls, they felt that spending time on such an exercise was not worth the trouble. They believed that few reliable data were available on either the actual frequency of security incidents or on the full costs of controls and of damage due to a lack of controls.

Risk assessments are more likely to be effective when performed by personnel with enough independence to be objective and with enough expertise (training and experience) to be able to adequately identify and assess technical and security risks.

Risk assessment and risk management are ongoing efforts. Although a formal, comprehensive risk assessment is performed periodically, such as part of a system security plan, risk should be considered whenever there is a change in an entity's operations or its use of technology or in outside influences affecting its operations. Changes to systems, facilities, or other conditions and identified security vulnerabilities should be analyzed to determine their impact on risk, and the risk assessment should be performed or revised as

necessary. The risk assessment and validation and related management approvals should be documented and maintained on file. Such documentation should include risk assessments, security test and evaluation results, security plans, and appropriate management approvals. Further, according to NIST SP 800-37, systems should be certified and accredited before being placed in operation and when major system changes occur.

The NIST SP 800-30 risk management guide discusses the development of an effective risk management program and contains both the definitions and the practical steps necessary for assessing and mitigating risks within IT systems, including related testing. According to this guide, the principal goal of an entity's risk management process should be to protect the entity and its ability to perform its mission, not only its information technology assets.

According to FISMA, federal agencies must periodically assess the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support their operations and assets. Policies and procedures are based on risk, and the rigor of management testing and evaluation of information security should also be based on risk. Also, OMB Circular A-123 states that management is responsible for developing and maintaining internal control activities that comply with certain standards, including risk assessment. The Circular further states that, under risk assessment, management should identify internal and external risks that may prevent the organization from meeting its objectives. Identified risks should then be analyzed for their potential effect or impact on the agency.

Further, Appendix III of OMB Circular A-130 requires that agencies consider risk when determining the need for and selecting computer-related control techniques. However, the Circular no longer requires formal periodic risk analyses that attempt to quantify in dollars an annual loss exposure resulting from unfavorable events.

Pursuant to FISMA, NIST developed standards for security categorization of federal information and information systems

according to a range of potential impacts (FIPS Pub 199). Table 6 summarizes these NIST standards using potential impact definitions for each security objective (confidentiality, integrity, and availability). Federal agencies should categorize/classify their non-national security systems according to these impact levels. The security categories are based on the potential impact on an entity should certain events occur that jeopardize the information and information systems needed by the entity to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. NIST also issued a guide for mapping types of information and information systems to security categories (NIST SP 800-60). Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an agency.

Table 6. NIST Impact Definitions for Security Objectives

	Potential impact		
Security objective	**Low**	**Moderate**	**High**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. {44 U.S.C., Sec 3542}	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Security objective	Potential impact		
	Low	**Moderate**	**High**
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. {44 U.S.C., Sec 3542}	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. {44 U.S.C. 3542}	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Source: National Institute of Standards and Technology (NIST), FIPS Publication 199, page 6.

One area that merits additional emphasis is the appropriate consideration of risks associated with sensitive privacy information. In addition to an appropriate consideration of related risk, specific controls are discussed at SM-5 and AC-4.2.

In addition to FISMA, federal agencies are subject to privacy laws aimed at preventing the misuse of personally identifiable

information.[58] The Privacy Act of 1974 and the privacy provisions of the E-Government Act of 2002 contain the major requirements for the protection of personal privacy by federal agencies. The Privacy Act places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records[59] and requires that when agencies establish or make changes to a system of records; they must notify the public by a "system-of-records notice."[60] The E-Government Act of 2002 strives to enhance protection for personal information in government information systems or information collections by requiring that agencies conduct privacy impact assessments. These privacy impact assessments include an analysis of how personal information is collected, stored, shared, and managed in a federal system.

According to OMB guidance, these privacy impact assessments must analyze and describe how the information will be secured including administrative and technological controls and should be current.[61] OMB Memorandum M-03-22[62] directs agencies to conduct reviews of how information about individuals is handled within their agency when they use information technology to collect new

[58]Personally identifiable information refers to any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, or biometric records, and any other information which is linked or linkable to an individual.

[59]The act describes a "record" as any item, collection, or grouping of information about an individual that is maintained by an agency and contains his or her name or another personal identifier. It also identifies "system of records" as a group of records under the control of any agency retrieved by the name of the individual or by an individual identifier.

[60]A system of records notice is a notice in the Federal Register identifying, among other things, the type of data collected, the types of individuals about whom information is collected, the intended "routine" uses of data, and procedures that individuals can use to review and correct personal information.

[61]See OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*. Also, according to FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, OMB Memorandum M-06-20, July 17, 2006, a privacy impact assessment or a system of records notice is current if that document satisfies the applicable requirements and subsequent substantial changes have not been made to the system.

[62]OMB, *Guidance for implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22 (Washington, DC.: September 26, 2003).

information, or when agencies develop or buy new IT systems to handle collection of personally identifiable information.

As discussed in NIST SP 800-60[63], in establishing confidentiality impact levels for each information type, responsible parties must consider the consequences of unauthorized disclosure of privacy information (with respect to violations of Federal policy and/or law). The impact of privacy violations will depend in part on the penalties associated with violation of the relevant statutes and policies. Further, it says that, in most cases, the impact on confidentiality for privacy information will be in the ***moderate*** range.

SM-2 Related NIST SP 800-53 Controls
CA-4 Security Certification
CA-6 Security Accreditation
RA-2 Security Categorization
RA-3 Risk Assessment
RA-4 Risk Assessment Update

Control Techniques and Suggested Audit Procedures for Critical Element SM-2

Table 7 Control Techniques and Suggested Audit Procedures for Critical Element SM-2: Periodically assess and validate risks

Control activities	Control techniques	Audit procedures
SM-2.1. Risk assessments and supporting activities are systematically conducted.	SM-2.1.1. Appropriate risk assessment policies and procedures are documented and based on security categorizations.	Review risk assessment policies, procedures, and guidance.
	SM-2.1.2. Information systems are categorized based on the potential impact that the loss of confidentiality, integrity, or availability would have on operations, assets, or individuals.	Determine if security risk categorizations are documented, reasonable, and, for federal entities, if they comply with NIST FIPS Pub 199 and SP 800-60.

[63]NIST Special Publication (SP) 800-60, *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories* – Revision 1 (August 2008).

Control activities	Control techniques	Audit procedures
	SM-2.1.3. Risks are reassessed for the entitywide, system, and application levels on a periodic basis or whenever systems, applications, facilities, or other conditions change.	Obtain the most recent risk assessments encompassing key areas of audit interest and critical control points. Determine if the risk assessments are up-to-date, appropriately documented, approved by management, and supported by sufficient testing (e.g., determine whether system vulnerabilities were identified using such techniques as automated scanning tools, security test evaluations or penetration tests). See NIST SP 800-30 for details. The objective of this step in an IS controls audit being performed as part of a financial audit or data reliability assessment is generally limited to understanding management's risk assessment process (including related controls), reading the risk assessments for the key systems relevant to the audit objectives, and determining whether risks identified by the IS controls audit are properly considered in the risk assessments.
	SM-2.1.4. Risk assessments and validations, and related management approvals are documented and maintained on file. Such documentation includes security plans, risk assessments, security test and evaluation results, and appropriate management approvals.	For a selection of risk assessments assess the completeness and adequacy of the required documentation.
	SM-2.1.5. Changes to systems, facilities, or other conditions and identified security vulnerabilities are analyzed to determine their impact on risk and the risk assessment is performed or revised as necessary based on OMB criteria.	Review criteria used for revising risk assessments. For recent changes that meet the criteria, determine if the risk assessment was redone or updated.
	SM-2.1.6. Federal systems are certified and accredited before being placed in operation and at least every 3 years, or more frequently if major system changes occur.	For federal systems that are significant to the audit objectives, review certification and accreditation documentation and determine compliance with NIST SP 800-37. The objective of this step in an IS controls audit being performed as part of a financial audit or data reliability assessment is generally limited to understanding the certification and accreditation process (including related controls), reading the certifications and accreditations for the key systems relevant to the audit objectives, and determining whether the certification and accreditation documentation for the systems tested is consistent with the testing results.

Source: GAO.

Critical Element SM-3. Document and implement security control policies and procedures

Security control policies and procedures should be documented and approved by management. They should also appropriately consider risk, address general and application controls, and ensure that users can be held accountable for their actions. Control policies and procedures may be written to be more general at the entitywide level and more specific at the systems (for example, specific configurations) and application levels (for example, user access rules for specific applications). For example, access control policies may be implemented at the entitywide level through communication of formal written guidance; at the system level through system-level security software, firewall rules, and access control lists; and at the application level through very specific controls built into the application. Also, a formal sanctions process should be established for personnel who fail to comply with established IS control policies and procedures.

According to FISMA, each federal agency information security program must include policies and procedures that are based on risk assessments that cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each agency information system. NIST provides guidance pertaining to computer security policy and procedures, described here.

Security policy is senior management's directives to create a computer security program, establish its goals, and assign responsibilities. The term is also used to refer to the specific security rules for particular systems. Because policy is written at a broad level, agencies also develop standards, guidelines, and procedures that offer users, managers, and others a clear approach to implementing policy and meeting organizational goals. Standards and guidelines specify technologies and methodologies to be used to secure systems. Standards, guidelines, and procedures may be promulgated throughout an entity via handbooks, regulations, or manuals.

Procedures are detailed steps to be followed to accomplish particular security-related tasks (for example, preparing new user accounts and assigning the appropriate privileges). Procedures provide more detail in how to implement the security policies, standards, and guidelines. Manuals, regulations, handbooks, or similar documents may mix policy, guidelines, standards, and procedures, since they are closely linked. In order for manuals and regulations to serve as important tools, they should clearly distinguish between policy and its implementation. This can help in promoting flexibility and cost-effectiveness by offering alternative approaches to implementing policies.

SM-3 Related NIST SP 800-53 Controls
See the first control for each family (e.g., AC-1, AT-1)

Control Techniques and Suggested Audit Procedures for Critical Element SM-3

Table 8. Control Techniques and Suggested Audit Procedures for Critical Element SM-3: Document and implement security control policies and procedures

Control activities	Control techniques	Audit procedures
SM-3.1 Security control policies and procedures are documented, approved by management and implemented.	SM-3.1.1. Security control policies and procedures at all levels • are documented, • appropriately consider risk, • address purpose, scope, roles, responsibilities, and compliance, • ensure that users can be held accountable for their actions, • appropriately consider general and application controls, • are approved by management, and • are periodically reviewed and updated.	Review security policies and procedures and compare their content to NIST guidance (e.g., SP 800-30, SP 800-37, SP 800-100) and other applicable criteria (e.g., configuration standards).

Source: GAO.

Critical Element SM-4. Implement effective security awareness and other security-related personnel policies

Effective security-related personnel policies are critical to effective security. Ineffective personnel policies can result in employees or contractors inadvertently or intentionally compromising security.

For example, security may be compromised due to an inadequate awareness or understanding, inadequate security training, or inadequate screening of employees.

An ongoing security awareness program should be implemented that includes first-time training for all new employees, contractors, and users; periodic refresher training for all employees, contractors and users; and distribution of security policies detailing rules and expected behaviors to all affected personnel. Relevant security awareness requirements and guidance are contained in FISMA, OMB Circular A-130, and NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*. In addition, employees with significant security responsibilities should receive specialized training, as described in NIST SP 800-16, "*Information Technology Security Training Requirements: A Role- and Performance-Based Model*" (April 1998). Also, see 5 CFR 930.301.

According to FISMA, an agencywide information security program for a federal agency must include security awareness training for not only agency personnel but also contractors and other users of information systems that support the agency's operations and assets. This training must cover (1) information security risks associated with users' activities and (2) users' responsibilities in complying with agency policies and procedures designed to reduce these risks. FISMA also includes requirements for training of personnel with significant responsibilities for information security. Further, OMB requires personnel to be trained before they are granted access to systems or applications. The training is to make sure that personnel are aware of the system or application's rules, their responsibilities, and their expected behavior.

Other security-related personnel policies are also relevant to effective security. Policies related to personnel actions, such as hiring, termination, and employee expertise, are important considerations in securing information systems. If personnel policies are not adequate, an entity runs the risk of (1) hiring unqualified or untrustworthy individuals; (2) providing terminated employees opportunities to sabotage or otherwise impair entity operations or assets; (3) failing to detect continuing unauthorized

employee actions; (4) lowering employee morale, which may in turn diminish employee compliance with controls; and (5) allowing staff expertise to decline.

As mentioned, FISMA requires agencies to implement agencywide security programs that include effective policies and procedures to ensure cost-effective risk reduction and ensure compliance with FISMA and applicable OMB (e.g., OMB Circular A-130) and NIST (e.g., SP 800-30) guidance. This guidance specifically addresses security-related personnel policies and procedures. For example, NIST SP 800-53 addresses personnel security and controls related to personnel screening, termination and transfer, and third-party security.

SM-4.1 Ensure that resource owners, system administrators, and users are aware of security policies

For a security program to be effective, those expected to comply with it must be aware of it. Typical means for establishing and maintaining security awareness include

- informing users of the importance of the information they handle and the legal and business reasons for maintaining its integrity and confidentiality;
- distributing documentation describing security policies, procedures, and users' responsibilities, including their expected behavior;
- requiring users to periodically sign a statement acknowledging their awareness and acceptance of responsibility for security (including the consequences of security violations) and their responsibilities for following all organizational policies (including maintaining confidentiality of passwords and physical security over their assigned areas); and
- requiring comprehensive security orientation, training, and periodic refresher programs to communicate security guidelines to both new and existing employees and contractors.

Leading organizations studied considered promoting awareness to be one of the most important factors in the risk management process. Awareness was considered to be especially important in

reducing the risks of "social engineering," where users are talked into revealing passwords or other sensitive information to potential thieves. Educating users about such risks makes them think twice before revealing sensitive data and makes them more likely to notice and report suspicious activity.

Employee awareness is also critical in combating security threats posed by spam, spyware, and phishing. Spam (unsolicited commercial e-mail) consumes significant resources and is used as a delivery mechanism for other types of cyberattacks; spyware (software that monitors user activity without user knowledge or consent) can capture and release sensitive data, make unauthorized changes, and decrease system performance; and phishing (fraudulent messages to obtain personal or sensitive data) can lead to identity theft, loss of sensitive information, and reduced trust and use of electronic government services. The blending of these threats creates additional risks that cannot be easily mitigated with currently available tools.

SM-4.2. Hiring, transfer, termination, and performance policies address security

The security policies and procedures (including relevant personnel and human resources policies and procedures) that should generally be in place include the following:

- Hiring procedures include contacting references, performing background investigations, and ensuring that periodic investigations are performed as required by law and implementing regulations, consistent with the sensitivity of the position, per criteria from the Office of Personnel Management.
- Individuals are screened before they are authorized to have access to organizational information and information systems.
- For employees and contractors assigned to work with confidential information, confidentiality, nondisclosure, or security access agreements specify precautions required and unauthorized disclosure acts, contractual rights, and obligations during employment and after termination.
- Periodic job rotations and vacations are used, if appropriate, and work is temporarily reassigned during vacations.

- A formal sanctions process enforces (including performance ratings for individual employees) compliance with security policies and procedures.
- Compensation and recognition are appropriate to promote high morale.
- Where appropriate, termination and transfer procedures include
  - exit interview procedures;
  - return of property, such as keys, identification cards, badges, and passes;
  - notification to security management of terminations, and prompt termination of access to the entity's resources and facilities (including passwords);
  - the immediate escorting of terminated employees—especially those who have access to sensitive resources—out of the entity's facilities; and
  - identification of the period during which nondisclosure requirements remain in effect.

SM-4.3. Employees have adequate training and expertise

Management should ensure that employees—including data owners, system users, data processing personnel, and security management personnel—have the expertise to carry out their information security responsibilities. To accomplish this, a security training program should be developed that includes

- job descriptions that include the education, experience, and expertise required;
- periodically reassessing the adequacy of employees' skills;
- annual training requirements and professional development programs to help make certain that employees' skills, especially technical skills, are adequate and current; and
- monitoring employee training and professional development accomplishments.

SM-4 Related NIST SP 800-53 Controls	
AT-2	Security Awareness
AT-3	Security Training
AT-4	Security Training Records
PL-4	Rules of Behavior
PS-1	Personnel Security Policy and Procedures
PS-2	Position Categorization
PS-3	Personnel Screening
PS-4	Personnel Termination
PS-5	Personnel Transfer
PS-6	Access Agreements
PS-7	Third-Party Personnel Security
PS-8	Personnel Sanctions

Control Techniques and Suggested Audit Procedures for Critical Element SM-4

Table 9. Control Techniques and Suggested Audit Procedures for Critical Element SM-4: Implement effective security awareness and other security-related personnel policies

Control activities	Control techniques	Audit procedures
SM-4.1. Owners, system administrators, and users are aware of security policies.	SM-4.1.1. An ongoing security awareness program has been implemented that includes security briefings and training that is monitored for all employees with system access and security responsibilities. Coordinate with the assessment of the training program in SM-4.3.	Review documentation supporting or evaluating the awareness program. Observe a security briefing. Interview data owners, system administrators, and system users. Determine what training they have received and if they are aware of their security-related responsibilities. Determine whether adequate procedures are implemented to monitor that all employees and contractors are receiving security awareness training.

Control activities	Control techniques	Audit procedures
	SM-4.1.2. Security policies are distributed to all affected personnel, including system and application rules and expected user behaviors.	Review memos, electronic mail files, or other policy distribution mechanisms. Review personnel files to test whether security awareness statements are current. If appropriate, call selected users, identify yourself as security or network staff, and attempt to talk them into revealing their password. (See Section 2.2.2 “Appropriateness of Control Testing” for discussion of performance issues relating to this type of testing).
SM-4.2. Hiring, transfer, termination, and performance policies address security.	SM-4.2.1. For prospective employees, references are contacted and background checks performed. Individuals are screened before they are given authorization to access organizational information and information systems.	Review hiring policies. For a selection of recent hires, inspect personnel records and determine whether references have been contacted and background checks have been performed.
	SM-4.2.2. Periodic reinvestigations are performed as required by law, and implementing regulations [at least once every 5 years], consistent with the sensitivity of the position. For federal entities, criteria can be obtained from the Office of Personnel Management (OPM).	Review applicable laws, regulations and reinvestigation policies (e.g. 5 CFR 731.106(a); OPM/Agency policy, regulations and guidance; FIPS 201 & NIST SP 800-73, 800-76, 800-78; and, any criteria established for the risk designation of the assigned position.) For a selection of sensitive positions, inspect personnel records and determine whether background reinvestigations have been performed as required.
	SM-4.2.3. Nondisclosure or security access agreements are required for employees and contractors assigned to work with sensitive information.	Review policies on confidentiality or security agreements. For a selection of such users, determine whether confidentiality or security agreements are on file.
	SM-4.2.4. When appropriate, regularly scheduled vacations exceeding several days are required, and the individual’s work is temporarily reassigned.	Review vacation policies. Inspect personnel records to identify individuals who have not taken vacation or sick leave in the past year. Determine who performed employee’s work during vacations.
	SM-4.2.5. A formal sanctions process is employed for personnel failing to comply with security policy and procedures.	Review the sanctions process. Determine how compliance with security policies is monitored and how sanctions were administered.

Control activities	Control techniques	Audit procedures
	SM-4.2.6. Where appropriate, termination and transfer procedures include • exit interview procedures; • return of property, keys, identification cards, passes, etc.; • notification to security management of terminations and prompt revocation of IDs and passwords; • immediate escort of terminated employees out of the entity's facilities; and • identification of the period during which nondisclosure requirements remain in effect.	Review pertinent policies and procedures. For a selection of terminated or transferred employees, examine documentation showing compliance with policies. Compare a system-generated list of users to a list of active employees obtained from personnel to determine whether IDs and passwords for terminated employees still exist.
SM-4.3. Employees have adequate training and expertise.	SM-4.3.1. Skill needs are accurately identified and included in job descriptions, and employees meet these requirements.	Review job descriptions for security management personnel and for a selection of other system users. For a selection of employees, compare personnel records on education and experience with job descriptions.
	SM-4.3.2. Employee training and professional development are documented and monitored.	Review training records and related documentation showing whether such records are monitored and whether employees are receiving the appropriate training.

Source: GAO.

Critical Element SM-5. Monitor the effectiveness of the security program

An important element of risk management is ensuring that policies and controls intended to reduce risk are effective on an ongoing basis. Effective monitoring involves the entity performing tests of IS controls to evaluate or determine whether they are appropriately designed and operating effectively to achieve the entity's control objectives. Senior management's awareness, support, and involvement are essential in establishing the control environment needed to promote compliance with the agency's/entity's information security program. However, because security is not an end in itself, senior managers should balance the emphasis on security with the larger objective of achieving the agency's/entity's mission. To do this effectively, top management should understand the agency's/entity's security risks and actively support and monitor the effectiveness of its security policies. If senior management does not monitor the security program, it is unlikely that others in the

organization will be committed to properly implementing it. Monitoring is one of GAO's five internal control standards.[64]

Over time, policies and procedures may become inadequate because of changes in threats, changes in operations or deterioration in the degree of compliance. Periodic assessments are an important means of identifying areas of noncompliance, reminding employees of their responsibilities, and demonstrating management's commitment to the security plan. Such assessments can be performed by entity staff or by external reviewers engaged by management. Independent audits performed or arranged by GAO and by agency inspectors general, while an important check on management performance, should not be viewed as substitutes for management evaluations of the adequacy of the entity's security program.

FISMA requires federal agencies to perform periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices. First, agencies must provide management testing of every system every year, but the level of rigor may vary depending on the risk. However, OMB in past FISMA reporting guidance (M-03-19) has noted that annual FISMA testing does not alter OMB's policy requiring system reauthorization (certification and accreditation) at least every 3 years or when significant changes are made.[65]

Second, FISMA requires annual independent evaluations of agency information security programs and practices to determine their effectiveness. Independent evaluations of non-national-security systems are to be performed by the agency's Inspector General, or by an independent external auditor chosen by the IG, if any, or by the head of the agency, if there is no agency IG. Evaluations related to national security systems are to be performed only by an entity designated by the agency head. These independent evaluations must test the effectiveness of control techniques for a representative

[64]Standards for Internal Control in the Federal Government (GAO/AIMD-00-21.3.1; November 1999).
[65]OMB's Circular A-130 requires that agencies review security controls and re-authorize system usage (i.e., certification and accreditation) at least every three years or more frequently if changes occur.

subset of systems. The head of each agency must report the evaluation results to OMB, which summarizes the results in a report to the Congress. GAO must also provide Congress with its independent assessment of agency information security policies and practices, including compliance with the annual evaluation and reporting requirements.

As part of its monitoring function, management should have policies and procedures for periodically assessing the appropriateness of security policies and the agency's compliance with them. At a minimum, such policies and procedures should address the following areas:

- Frequency of periodic testing. The frequency, nature, and extent of management's assessment should appropriately consider information security risks. Consequently, certain higher-risk systems may be tested more frequently or more extensively than lower-risk systems. FISMA requires periodic testing to be performed with a frequency depending on risk, but no less than annually.

- Depth and breadth of testing. The depth and breadth of testing should be based on a consideration of potential risk and magnitude of harm, the relative comprehensiveness of prior reviews, the nature and extent of tests performed as part of periodic risk and vulnerability assessments, and the adequacy and successful implementation of remediation plans.

- Common controls. To facilitate efficient periodic testing, entities should identify common IS controls that can be tested and the results used for multiple systems.

- Roles and responsibilities of personnel involved in testing. Personnel assigned to perform and supervise periodic testing should possess appropriate technical skills and have appropriate organizational placement to reasonably assure that tests are properly performed and results properly reported to entity management. In addition, personnel should not perform tests of controls for which they are responsible for implementation or operation.

- Documentation. Tests performed and the results and related analysis of such tests should be documented to the extent necessary to support effective supervisory review and independent evaluation.

An integrated testing plan or strategy helps to facilitate effective and efficient periodic testing. Without such an integrated plan or strategy, the nature and extent of periodic testing may be inadequate or testing may be inefficient.

Such tests may include tests performed as part of periodic risk and vulnerability assessments, continuous monitoring through scanning or agent-based software tools, or specifically designed tests. Management should periodically perform vulnerability assessments to help ensure that entity information resources are adequately protected. Vulnerability assessments involve analyzing a network to identify potential vulnerabilities that would allow unauthorized access to network resources, simulating what might be performed by someone trying to obtain unauthorized access. Vulnerability assessments typically consider both unauthorized access by outsiders as well as insiders. Vulnerability assessments typically include the use of various tools discussed in Table 10 below, such as scanning tools, password crackers, and war dialing and war driving tools. Also, vulnerability assessments may include penetration testing. Vulnerability assessments should be performed in addition to testing individual access controls and other control categories.

Since the methods used for unauthorized access vary greatly and are becoming more sophisticated, the vulnerability assessment techniques defined here are general in nature and should be supplemented with techniques and tools specific to the specific environment.

The effectiveness of management's security testing, including vulnerability assessments, may affect the auditor's judgments about IS risk and consequently, the nature, timing, and extent of audit testing. Factors to consider in assessing the effectiveness of management's testing include:

- the nature of management's testing (the types of testing management applied, the strength of the evidence obtained, the experience, capabilities, and objectivity of the persons performing the testing, and the quality of documentation of testing),
- the timing of management's testing (the recentness of testing), and
- extent of management's testing (the completeness of testing)

The auditor should review management vulnerability assessments and may independently perform their own vulnerability assessments to determine whether management vulnerability assessments are effective.

The type of vulnerability assessments that are conducted by the auditor affect the scope of the evaluation, methodology used, and the level of assurance achieved. It is important that the methods chosen by the auditor provide the least amount of disruption to the entity based on a cost/risk analysis. Auditors may need to conduct these types of audits without tools,[66] because some audited entities will not want to accept the risk of an auditor running tools in a "live" environment. There generally should be an agreement between the auditor and the audited entity on the type of testing to be conducted (intrusive or nonintrusive). Section 2.1.9.F "Communication with Entity Management and Those Charged with Governance" provides further guidance on communicating the nature and extent of planned testing with the entity.

Due to the highly technical nature of such testing by the auditor, it should be performed by persons possessing the necessary technical skills (e.g., an IT specialist). See Appendix V for additional information on the Knowledge, Skills, and Abilities needed to perform IS control audits. Also, section 2.5.2 "Automated Audit

[66] Assessments performed relying on reviews of system documentation such as hardware and software security settings and use of software features that are inherent to the application under review.

Tools" provides further guidance on the auditor's use of testing tools. Audit testing is discussed further in connection with AC-.1.1.

There are several different types of security testing. Some testing techniques are predominantly manual, requiring an individual to initiate and conduct the test. Other tests are highly automated and require less human involvement. Testing may also be conducted from external connections (for example, from the Internet, dial-up, wireless), from wide area network connections, or from internal connections. Regardless of the type of testing, staff that set up and conduct security testing should have significant security and networking knowledge, including significant expertise in the following areas: network security, firewalls, intrusion detection systems, operating systems, programming and networking protocols (such as Transmission Control Protocol/Internet Protocol (TCP/IP) – which is a low-level communication protocol that allows computers to send and receive data).

Table 10 summarizes types of security testing.

Table 10. Types of Security Testing

Test type	What it does
Network scanning	• Enumerates the network structure and determines the set of active hosts and associated software • Identifies unauthorized hosts connected to a network • Identifies open ports • Identifies unauthorized services
General vulnerability scanning	• Enumerates the network structure and determines the set of active hosts and associated software • Identifies a target set of computers to focus vulnerability analysis • Identifies potential vulnerabilities on the target set • Verifies that software (e.g., operating systems and major applications) is up-to-date with security patches and software versions
Penetration testing	• Determines how vulnerable an organization's network is to penetration and the level of damage that can be incurred • Tests IT staff's response to perceived security incidents and their knowledge of and implementation of the organization's security policy and system's security requirements • Verifies potential impact of multiple security weaknesses
Password cracking	• Verifies that the policy is effective in producing passwords that are more or less difficult to break • Verifies that users select passwords that are compliant with the organization's security policy

Test type	What it does
Log reviews	• Verifies that the system is operating according to policy
Integrity checkers	• Detects unauthorized file modifications
Virus detectors	• Detects and deletes viruses before successful installation on the system
War dialing	• Detects unauthorized modems and prevents unauthorized access to a protected network
War driving	• Detects unauthorized wireless access points and prevents unauthorized access to a protected network
Specialty scanning tools	• Detects security risks related to specific IS control areas (e.g., weaknesses in web pages, application code, and databases, network sniffers[67])

Source: Guideline on Network Security Testing (NIST SP 800-42, October 2003).

Often, several of these testing techniques are used together for a more comprehensive assessment of the overall network security posture. For example, penetration testing usually includes network scanning and vulnerability scanning to identify vulnerable hosts and services that may be targeted for later penetration. Some vulnerability scanners incorporate password cracking. None of these tests by themselves will provide a complete picture of the network or its security posture. NIST SP 800-42 describes these testing types in detail and summarizes the strengths and weaknesses of each test. In addition, NIST SP 800-115 provides guidance on the basic technical aspects of conducting information security assessments.

However, since penetration testing requires extensive planning and experienced staff to conduct, the auditor typically considers several factors before deciding to perform this testing. For example, penetration testing may be a desirable testing option when significant changes have been made to the entity's network (e.g., upgrades to server, routers, switches, network software), there are no recent penetration tests performed, or results of recent penetration testing identified significant security weaknesses that management represented were substantially corrected. Conversely, if recent independent penetration testing disclosed few security weaknesses and the scope and level of testing is determined by the

[67]Network "sniffers" (software that can intercept and log traffic passing over a network) can identify the transmission of passwords or sensitive information in clear text.

auditor to be sufficient, then the use of other types of testing may be more appropriate.

Other tools that may be used include specialty scanning tools (for example, application code, Web, database, SNMP[68]), host data extraction tools, packet analyzers or sniffers (for example, ethereal), and patch assessment tools. Separate patch assessment tools are more reliable than vulnerability scanners for this purpose. Also, the auditor is more likely to check for the presence of integrity checkers and virus detectors than to use them in an audit. After running any tests, certain procedures should be followed, including documenting the test results, informing system owners of the results, and ensuring that vulnerabilities are patched or mitigated.

When implementing system security plans for federal systems, as required by FISMA and OMB Circular A-130, management should monitor their implementation and adjust the plans in accordance with changing risk factors. Management should

- develop and document appropriate testing policies and procedures (all levels),
- test and document security controls related to each major system at least annually (system level),
- ensure that the frequency and scope of testing is commensurate with risk (all levels), and
- employ automated mechanisms to verify the correct operation of security functions when anomalies are discovered (system and application level).

In addition to the FISMA provisions in the E-Government Act of 2002, section 208 requires that agencies conduct privacy impact assessments. A privacy impact assessment is an analysis of how information is handled (1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) to determine the risks and effects of collecting,

[68]SNMP (Simple Network Management Protocol) provides remote administration of network devices.

maintaining, and disseminating information in identifiable form in an electronic information system; and (3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks (OMB Memorandum M-03-22). OMB combined the FISMA and privacy annual reporting beginning in fiscal year 2005 (OMB Memorandum M-05-15).

Further, OMB has developed performance measures for federal agency reporting and requires that agencies provide quarterly performance metric updates. For example, one such measure requests the number of systems for which security controls have been tested and evaluated in the past year. NIST SP 800-55 provides additional guidance on performance measures and compliance metrics to monitor the security process and periodically report on the state of compliance.

In addition, NIST SP 800-100 provides information on how entities can develop information security metrics that measure the effectiveness of their security program, and provide data to be analyzed and used by program managers and system owners to isolate problems, justify investment requests, and target funds specifically to the areas in need of improvement. It describes metric types and discusses development and implementation approaches.

As mentioned, OMB Circular A-130 requires that federal agencies review and test the security of their general support systems and major applications at least once every 3 years—sooner if significant modifications have occurred or where the risk and magnitude of harm are high. Although not required, it would be appropriate for an agency to describe its evaluation program, including the expected type of testing and frequency of evaluations, in its security plan. (Security plans are discussed in critical element SM-1.)

OMB also requires that a management official authorize in writing the use of each general support system and major application. NIST SP 800-37 refers to this authorization as accreditation. OMB Circular A-130 allows self-reviews of controls for general support systems, but requires an independent review or audit of major applications. The authorizations or accreditations are to be provided by the program or functional managers whose missions are supported by

the automated systems; these represent the managers' explicit acceptance of risk based on the results of any security reviews, including those performed as part of financial statement audits and during related risk assessments. Additional guidance on accrediting federal automated systems can be found in NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*.

In addition, FMFIA and OMB Circular A-123[69] require agencies to annually assess their internal controls, including computer-related controls, and report any identified material weaknesses to the President and the Congress. The quality of the FMFIA process is a good indicator of management's (1) philosophy and operating style, (2) methods of assigning authority and responsibility, and (3) control methods for monitoring and follow-up. Weaknesses identified during security reviews conducted under OMB Circular A-130 are to be considered for reporting under FMFIA and OMB Circular A-123, particularly if the weakness involves no assignment of security responsibility, an inadequate security plan, or missing management authorization.

SM-5 Related NIST SP 800-53 Controls
CA-2 Security Assessments
CA-7 Continuous Monitoring
PL-5 Privacy Impact Assessment
RA-5 Vulnerability Scanning

Control Techniques and Suggested Audit Procedures for Critical Element SM-5

Table 11. Control Techniques and Suggested Audit Procedures for Critical Element SM-5: Monitor the effectiveness of the security program

Control activities	Control techniques	Audit procedures
SM-5.1. The effectiveness of security controls are periodically assessed	SM-5.1.1. Appropriate monitoring and testing policies and procedures are documented.	Review testing policies and procedures. Determine if there is an overall testing strategy or plan.

[69]Office of Management and Budget, *Management's Responsibility for Internal Control*, OMB Circular No. A-123 (Washington, D.C.: December 2004).

Control activities	Control techniques	Audit procedures
	SM-5.1.2. Management routinely conducts vulnerability assessments and promptly corrects identified control weaknesses.	Interview officials who conducted the most recent agency/entity vulnerability assessment. Review the methodology and tools used, test plans and results obtained, and corrective action taken. Determine if testing is performed that complies with OMB and NIST certification and accreditation and other testing requirements. If appropriate, perform independent testing with the approval of management. Determine if identified control weaknesses are promptly corrected.
	SM-5.1.3. Management routinely conducts privacy impact assessments and promptly corrects identified control weaknesses.	Review privacy impact assessments, including the methodology, a selection of test plans, and related testing results.
	SM-5.1.4. The frequency and scope of security control testing is commensurate with risk.	Determine if the frequency and scope of security control testing is based on risk.
	SM-5.1.5. Performance measures and compliance metrics monitor the security processes and report on the state of compliance in a timely manner.	Review agency/entity performance measures and compare to NIST guidance (e.g., NIST SP 800-55).
	SM-5.1.6. An independent evaluation (periodic, e.g., annual) of the entity's information security program tests the effectiveness of the security policies, procedures, and practices.	Review the results of these evaluations and assess their adequacy and effectiveness.
	SM-5.1.7. Federal agencies report on the results of the annual independent evaluations to appropriate oversight bodies. Under OMB guidance, the head of each agency must submit security and privacy reports to OMB, which consolidates the information for a report to Congress. The Comptroller General must also periodically evaluate and report to Congress on the adequacy and effectiveness of agency information security policies and practices.	Evaluate the reporting/summarization process and identify any significant discrepancies between reports at each level and whether the reports agree with independent audit evaluations. Note that OMB has annual requirements for FISMA and privacy reporting.

Source: GAO.

Critical Element SM-6. Effectively Remediate Information Security Weaknesses

When weaknesses are identified, the related risks should be reassessed, appropriate corrective or remediation actions taken, and follow-up monitoring performed to make certain that corrective actions are effective. Procedures should be established to reasonably assure that all IS control weaknesses, regardless of how or by whom they are identified, are included in the entity's remediation processes. For each identified IS control weakness, the entity should develop and implement appropriate action plans and milestones. Action plans and

milestones should be developed based on findings from security control assessments, security impact analyses, continuous monitoring of activities, audit reports, and other sources. For federal agencies, such plans are referred to as Plans of Actions and Milestones (POAMs). When considering appropriate corrective actions to be taken, the entity should, to the extent possible, consider the potential implications throughout the entity and design appropriate corrective actions to systemically address the deficiency. Limiting corrective action only to identified deficiencies would not necessarily address similar weaknesses in other systems or applications or result in the most effective and efficient corrective action.

In addition to developing action plans and modifying written policies to correct identified problems, entities should test the implementation of the corrective actions to determine whether they are effective in addressing the related problems. Management should continue to periodically review and test such corrective actions to determine if they remain effective on a continuing basis. This is an important aspect of managers' risk management responsibilities.

FISMA specifically requires that agencywide information security programs include a "process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency." Further, agencies must report on the adequacy and effectiveness of the information security program and practices in annual reports to OMB, Congress, and GAO and in annual budget and management plans and reports. The latter include reporting a FISMA "significant deficiency" in information security as a material weakness. Government Performance and Results Act performance plans must describe time periods and resources needed to effectuate a risk-based program.

SM-6 Related NIST SP 800-53 Controls
CA-5 Plan of Action and Milestones

Control Techniques and Suggested Audit Procedures for Critical Element SM-6

Table 12. Control Techniques and Suggested Audit Procedures for Critical Element SM-6: Effectively remediate information security weaknesses

Control activities	Control techniques	Audit procedures
SM-6.1. Information security weaknesses are effectively remediated.	SM-6.1.1. Management initiates prompt action to correct deficiencies. Action plans and milestones are documented.	Review recent POA&Ms, FMFIA reports and prior year audit reports and determine the status of corrective actions. The objective of this procedure in an IS controls audit being performed as part of a financial audit or data reliability assessment is generally limited to understanding management's POAM process and related controls to ensure the accuracy of the information in the POA&Ms, determining whether IS control weaknesses identified by the IS controls audit are included in the POA&Ms, and, if not, determining the cause. See OMB A-11 which recommends that audit remediation items be addressed within 6 months.
	SM-6.1.2. Deficiencies are analyzed in relation to the entire agency/entity, and appropriate corrective actions are applied entitywide.	Review corrective action plans to determine whether entitywide solutions were appropriately considered.
	SM-6.1.3. Corrective actions are tested and are monitored after they have been implemented and monitored on a continuing basis.	Review a selection of corrective action plans to determine whether testing was performed and monitoring was conducted after implementation of corrective actions.

Source: GAO.

Critical Element SM-7. Ensure that Activities Performed by External Third Parties are Adequately Secure

Appropriate policies and procedures should be developed, implemented, and monitored to ensure that the activities performed by external third parties (for example, service bureaus, contractors, other service providers such as system development, network management, and security management) are documented, agreed to, implemented, and monitored for compliance. These should include provisions for (1) security clearances (where appropriate and required), (2) background checks, (3) required expertise, (4) confidentiality/nondisclosure agreements, (5) security roles and responsibilities, (6) connectivity agreements, (7) individual accountability (for example, expectations, remedies), (8) audit access and reporting, (9) termination procedures, (10) security awareness training, (11)

requirements definition, (12) security responsibilities, and (13) performance metrics. In addition, checks should be performed to periodically ensure that the procedures are being correctly applied and consistently followed, including the security of relevant contractor systems. Appropriate controls also need to be applied to outsourced software development.

FISMA information security requirements apply not only to information systems used or operated by an agency but also to information systems used or operated by a contractor of an agency or other agency on behalf of an agency. In addition, the Federal Acquisition Regulation (FAR) requires that federal agencies prescribe procedures for ensuring that agency planners on information technology acquisitions comply with the information technology security requirements of FISMA, OMB's implementing policies including Appendix III of OMB Circular A-130, and guidance and standards from NIST.[70] For example, NIST SP 800-35 *Guide to Information Technology Security Services* provides guidance pertaining to the acquisition or outsourcing of dedicated information system security services such that (1) incident monitoring, analysis, and response; (2) operation of information system security devices (for example, firewalls); and (3) key management services are supported by a risk assessment and approved by the appropriate, designated entity official. Acquisition or outsourcing of information system services explicitly addresses government, service provider, and end-user security roles and responsibilities.

Governmental and private entities face a range of risks from contractors and other users with privileged access to their systems, applications and data. Contractors that provide systems and services or other users with privileged access to agency/entity systems, applications, and data can introduce risks to their information and systems; for example, contractors often provide unsupervised remote maintenance and monitoring of agency/entity

[70]The FAR was established to codify uniform policies for acquisition of supplies and services by executive agencies. The FAR appears in the Code of Federal Regulations at 48 CFR Chapter 1. See 48 CFR 7.103(u).

systems. Contractor risks to people, processes, and technology are summarized in table 13.

Table 13. Examples of Agency-Identified Risks to Federal Systems and Data Resulting from Reliance on Contractors

Category	Risk description
People	Unauthorized personnel having physical access to entity IT resources (including systems, applications, facilities, and data).
	Unauthorized personnel having electronic access to entity IT resources (including systems, applications, and data).
	Increased use of foreign nationals.
	Contractor or privileged users of federal data and systems who may not receive appropriate, periodic background investigations.
	Inadequate segregation of duties (for example, software developer is the same individual who puts the software into production).
Processes	Failure by contractor or privileged users of federal data and systems to follow entity IT security requirements.
	Possible disclosure of entity-sensitive information to unauthorized individuals or entities.
	Lack of effective compliance monitoring of contractors performing work off-site or privileged users of federal data and systems.
	Contractor or privileged users of federal data and systems may have ineffective patch management processes.
Technology	Incorporation of unauthorized features in customized application software. For example, a third-party software developer has the potential to incorporate “back doors,” spyware, or malicious code into customized application software that could expose entity IT resources to unauthorized loss, damage, modification, or disclosure of data.
	Encryption technology may not meet federal standards.
	Intentional or unintentional introduction of viruses and worms.

Source: Improving Oversight of Access to Federal Systems and Data by Contractors Can Reduce Risk (GAO-05-362, April 2005).

Note: The various risks identified could represent multiple risks (i.e., risks in one or more of the identified categories of people, processes, and technology).

In addition to the risks identified in the table, there are specific risks from contractor software development activities and off-site operations. These risks include a poor patch management process that could impact entity operations (for example, entity Web sites), a hosting infrastructure that may not separate customer and company data, and inadequate oversight at an off-site facility.

SM-7 Related NIST SP 800-53 Controls
AC-20 Use of External Information Systems
MA-4 Remote Maintenance
PS-7 Third-Party Personnel Security

Control Techniques and Suggested Audit Procedures for Critical Element SM-7

Table 14. Control Techniques and Suggested Audit Procedures for Critical Element SM-7: Ensure that activities performed by external third parties are adequately secure

Control activities	Control techniques	Audit procedures
SM-7.1. External third party activities are secure, documented, and monitored.	SM-7.1.1. Appropriate policies and procedures concerning activities of external third parties (for example, service bureaus, contractors, other service providers such as system development, network management, security management) are documented, agreed to, implemented, and monitored for compliance and include provisions for • clearances, • background checks, • required expertise, • confidentiality agreements, • security roles and responsibilities, • connectivity agreements, • expectations, • remedies, • audit access/audit reporting, • monitoring • termination procedures, • security awareness training, • requirements definition, • security responsibilities, and • performance metrics.	Review policies and procedures pertaining to external third parties for the entitywide, system, and application levels. Identify use of external third parties and review activities including compliance with applicable policies and procedures. See NIST SP 800-35 for guidance on IT security services. Determine how security risks are assessed and managed for systems operated by a third party. Assess the adequacy of controls over monitoring external third party services. Coordinate assessment of security awareness training with SM-4. Review any available SAS 70 reports to determine the nature, timing, and extent of tests of operating effectiveness and assess whether results provide sufficient information to obtain an understanding of the service organization's controls that would affect the entity's controls being assessed.
	SM-7.1.2. Security requirements are included in the information system acquisition contracts based on an assessment of risk.	Review security provisions of selected contracts and determine that requirements are implemented. See FAR requirements for acquisition plans (48 CFR 7.1, 7.103 (u)).

Source: GAO.

3.2. Access Controls (AC)

Access controls limit or detect inappropriate access to computer resources (data, equipment, and facilities), thereby protecting them from unauthorized modification, loss, and disclosure. Such controls include both logical and physical controls. Logical access controls require users[71] to authenticate themselves (through the use of secret passwords or other identifiers) and limit the files and other resources that authenticated users can access and the actions that they can execute. Physical access controls involve restricting physical access to computer resources and protecting them from intentional or unintentional loss or impairment. Without adequate access controls, unauthorized individuals, including outside intruders and former employees, can surreptitiously read and copy sensitive data and make undetected changes or deletions for malicious purposes or personal gain. In addition, authorized users can intentionally or unintentionally read, add, delete, modify, or exfiltrate data or execute changes that are outside their span of authority.

Access control policies and procedures should be formally developed, documented, disseminated, and periodically updated. Policies should address purpose, scope, roles, responsibility, and compliance issues; procedures should facilitate the implementation of the policy and associated access controls. NIST SP 800-12 provides guidance on security policies and procedures. It is fundamental that control techniques for both logical and physical access controls be risk-based. Access control policies and procedures and risk assessments are covered in section 3.1 of the manual.

For access controls to be effective, they should be properly authorized, implemented, and maintained. First, an entity should analyze the responsibilities of individual computer users to determine what type of access (for example, read, modify, delete)

[71] As used herein, users include those given any level of authorized access to computer resources, including business process application users, system administrators, etc.

users need to fulfill their responsibilities. Then, specific control techniques, such as specialized access control software, should be implemented to restrict access to these authorized functions alone. Such software can be used to limit a user's activities associated with specific systems or files and keep records of individual users' actions on the computer. Finally, access authorizations and related controls should be monitored, maintained, and adjusted on an ongoing basis to accommodate new and departing employees and changes in users' responsibilities and related access needs.

Inadequate access controls diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure of data. The following examples illustrate the potential consequences of such vulnerabilities.

- By obtaining direct logical access to data files, an individual could make unauthorized changes for personal gain or obtain sensitive information. For example, a person could (1) alter the address of a payee and thereby direct a disbursement to himself or herself, (2) alter inventory quantities to conceal a theft of assets, (3) alter critical data needed to make a strategic policy decision, or (4) obtain confidential personal, commercial, and governmental information.
- By obtaining logical access to business process applications[72] used to process transactions, an individual could grant unauthorized access to the application, make unauthorized changes to these programs, or introduce malicious programs, which, in turn, could be used to access data files, resulting in situations similar to those just described, or the processing of unauthorized transactions. For example, a person could alter a payroll or payables program to inappropriately generate a check for him/herself.
- By obtaining access to system-level resources, an individual could circumvent security controls to read, add, delete, modify,

[72]A computer program designed to help perform a business function such as payroll, inventory control, accounting, and mission support. Depending on the work for which it was designed, an application can manipulate text, numbers, graphics, or a combination of these elements.

or exfiltrate critical or sensitive business information or programs. Further, authorized users could gain unauthorized privileges to conduct unauthorized actions or to circumvent edits and other controls built into the application programs.

- By obtaining physical access to computer facilities and equipment, an individual could (1) obtain access to terminals or telecommunications equipment that provide input into the computer, (2) obtain access to confidential or sensitive information on magnetic or printed media, (3) substitute unauthorized data or programs, or (4) steal or inflict malicious damage on computer equipment and software.

The objectives of limiting access are to ensure that

- outsiders (for example, hackers) cannot gain unauthorized access to the entity's systems or data;
- authorized users have only the access needed to perform their duties;
- access to very sensitive resources, such as operating systems and security software programs, are limited to very few individuals;
- employees/contractors are restricted from performing incompatible functions or functions beyond their responsibility. (Segregation of duties is discussed in greater detail in section 3.4.)

If these objectives are met, the risk of inappropriate modification or disclosure of data can be reduced without interfering with users' practical needs. However, establishing the appropriate balance between user needs and security requires a careful analysis of the criticality and sensitivity of information resources available and the tasks performed by users. Access controls also apply to alternate work sites (for example, employee residence or contractor facility).

Implementing adequate access controls involves first determining what level and type of protection is appropriate for individual resources based on a risk assessment and on who needs access to these resources. These tasks should be performed by the resource owners. For example, program managers should determine how valuable their program data resources are and what access is

appropriate for personnel who must use an automated system to carry out, assess, and report on program operations. Similarly, managers in charge of systems development and modification should determine the sensitivity of hardware and software resources under their control and the access needs of systems analysts and programmers, and system administration officials should determine the access needs of their personnel. Levels of access granted to information resources should be consistent with FIPS 199 risk levels.

This section defines a set of critical elements that should be considered when conducting a comprehensive assessment of access controls. Today's networks and control environments are highly diverse, complex, and interconnected. Devices that are interconnected develop control dependencies (discussed in Chapter 2), directly and indirectly, on other devices such as routers, firewalls, switches, domain name servers, Web servers, network management stations, e-mail systems, and browser software. Audit objectives that are limited to targeted assessments such as a UNIX or Windows audit may not fully recognize the control dependencies on these systems.

Unfortunately, there are no simple solutions to controlling logical access. Each entity decides what combination of technologies to deploy and to what degree, based on business needs and priorities, risk management, and other factors. For instance, an entity may decide not to require users to periodically change passwords for e-mail because initial entry to the system relies on a two-factor token-based authentication system. Other entities may rely less on boundary protection but place more emphasis on audit and monitoring. Accordingly, the collection of controls used will vary from entity to entity.

The six critical elements for access controls are described here.

- *Boundary Protection.* Boundary protection pertains to the protection of a logical or physical boundary around a set of information resources and implementing measures to prevent unauthorized information exchange across the boundary in either

direction. Firewall devices represent the most common boundary protection technology at the network level

- *Identification and authentication*. If logical connectivity is allowed, then the users, processes acting on behalf of users, services, and specific devices are identified and authenticated by the information system. For example, users' identities may be authenticated through something they know (a traditional password), something they have (such as a smart card), or something about them that identifies them uniquely (such as a fingerprint).
- *Authorization*. If authentication is successful, authorization determines what users can do; i.e., it grants or restricts user, service, or device access to various network and computer resources based on the identity of the user, service, or device.
- *Sensitive system resources*. Controls over sensitive system resources are designed to ensure the confidentiality, integrity, and availability of system data such as passwords and keys during transmission and storage. Technologies used to control sensitive data include encryption, certificate management, hashing, checksums, and steganography.[73]
- *Audit and monitoring*. Audit and monitoring control involves the collection, review, and analysis of auditable events for indications of inappropriate or unusual activity. These controls should be used to routinely assess the effectiveness of information security controls, perform investigations during and after an attack, and recognize an ongoing attack.
- *Physical security*. Physical security controls restrict physical access or harm to computer resources and protect these resources from intentional or unintentional loss or impairment. Such controls include guards, gates, and locks, and also environmental controls such as smoke detectors, fire alarms and extinguishers, and uninterruptible power supplies.

[73]Steganography is a technique that hides the existence of a message (for example, by embedding it within another message) and may be used where encryption is not permitted or to hide information in an encrypted file in case the encrypted file is deciphered. Other uses include digital watermarking and fingerprinting of audio and video files.

Although the primary relevance of these concepts is to access controls, they are also relevant to other areas, such as security management and configuration management. For example, configuration management assurance controls help ensure that network devices are configured and are operating as intended. This would include verifying operational patch levels, disabling unnecessary and dangerous services, correcting poorly configured services, and protecting against viruses and worms. Also, these concepts are relevant to activities such as periodic self-assessment programs (covered in Section 3.1, Security Management).

Assessing access controls involves evaluating the entity's success in performing each of the critical elements listed in Table 15. When evaluating control techniques and performing audit procedures for access controls, the auditor considers access to networks, access to operating systems, and access to infrastructure applications.[74]

As discussed in section 2.2.2, the auditor may determine that it is appropriate to attempt to gain access to identified key systems (e.g., vulnerability assessments or penetration tests). In performing this testing, it is important that the auditor and entity management have a common understanding of the type of tests to be performed, scope of the tests, and the risks involved in performing this testing. See section 2.1.9.F concerning communication with entity management.

Table 15. Critical Elements for Access Control

Number	Description
AC-1.	Adequately protect information system boundaries
AC-2.	Implement effective identification and authentication mechanisms
AC-3.	Implement effective authorization controls
AC-4.	Adequately protect sensitive system resources
AC-5.	Implement an effective audit and monitoring capability
AC-6.	Establish adequate physical security controls

Source: GAO

[74]Infrastructure applications include databases, e-mail, browsers, plug-ins, utilities, and other applications.

Critical Element AC-1. Adequately protect information system boundaries

Boundary protection controls logical connectivity into and out of networks and controls connectivity to and from network connected devices. At the entitywide level, access control policy is developed and promulgated through procedures, manuals, and other guidance. At the system level, any connections to the Internet, or to other external and internal networks or information systems, should occur through controlled interfaces (for example, proxies, gateways, routers and switches, firewalls, and concentrators). At the host or device level, logical boundaries can be controlled through inbound and outbound filtering provided by access control lists and personal firewalls. At the application level, logical boundaries to business process applications may be controlled by access control lists in security software or within the applications.

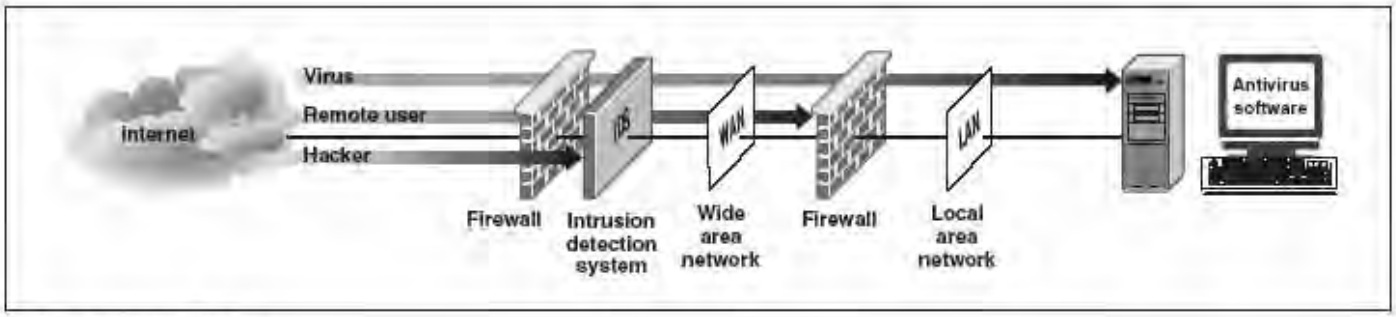
Implementing multiple layers of security to protect information system internal and external boundaries provides Defense-in-Depth(described earlier in Additional IS Risk Factors). According to security experts, a best practice for protecting systems against cyber attacks is for entities to build successive layers of defense mechanisms at strategic points in their information technology infrastructures. By using the strategy of Defense-in-Depth, entities can reduce the risk of a successful cyber attack. For example, multiple firewalls could be deployed to prevent both outsiders and trusted insiders from gaining unauthorized access to systems: one firewall could be deployed at the network's Internet connection to control access to and from the Internet, while another firewall could be deployed between wide area networks and local area networks to limit employees' access.

In addition to deploying a series of security technologies at multiple layers, deploying diverse technologies at different layers also mitigates the risk of successful cyber attacks. If several different technologies are deployed between the adversary and the targeted system, the adversary must overcome the unique obstacle presented by each of the technologies. For example, firewalls and intrusion detection technologies can be deployed to defend against attacks from the Internet, and antivirus software can be used to provide integrity protection for data transmitted over the network. Thus,

Defense-in-Depth can be effectively implemented through multiple security measures among hosts, local area networks and wide area networks, and the Internet.

Defense-in-Depth also entails implementing an appropriate network configuration, which can, in turn, affect the selection and implementation of cybersecurity technologies. For example, configuring the entity's network to channel Internet access through a limited number of connections improves security by reducing the number of points that can be attacked from the Internet. At the same time, the entity can focus technology solutions and attention on protecting and monitoring the limited number of connections for unauthorized access attempts. Figure 4 depicts how applying a layered approach to security through deploying both similar and diverse cybersecurity technologies at multiple layers can deflect different types of attacks.

Figure 4. Layered Approach to Network Security



Source: GAO analysis and Corel Draw.

Note: Excerpt from GAO, *Technologies to Secure Federal Systems,* GAO-04-467 (Washington, D.C.: March 2004).

AC-1.1. Appropriately control connectivity to system resources

Users obtain access to data files and software programs through one or more access paths through the networks and computer hardware and software. Accordingly, to implement an appropriate level of security, it is important that the entity, to the extent possible, identify, document, and control all access paths. Further, connectivity between systems should be approved only when

appropriate by entity management. Consideration should be given to the risk and corresponding safeguards needed to protect sensitive data. NIST SP 800-47 provides guidance on interconnecting information systems.

Networks should be appropriately configured to adequately protect access paths between systems and consider the existing technologies. For standalone computers, identifying access paths may be relatively simple. However, in a networked environment, careful analysis is needed to identify all of the system's entry points and paths to sensitive files. Networked systems typically consist of multiple personal computers that are connected to each other and to larger computers, such as file servers or mainframe processors. Many allow remote access (for example, dial-up, wireless, Internet) to the information systems from virtually any remote location. As a result, the entry points to the system can be numerous. Also, once the system has been entered, the programs available may provide multiple paths to various data resources and sensitive applications. Consequently, it is very important that all access paths be appropriately controlled and protected based on risk.

It is critical that access paths are identified as part of a risk analysis and documented in an access path diagram or similar network schematic. Such a diagram or schematic identifies the users of the system, the type of device from which they can access the system, the software used to access the system, the resources they may access, the system on which these resources reside, and the modes of operation and telecommunications paths. The goal in identifying access paths is to assist in identifying the points from which system resources could be accessed and the data stored—points that, therefore, must be controlled. Specific attention should be given to "backdoor" methods of accessing data by operators and programmers. As with other aspects of risk analysis, the access path diagram should be reviewed and updated whenever any changes are made to the system or to the nature of the program and program files maintained by the system.

If entry points and access paths are not identified, they may not be adequately controlled and may be exploited by unauthorized users to bypass existing controls to gain access to sensitive data,

programs, or password files. Should this happen, managers will have an incomplete understanding of the risks associated with their systems and, therefore, may make erroneous risk management decisions.

Connecting to the Internet presents a multitude of vulnerabilities for an entity due to the Internet's potential access to billions of people worldwide. Some Internet users are motivated to try to penetrate connected systems and have sophisticated software tools as aids, such as to repeatedly attempt access using different passwords. A variety of specialized software and hardware is available to limit access by outside systems or individuals through telecommunications networks. Examples of network components that can be used to limit access include secure gateways (firewalls) that restrict access between networks (an important tool to help reduce the risk associated with the Internet); teleprocessing monitors, which are programs incorporated into the computer's operating system that can be designed to limit access; and communications port protection devices, such as a security modem that requires a password from a dial-in terminal before establishing a network connection. Also available is the smart card, a device about the size of a credit card that contains a microprocessor, which can be used to control remote access to a computer with authenticating information generated by the microprocessor and communicated to the computer. Encryption is often used to protect the confidentiality of remote access sessions and is extremely important to protecting wireless access to information systems.

Information systems may identify and authenticate specific devices before establishing a connection. Device authentication typically uses either shared known information (for example, media access control or transmission control program/Internet protocol addresses) or an organizational authentication solution to identify and authenticate devices on local and wide area networks. Thus, it is important for the auditor to identify the controls over devices that provide this type of protection.

Emerging threats from the Internet (for example, spam and spyware) require new and updated protection mechanisms. The entity should employ spam and spyware protection mechanisms at

critical information system entry points (for example, firewalls, electronic mail servers, remote access servers) and at workstations, servers, or mobile computing devices on the network. Consideration should be given to using spam and software protection products from multiple vendors (for example, using one vendor for boundary devices and another vendor for workstations) to provide additional layers of defense. It is also important to centrally manage spam and software protection mechanisms and to have the system automatically update these mechanisms.

Depending on how access control techniques and devices are implemented, they can be used to

- verify terminal identifications to restrict access through specific terminals,
- verify IDs and passwords for access to specific applications,
- control access between telecommunications systems and terminals,
- restrict an application's use of network facilities,
- automatically disconnect at the end of a session,
- provide network activity logs that can be used to monitor network use and configuration,
- allow authorized users to shut down network components,
- monitor dial-in access to the system by monitoring the source of calls or by disconnecting and then dialing back users at preauthorized phone numbers,
- restrict in-house access to communications software,
- control changes to communications software, and
- restrict and monitor access to telecommunications hardware or facilities.

As with other access controls, to be effective remote access controls should be properly implemented in accordance with authorizations that have been granted. In addition, tables or lists used to define security limitations should be protected from unauthorized modification, and in-house access to communications security software should likewise be protected from unauthorized access

and modification. Dial-in phone numbers should not be published, and should be changed periodically.

An understanding of the system and network configurations and the control techniques that have been implemented is necessary to assess the risks associated with external access through telecommunications networks and the effectiveness of related controls. This is likely to require assistance from an auditor with special expertise in communications-related controls.

Connectivity should only be approved when appropriate to perform assigned official duties. Significant threats are posed by portable and mobile devices and personally owned information systems. Portable and mobile devices (for example, notebook computers, workstations, personal digital assistants) should not be allowed access to entity networks without first complying with security policies and procedures. Security policies and procedures might include activities such as scanning the devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (for example, wireless). Security controls include

- usage restrictions and implementation guidance,
- authorization by appropriate organizational officials, and
- documentation and monitoring of device access to entity networks.

The entity should also establish strict terms and conditions for the use of personally-owned information systems. The terms and conditions should address, at a minimum: (1) the types of applications that can be accessed from personally-owned information systems; (2) the maximum FIPS 199 security category of information that can be processed, stored, and transmitted; (3) how other users of the personally-owned information system will be prevented from accessing federal information; (4) the use of virtual private networking and firewall technologies; (5) the use of and protection against the vulnerabilities of wireless technologies;

(6) the maintenance of adequate physical security controls; (7) the use of virus and spyware protection software; and (8) how often the security capabilities of installed software are to be updated (for example, operating system and other software security patches, virus definitions, firewall version updates, spyware definitions). For guidance on protection of remote information refer to OMB M-06-16[75].

AC-1.2. Appropriately control network sessions

It is desirable that information systems prevent further access to the system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures. Users should be able to directly initiate session-lock mechanisms. The information system may also activate session-lock mechanisms automatically after a specified period of inactivity defined by the entity. A session lock is not, however, a substitute for logging out of the information system. When connectivity is not continual, network connections should automatically disconnect at the end of a session. OMB Memorandum M-06-16 requires that all federal agencies use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity.

In addition to technical controls, the initial screen viewed by an individual accessing an entity's systems through a telecommunications network should provide a warning banner to discourage unauthorized users from attempting access, and make it clear that unauthorized browsing will not be tolerated. For example, an opening warning screen should state that the system is for authorized users only and that activity will be monitored. The information system should also display the entity's privacy policy before granting access. Also, the warning screen generally should refer to 18 U.S.C. 1030, which provides criminal penalties for intentional unauthorized access. Previous logon notification is another control that can identify unauthorized access. The

[75]OMB, *Protection of Sensitive Agency Information* (Washington, DC.: June 23, 2006).

information system notifies the user on successful logon, of the date and time of the last logon, the location of the last logon, and the number of unsuccessful logon attempts since the last successful logon.

AC-1 Related NIST SP 800-53 Controls
AC-4 Information Flow Enforcement
AC-8 System use Notification
AC-9 Previous Logon Notification
AC-11 Session Lock
AC-12 Session Termination
AC-17 Remote Access
AC-18 Wireless Access Restrictions
AC-19 Access Control for Portable and Mobile Devices
CA-3 Information System Connections
SC-7 Boundary Protection
SC-10 Network Disconnect

Control Techniques and Suggested Audit Procedures for Critical Element AC-1

Table 16. Control Techniques and Suggested Audit Procedures for Critical Element AC-1: Adequately protect information system boundaries

Control activities	Control techniques	Audit procedures
AC-1.1. Appropriately control connectivity to system resources.	AC-1.1.1. Connectivity, including access paths and control technologies between systems and to internal system resources, is documented, approved by appropriate entity management, and consistent with risk.	Review access paths in network schematics, interface agreements, systems documentation, and in consultation with IT management and security personnel identify control points; determine whether the access paths and related system documentation is up-to-date, properly approved by management, and consistent with risk assessments.
	AC-1.1.2. Networks are appropriately configured to adequately protect access paths within and between systems, using appropriate technological controls (e.g. routers, firewalls, etc.)	Interview the network administrator; determine how the flow of information is controlled and how access paths are protected. Identify key devices, configuration settings, and how they work together. (This step is performed as a basis for the steps below).

Control activities	Control techniques	Audit procedures
		Perform security testing by attempting to access and browse computer resources including critical files, security software, and the operating system. These tests may be performed as (1) an “outsider” with no information about the entity’s computer systems, (2) an “outsider” with prior knowledge about the systems—for example, an ex-insider, and (3) an “insider” with and without specific information about the entity’s computer systems and with access to the entity’s facilities. Note: Due to the highly technical nature of such testing, it should be performed by persons possessing the necessary technical skills (e.g., an IT specialist). See Appendix V for additional information on the Knowledge, Skills, and Abilities needed to perform IS control audits. Also, see SM-5 for additional information on performing vulnerability assessments.
		When performing insider tests, use an ID with no special privileges to attempt to gain access to computer resources beyond those available to the account. Also, try to access the entity’s computer resources using default/generic IDs with easily guessed passwords. See NIST SP 800-42 for more details.
		When performing outsider tests, test the controls over external access to computer resources, including networks, dial-up, wireless, local area network, wide area network, and the Internet. See NIST SP 800-42 for more details.
	AC-1.1.3. The information system identifies and authenticates specific network devices before establishing a connection.	Determine whether authentication methods used are appropriate based on risk in accordance with FIPS Pub 200 and NIST SP 800-53.
	AC-1.1.4. Remote dial-up access is appropriately controlled and protected.	Interview network administrator and users; determine how remote dial-up access is controlled and protected (for example, monitor the source of calls and dial back mechanism); identify all dial-up lines through automatic dialer software routines and compare with known dial-up access; discuss discrepancies with management.

Control activities	Control techniques	Audit procedures
	AC-1.1.5. Remote Internet access is appropriately controlled and protected.	Interview network administrator and users; determine how connectivity is controlled and protected. Determine if federal agency policies, procedures, and practices comply with NIST SP 800-63 guidance on remote electronic authentication. Also, refer to OMB Memorandum 04-04 E-Authentication Guidance for Federal Agencies.
	AC-1.1.6. Remote wireless access is appropriately controlled and protected.	Interview network administrator and users; determine how connectivity is controlled and protected. Refer to NIST SP 800-97 *Establishing Wireless Robust Security Networks: A guide to IEEE.802.11i* for additional security assessment guidance. Test and validate entity controls: (1) use a wireless sniffer to capture data (for example, service set IDs (SSID), (2) if an SSID is obtained, associate the SSID to the access point, (3) identify what network resources are available, (4) determine if a security protocol[76] is implemented, and (5) if a security protocol is used, employ a program to test the strength of the encryption algorithm. Test and validate entity controls to identify rogue wireless access points. Test for rogue wireless access points. (See Section 2.2.2 “Appropriateness of Control Testing” for discussion of performance issues relating to this type of testing).
	AC-1.1.7. Connectivity is approved only when appropriate to perform assigned official duties. This includes portable and mobile devices, and personally-owned information systems. Appropriate safeguards are established to detect viruses, provide for timely patch management, and other security measures are in place to validate appropriate access for users working remotely (e.g., home)	Interview network administrator and users; review justifications for a selection of connections. Determine if these systems use appropriate safeguards such as automatic updates for virus protection and up-to-date patch protection, etc.
AC-1.2. Appropriately control network sessions.	AC-1.2.1. The information system prevents further access to the system by initiating a session lock, after a specified period of inactivity that remains in effect until the user reestablishes access using identification and authentication procedures.	Observe whether the system automatically initiates a session lock during a period of inactivity, and how the user can directly initiate a session lock, and then unlock the session (See OMB M-06-16)

[76] The optional cryptographic confidentiality algorithm specified by IEEE 802.11 used to provide data confidentiality that is subjectively equivalent to the confidentiality of a wired local area network (LAN) medium that does not employ cryptographic techniques to enhance confidentiality

Control activities	Control techniques	Audit procedures
	AC-1.2.2 Where connectivity is not continual, network connection automatically disconnects at the end of a session.	Interview network administrator and users; observe whether the control is implemented.
	AC-1.2.3. Appropriate warning banners are displayed before logging onto a system • system use notification (for example, U. S. Government system, consent to monitoring, penalties for unauthorized use, privacy notices) • previous logon notification (for example, date and time of last logon and unsuccessful logons).	Interview network administrator and users; observe whether the control is fully implemented and complies with NIST guidance.

Source: GAO.

Critical Element AC-2. Implement effective identification and authentication mechanisms

Users (or processes on behalf of users), and devices should be appropriately identified and authenticated through the implementation of adequate logical access controls. User authentication establishes the validity of a user's claimed identity, typically during access to a system or application (for example, login). Users can be authenticated using mechanisms such as requiring them to provide something they have (such as a smart card); something they alone know (such as a password or personal identification number); or something that physically identifies them uniquely (such as a biometric fingerprint or retina scan). Logical controls should be designed to restrict legitimate users to the specific systems, programs, and files that they need, and prevent others, such as hackers, from entering the system at all.

At the entitywide level, information systems accounts need to be managed to effectively control user accounts and identify and authenticate users. Account management includes the identification of account types (i.e., individual, group, system), establishment of conditions for group membership, and assignment of associated authorizations. Resource owners should identify authorized users of the information system and specify access rights. Access to the information system should be granted based on a valid need to know that is determined by assigned official duties and should also consider proper segregation of duties. The entity should require proper identification for requests to establish information system accounts and approve all such requests. The entity should also

specifically authorize and monitor the use of guest/anonymous accounts and remove, disable, or otherwise secure unnecessary accounts. Finally, the entity should ensure that account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured.

AC-2.1. Users are appropriately identified and authenticated

Identification and authentication is unique to each user (or processes acting on behalf of users). Account policies (for example, password policies, account lock out policies) should be formally established and enforced based on risk. Passwords, tokens, or other devices are used to identify and authenticate users. Identification is the process of distinguishing one user from all others, usually through user IDs. These are important because they are the means by which specific access privileges are assigned and recognized by the computer. However, the confidentiality of user IDs is typically not protected. For this reason, other means of authenticating users—that is, determining whether individuals are who they say they are—are typically implemented (for example, passwords, security tokens, etc.). In addition, the information system should limit the number of concurrent sessions for any user. NIST SP 800-63 provides additional guidance on authentication.[77]

An entity may allow limited user activity without identification and authentication for publicly available information systems and Web sites. However, for actions without identification and authentication, management should consider the risk and only allow such actions to the extent necessary to accomplish mission objectives.

The most widely used means of authentication is through the use of passwords. However, passwords are not conclusive identifiers of specific individuals since they may be guessed, copied, overheard,

[77]NIST, *Electronic Authentication Guidance* (Washington, DC: April 2006).

or recorded and played back. Typical controls for protecting the confidentiality of passwords include the following:

- Individual users are uniquely identified rather than having users within a group share the same ID or password; generic user IDs and passwords should not be used.
- Passwords are not the same as user IDs.
- Password selection is controlled by the assigned user and not subject to disclosure.
- Passwords are changed periodically, about every 30 to 90 days. The more sensitive the data or the function, the more frequently passwords should be changed.
- Passwords are not displayed when they are entered.
- Passwords contain alphanumeric and special characters and do not use names or words that can be easily guessed or identified using a password-cracking mechanism.
- A minimum character length, at least 8 characters, is set for passwords so that they cannot be easily guessed.
- Use of old passwords (for example, within six generations) is prohibited.
- Vendor-supplied passwords such as SYSTEM, DEFAULT, USER, DEMO, and TEST, are replaced immediately on implementation of a new system.

To help ensure that passwords cannot be guessed, attempts to logon to the system with invalid passwords should be limited. Typically, potential users are allowed 3 to 7 attempts to log on. This, in conjunction with the use of pass phrases or other complex passwords, reduces the risk that an unauthorized user could gain access to a system by using a computer to try thousands of words or names until they found a password that provided access. NIST SP 800-63 provides guidance on password selection and content.

Another technique for reducing the risk of password disclosure is encrypting the password file. Encryption may be used to transform passwords into a form readable only by using the appropriate key, held only by authorized parties. Access to this file should be restricted to only a few people; encryption further reduces the risk

that passwords could be accessed and read by unauthorized individuals. Passwords transmitted on the network may likewise be encrypted to prevent disclosure. Cryptographic controls and related audit procedures are covered in section AC-4.3.

In addition to passwords, identification devices such as ID cards, access cards, tokens, and keys may be used. Factors affecting the effectiveness of such devices include (1) the frequency that possession by authorized users is checked and (2) users' understanding that they should not allow others to use their identification devices and should report the loss of such devices immediately. Procedures should also be implemented to handle lost or compromised passwords, access cards, or tokens. OMB Memorandum M-06-16 requires that federal agencies allow remote access to personally identifiable information and other sensitive information only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access. Also see AC-4.2.

A less common means of authentication is based on biometrics, an automated method of verifying or recognizing the identity of a person based on physiological or behavioral characteristics. Biometrics devices include fingerprints, retina patterns, hand geometry, speech patterns, and keystroke dynamics. Tests of biometric techniques include reviewing the devices, observing the operations, and taking whatever other steps may be necessary to evaluate their effectiveness, including obtaining the assistance of a specialist.

To further increase security, identification and authentication may be accomplished using any combination of multiple mechanisms such as a token ID in conjunction with a number, or a biometric reader in conjunction with a password (also known as multifactor identification). Management should implement effective procedures to determine compliance with authentication policies. Whatever technique is used, the implementation cost versus the risk and potential loss to the entity's operations from a breach in security should be taken into consideration.

Electronic signatures such as digital signatures and public key infrastructure (PKI) are used to identify the sender of information and ensure the integrity of critical information received from the sender. Several technologies such as personal identification numbers, smart cards, biometrics, or digital signatures (an encrypted set of bits that identify the user) can be used to create electronic signatures. The most common electronic signature in use today is the digital signature, which is unique to each individual and to each message. Digital signatures are used in conjunction with certificate authorities and other PKI encryption hardware, software, policies, and people to verify that the individuals on each end of a communication are who they claim to be and to authenticate that nothing in the message has been changed. A digital certificate or shared secret may also be used to authenticate the identity of a device or devices involved in system communications, as opposed to the users. Also, see NIST SP 800-32[78], OMB Memorandum M-04-04[79], and the Federal Bridge Certification Authority for further information.

In addition, appropriate session-level identification and authentication controls should be implemented, such as those related to name/address resolution service and the authenticity of communication sessions.

In accordance with OMB policy, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. OMB Memorandum 04-04 requires agencies to conduct e-authentication risk assessments of e-government systems. These assessments will measure the relative severity of the potential harm and likelihood of occurrence of a wide range of impacts associated with the e-government system in the event of a compromise in identity authentication.

[78]NIST, *Introduction to Public Key Technology and the Federal PKI Infrastructure* (Washington, DC.: February 2001).

[79]OMB, *E-Authentication Guidance* (Washington, DC.: December 16, 2003).

AC-2 Related NIST SP 800-53 Controls	
AC-7	Unsuccessful Login Attempts
AC-10	Concurrent Session Control
AC-14	Permitted Actions Without Identification or Authentication
AU-10	Non-Repudiation
IA-2	User Identification and Authentication
IA-3	Device Identification and Authentication
IA-4	Identifier Management
IA-5	Authenticator Management
IA-6	Authenticator Feedback
SC-17	Public Key Infrastructure Certificates
SC-20	Secure Name/Address Resolution Service (Authoritative Source)
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)
SC-22	Architecture and Provisioning for Names/Address Resolution Service
SC-23	Session Authenticity

Control Techniques and Suggested Audit Procedures for Critical Element AC-2

Table 17. Control Techniques and Suggested Audit Procedures for Critical Element AC-2: Implement effective identification and authentication mechanisms

Control activities	Control techniques	Audit procedures
AC-2.1. Users are appropriately identified and authenticated.	AC-2.1.1. Identification and authentication is unique to each user (or processes acting on behalf of users), except in specially approved instances (for example, public Web sites or other publicly available information systems).	Review pertinent policies and procedures and NIST guidance pertaining to the authentication of user identities; interview users; review security software authentication parameters.
	AC-2.1.2. Account policies (including authentication policies and lockout policies) are appropriate given the risk, and enforced.	Review account policies and determine if they are based on risk and seem reasonable, based on interviews with system administrator and users. Determine how they are enforced, and test selected policies.
	AC-2.1.3. Effective procedures are implemented to determine compliance with identification and authentication policies.	Review adequacy of procedures for monitoring compliance with specific identification and authentication policies; selectively test compliance with key identification and authentication policies.

Control activities	Control techniques	Audit procedures
	AC-2.1.4. Selection of authentication methods (for example, passwords, tokens, biometrics, key cards, PKI certificates, or a combination therein) are appropriate, based on risk.	Determine whether authentication methods used are appropriate, based on system risk levels determined by the entity using NIST FIPS 199. See NIST SP 800-53 authentication controls as specified for entity designated system risk levels.
	AC-2.1.5. Authenticators: • are adequately controlled by the assigned user and not subject to disclosure; and • cannot be easily guessed or duplicated. Additional considerations for passwords are described below.	Review pertinent entity policies and procedures; assess procedures for generating and communicating authenticators to users; interview users; review related security software parameters. Observe users using authenticators; attempt to logon without a valid authenticator. Assess compliance with NIST guidance on authenticator selection, content, and usage.
	AC-2.1.6. Password-based authenticators: • are not displayed when entered; • are changed periodically (e.g., every 30 to 90 days); • contain alphanumeric and special characters; • are sufficiently long (e.g., at least 8 characters in length); • have an appropriate life (automatically expire); • are prohibited from reuse for a specified period of time (e.g., at least 6 generations); and • are not the same as the user ID.	Review pertinent entity policies and procedures; assess procedures for generating and communicating passwords to users; interview users; review security software password parameters. Observe users keying in passwords; attempt to logon without a valid password; make repeated attempts to guess passwords. (See Section 2.2.2 “Appropriateness of Control Testing” for discussion of performance issues relating to this type of testing). Assess entity compliance with NIST SP 800-63, which provides guidance on password selection and content.
	AC-2.1.7. Attempts to log on with invalid passwords are limited (e.g., 3–7 attempts).	Examine security parameters for failed log-on attempts; review security logs to determine whether attempts to gain access are logged and reviewed by entity security personnel; if appropriate, repeatedly attempt to logon using invalid passwords.
	AC-2.1.8. Use of easily guessed passwords (such as names or words) are prohibited.	As appropriate, review a system-generated list of current passwords; search password file using audit software to identify use of easily guessed passwords. Review management’s controls to prevent or detect easily guessed passwords.
	AC-2.1.9. Generic user IDs and passwords are not used.	Interview users and security managers; review a list of IDs and passwords to identify generic IDs and passwords in use.
	AC-2.1.10. Vendor-supplied default passwords are replaced during installation.	Attempt to log on using common vendor-supplied passwords; search password file using audit software. (See Section 2.2.2 “Appropriateness of Control Testing” for discussion of performance issues relating to this type of testing).

Control activities	Control techniques	Audit procedures
	AC-2.1.11. Passwords embedded in programs are prohibited. (Note: An embedded password is a password that is included into the source code of an application or utility. Applications often need to communication with other applications and systems and this requires an "authentication" process which is sometimes accomplished through the use of embedded passwords).	Discuss with entity security management how it obtains reasonable assurance that there are no embedded passwords used. If used, determine whether procedures have been established to monitor their use. Review selected programs for embedded passwords.
	AC-2.1.12. Use of and access to authenticators is controlled (e.g., their use is not shared with other users).	Review procedures to ensure that accounts are not shared. Select accounts to determine compliance with procedures.
	AC-2.1.13. Effective procedures are implemented to handle lost, compromised, or damaged authenticators (e.g., tokens, PKI certificates, biometrics, passwords, and key cards).	Identify procedures for handling lost or compromised authenticators; interview users and selectively test compliance with procedures.
	AC-2.1.14. Concurrent sessions are appropriately controlled.	Review procedures for controlling and auditing concurrent logons from different workstations. See NIST SP 800-53.
	AC-2.1.15. Where appropriate, digital signatures, PKI, and electronic signatures are effectively implemented.	Determine how nonrepudiation is assured and if PKI and electronic/digital signatures are effectively implemented.
	AC-2.1.16. PKI-based authentication • validates certificates by constructing a certification path to an accepted trust anchor; • establishes user control of the corresponding private key; and • maps the authenticated identity to the user account.	Review pertinent entity policies and procedures; assess procedures for generating and communicating certificates to users; interview users; review security software certificate parameters; obtain the help of experts if needed.
	AC-2.1.17. Authentication information is obscured (e.g., password is not displayed)	Review procedures for controlling the display of authentication information.
	AC-2.1.18. Appropriate session-level controls are implemented (e.g., name/address resolution service, session authenticity)	Assess the adequacy of session-level controls to include name/address resolution service, session authenticity, protection of session level information held in temporary storage, and controls to ensure that one session ends before the next session begins (prevent overlapping sessions).

Source: GAO.

Critical Element AC-3. Implement effective authorization controls

Once a user is authenticated, authorization[80] is used to allow or prevent actions by that user based on predefined rules. Authorization includes the principles of legitimate use, least privilege, and separation of duties (discussed in section 3.4).

[80] Access privileges granted to a user, program, or process.

Operating systems have some built-in authorization features such as user rights and privileges, groups of users, and permissions for files and folders. Network devices, such as routers, may have access control lists that can be used to authorize users who can access and perform certain actions on the device. Access rights and privileges are used to implement security policies that determine what a user can do after being allowed into the system.

Access rights, also known as permissions, allow the user to look, read, or write to a certain file or directory. Privileges are a set of access rights permitted by the access control system. In a Microsoft Windows™ system, rights are what give the user or members of a group the access needed to perform management tasks or simply to access a system. Information system access permissions are a Unix term that describe the kind of access to files a user is granted. A set of permissions is associated with every file and directory that determines who can read it, write to it, or execute it. Only the owner of the file (or the super user[81]) can change these permissions. Maintaining access rights, permissions, and privileges is one of the most important aspects of administering system security.

AC-3.1. User accounts are appropriately controlled

In order to adequately control user accounts, an entity should institute policies and procedures for authorizing logical access to information resources and document such authorizations. These policies and procedures should cover user access needed for routine operations, emergency access, and the sharing and disposition of data with individuals or groups outside the entity. Further, logical access controls should enforce segregation of duties.

The computer resource owner should identify the specific user or class of users authorized to obtain direct access to each resource for which they are responsible. Access should be limited to individuals with a valid business purpose (least privilege). Unnecessary accounts (default, guest accounts) should be removed, disabled, or

[81]The term “super user” denotes the highest level of user privilege and can allow unlimited access to a system's file and set up.

otherwise secured. This process can be simplified by developing standard profiles, which describe access needs for groups of users with similar duties, such as accounts payable clerks.

The owner should also identify the nature and extent of access to each resource that is available to each user. This is referred to as the user's profile. In general, users may be assigned one or more of the following types of access to specific computer resources:

- read access—the ability to look at and copy data or a software program
- update access—the ability to change data or a software program
- delete access—the ability to erase or remove data or programs
- merge access—the ability to combine data from two separate sources
- execute access—the ability to execute a software program

Access may be permitted at the file, record, or field level. Files are composed of records, typically one for each item or transaction. Individual records are composed of fields that contain specific data elements relating to each record.

Owners should periodically review access authorization listings and determine whether they remain appropriate. Access authorizations should be documented on standard forms and maintained on file. Listings of authorized users and their specific access needs and any modifications should be approved by an appropriate senior manager and directly communicated in writing by the resource owner to the security management function. A formal process for transmitting these authorizations, including the use of standardized access request forms, should be established to reduce the risk of mishandling, alterations, and misunderstandings.

Security managers should review access authorizations for new or modified access privileges and discuss any questionable authorizations with the resource owners (authorizing officials).

Approved authorizations should be maintained on file. Compliance with access authorizations should be monitored by periodically

comparing authorizations to actual access activity. Access control software typically provides a means of reporting user access authorizations and access activity. All changes to security access authorizations should be automatically logged and periodically reviewed by management independent of the security function. Unusual activity should then be investigated.

Broad or special access privileges, such as those associated with operating system software that allow normal controls to be overridden, are only appropriate for a small number of users who perform system maintenance or manage emergency situations. Such special privileges may be granted on a permanent or temporary basis. However, any such access should also be approved by a senior security manager, written justifications should be kept on file, and the use of highly sensitive files or access privileges should be routinely reviewed by management. Special access privileges, access to sensitive files, and related audit procedures are covered in section AC-4.1.

For systems that can be accessed through public telecommunications lines, some users may be granted dial-up access. This means that these individuals can use a modem to access and use the system from a remote location, such as their home or a field office. Because such access can significantly increase the risk of unauthorized access, it should be limited and the associated risks weighed against the benefits. To help manage the risk of dial-up access, justification for such access should be documented and approved by owners. (See section AC-1 for controls to help manage the risks of dial-up access, such as dial-back procedures to preauthorized phone numbers or the use of security modems, tokens, or smart cards to authenticate a valid user.)

Inactive accounts and accounts for terminated individuals should be disabled or removed in a timely manner. It is important to notify the security function immediately when an employee is terminated or, for some other reason, is no longer authorized access to information resources.

Notification may be provided by the human resources department or by others, but policies should exist that clearly assign responsibility for such notification. Terminated employees who continue to have access to critical or sensitive resources pose a major threat, as do individuals who may have left under acrimonious circumstances.

Owners should determine disposition and sharing of data. A mechanism should be established so that the owners of data files and programs determine whether and when these resources are to be maintained, archived, or deleted. Standard disposition forms can be used and maintained on file to document the users' approvals. In addition, resource owners should determine if, with whom, and by what means information resources can be shared. When files are shared with other entities, it is important that (1) data owners understand the related risks and approve such sharing and (2) receiving entities understand the sensitivity of the data involved and safeguard the data accordingly. This should require a written agreement before sensitive information is shared.

Required access to shared file systems should be restricted to the extent possible (for example, only to particular hosts, and only for the level of access required). Many scientific agencies, use file sharing networks. File sharing facilitates connections between persons who are looking for certain types of files. A type of file sharing known as peer-to-peer (P2P) refers to any software or system allowing individual users of the Internet to connect directly to each other and trade files. While there are many appropriate uses of this technology, several studies show that the vast majority of files traded on P2P networks are copyrighted music files and pornography. Data also suggest that P2P is a common avenue for the spread of computer viruses within IT systems. As required by FISMA, agencies are to use NIST standards and guidance to complete system risk and impact assessments in developing security plans and authorizing systems for operation. Operational controls detailing procedures for handling and distributing information and management controls outlining rules of behavior for users should

ensure that proper controls are in place to prevent and detect improper file sharing.[82]

Emergency and temporary access authorization needs to be controlled. Occasionally, there will be a need to grant temporary access privileges to an individual who is not usually authorized access. Such a need may arise during emergency situations, when an individual is temporarily assigned duties that require access to critical or sensitive resources, or for service or maintenance personnel. In addition, contractor personnel may require temporary access while involved in systems development or other work. As with normal access authorizations, temporary access should be approved and documented and the related documentation maintained on file. Temporary user identifications and authentication devices, such as passwords, should be designed to automatically expire after a designated date. Also, management should periodically review emergency and temporary access accounts to determine that they are still necessary.

AC-3.2. Processes and services are adequately controlled

Only authorized processes and services should be permitted in information systems and they should be limited to what is essential to effectively perform an entity's mission and business functions. In an information system, processes are systematic sequences of operations to produce a specified result. This includes all functions performed within a computer such as editing, calculating, summarizing, categorizing, and updating. Services refer to "customer or product-related business functions" such as file transfer protocol (FTP), hypertext transfer protocol (HTTP), and mainframe supervisor calls. Each system provides a set of services. For example, a computer network allows its users to send packets to specified destinations; a database system responds to queries; and a processor performs a number of different instructions. Controls related to processes and services include all of the technological and managerial safeguards established and applied to

[82]OMB Memorandum M-04-26, *Personal Use Policies and "File Sharing" Technology*, (Washington, D.C.: September 8, 2004).

an information system to protect hardware, software, and data from accidental or malicious modification, destruction, or disclosure.

When evaluating an entity's processes and services, it is important to consider the following:

- available processes and services should be minimized,
- the functions and purposes of processes and services should be documented and approved by management, and
- information available to unauthorized users should be restricted.

Proper control of information system processes and services is critical to ensuring the confidentiality, integrity, and availability of user data and, ultimately, the accomplishment of an entity's mission. Access control policies and enforcement mechanisms are employed by entities to control access between users (or processes acting on behalf of users) and objects (for example, segments, devices, files, records, fields, processes, programs) in the information system. Access control policies can be identity-based, role-based, or rule-based.[83] Associated enforcement mechanisms include access control lists, access control matrices, and cryptography. Where encryption of stored information is used as an access enforcement mechanism, the cryptography used should be in compliance with applicable standards.

Configuring systems only for necessary capabilities minimizes processes and services. First, only required services should be installed. Second, the number of individuals with access to such services should be restricted based on the concept of least privilege; this means that users should have the least amount of privileges (access to services) necessary to perform their duties. Third, the use of information services needs to be monitored. Fourth, it is important to maintain current service versions. According to NIST guidance, the information system should be periodically reviewed to identify and eliminate unnecessary services (for example, FTP,

[83]Identity-based access is based on the identities of users and information system resources. Role-based access is based on users' roles/responsibilities. Rule-based access is based on user or resource attributes and a predetermined rule set.

HTTP, mainframe supervisor calls) and protocols that would introduce an unacceptable level of risk should be disabled.[84] The information system that supports the server functionality should be, as much as possible, dedicated to that purpose. In addition, the function and purpose of processes and services should be documented and approved by appropriate entity officials.

According to NIST SP 800-53, additional process and service controls should be implemented to

- prohibit remote activation of collaborative computing mechanisms (e.g. video and audio devices),
- ensure that lower priority process do not interfere with higher priority processes, and
- ensure proprietary information and applications is protected from processes and systems available to the public.

AC-3 Related NIST SP 800-53 Controls	
AC-2	Account Management
AC-3	Access Enforcement
AC-6	Least Privilege
CM-7	Least Functionality
SC-6	Resource Priority
SC-14	Public Access Protections
SC-15	Collaborative Computing

[84]See NIST Special Publications (SP) 800-10 and 800-41 for information on configuring firewalls and filtering common protocols to minimize vulnerabilities from Internet services. SP 800-10, from 1994, contains basic information that is still applicable, but SP 800-41 updates the earlier document and covers Internet protocol packet filtering and more recent policy recommendations.

Control Techniques and Suggested Audit Procedures for Critical Element AC-3

Table 18. Control Techniques and Suggested Audit Procedures for Critical Element AC-3: Implement effective authorization controls

Control activities	Control techniques	Audit procedures
AC-3.1. User accounts are appropriately controlled.	AC-3.1.1. Resource owners have identified authorized users and the access they are authorized to have.	These audit procedures should be coordinated with section 3.4 (segregation of duties) to ensure that users do not have access to incompatible functions. Review written policies and procedures; for a selection of users (both application and information security personnel), review access authorization documentation and applicable rights and privileges in the information system.
	AC-3.1.2. Security administration personnel set parameters of security software to provide access as authorized and restrict access that has not been authorized. This includes access to data files, load and source code libraries (if applicable), security files, and operating system files. Standard naming conventions are established and used effectively as a basis for controlling access to data, and programs. (Standard naming conventions are essential to ensure effective configuration management identification and control of production files and programs vs. test files and programs)	Determine directory names for sensitive or critical files and obtain security reports of related access rules. Using these reports, determine who has access to sensitive files and whether the access matches the level and type of access authorized. Determine whether standard naming conventions are established and used effectively.
	AC-3.1.3. Security managers review access authorizations and discuss any questionable authorizations with resource owners.	Interview security managers and review documentation provided to them to determine whether they review access authorizations to include follow-ups with resource owners on questionable authorizations
	AC-3.1.4. All changes to security access authorizations are automatically logged and periodically reviewed by management independent of the security function; unusual activity is investigated.	Review a selection of recent changes to security access authorizations and related logs for evidence of management review and unusual activity; determine if unusual activity is being/has been investigated.
	AC-3.1.5. Resource owners periodically review access authorizations for continuing appropriateness.	Interview owners and review supporting documentation; determine whether they review access authorizations; determine whether inappropriate access rights are removed in a timely manner.
	AC-3.1.6. Access is limited to individuals with a valid business purpose (least privilege).	Identify who has access to user accounts and sensitive system resources and the business purpose for this access.
	AC-3.1.7. Unnecessary accounts (default, guest accounts) are removed, disabled, or otherwise secured.	Verify that unnecessary accounts are removed, disabled, or secured.

Control activities	Control techniques	Audit procedures
	AC-3.1.8. Inactive accounts and accounts for terminated individuals are disabled or removed in a timely manner.	Review security software parameters; review system-generated list of inactive logon IDs, and determine why access for these users has not been terminated. Obtain a list of recently terminated employees from Personnel and, for a selection, determine whether system access was promptly terminated.
	AC-3.1.9. Access to shared file systems are restricted to the extent possible (for example, only to particular hosts, and only for the level of access required).	Determine how access to shared file systems is restricted and verify that it works effectively.
	AC-3.1.10. Emergency or temporary access (e.g., firecall IDs) is appropriately controlled, including • documented and maintained, • approved by appropriate managers, • securely communicated to the security function, • automatically terminated after a predetermined period, and • all activity is logged.	Review pertinent policies and procedures for emergency/temporary access IDs, including firecall IDs; compare a selection of both expired and active temporary and emergency authorizations (obtained from authorizing parties) with a system-generated list of authorized users. Determine the appropriateness of access documentation and approvals and the timeliness of terminating access authorization when no longer needed. Review procedures for monitoring the use of emergency/temporary IDs (including firecall IDs) to ensure that access was used properly to correct a problem.
AC-3.2. Processes and services are adequately controlled.	AC-3.2.1. Available processes and services are minimized, such as through • installing only required processes and services based on least functionality, • restricting the number of individuals with access to such services based on least privilege, • monitoring the use of such services, and • maintaining current service versions. Note; Installed processes and services should be consistent with approved system baseline.	Review procedures for minimizing processes and services consistent with approved system baseline; interview system administrator; identify what services are installed and determine if they are required; determine who has access to these services and if they need them; determine how access to these services is monitored; and determine if the service versions are kept current. If appropriate, scan for poorly configured, unnecessary, and dangerous processes and services.
	AC-3.2.2. The function and purpose of processes and services are documented and approved by management.	Obtain documentation describing the function and purpose of processes and services, and evidence of management approval.
	AC-3.2.3. Information available to potential unauthorized users is appropriately restricted.	Determine if information about available processes and services is appropriately restricted.

Control activities	Control techniques	Audit procedures
	AC-3.2.4. The information system prohibits remote activation of collaborative computing mechanisms (for example, video and audio conferencing) and provides an explicit indication of use to the local users (for example, use of camera or microphone).	Determine if remote activation of collaborative computing services have been physically disconnected.
	AC-3.2.5. For publicly available systems, the information system controls protect the integrity and availability of the information and applications.	Identify controls used to protect the integrity and availability of the information and applications on such systems and test controls to ensure their effectiveness.

Source: GAO.

Critical Element AC-4. Adequately protect sensitive system resources

Certain system resources are more sensitive than others because, if compromised, serious security breaches could occur. Three areas related to sensitive system resources are: (1) restricting and monitoring access, (2) implementing adequate media controls over sensitive data, and (3) where appropriate, implementing effective cryptographic controls. Such sensitive system resources include system software, system utilities, configuration management systems, file maintenance systems, security software, data communications systems, and database management systems. Restricting access to sensitive system resources such as system software and related documentation is critical to controlling the overall integrity of information systems. For example, if system software is not adequately protected, an individual could gain access to capabilities that would allow him or her to bypass security features found in either operating system security software or access controls built into application software. The individual would then be able to read, modify, or destroy application programs, master data files, and transaction data, and subsequently erase any electronic audit trail of his or her activities. In addition, inadequate media controls can result in a loss of confidentiality of sensitive data. Further, cryptographic controls may be needed to protect sensitive information where it is not otherwise possible or practical to adequately restrict access through either physical or logical access controls.

AC-4.1. Access to sensitive system resources is restricted and monitored

Access to sensitive system resources, such as system software and powerful system utilities, should be appropriately restricted and monitored. System software is a set of programs designed to operate and control the processing activities of computer equipment. Generally, one set of system software is used to support and control a variety of applications that may run on the same computer hardware. System software helps control and coordinates the input, processing, output, and data storage associated with all of the applications that run on a system. Some system software can change data and program code on files without leaving an audit trail. The following are examples of system software:

- operating system software
- system utilities
- configuration management systems
- file maintenance software
- security software
- data communications systems
- database management systems

Access to sensitive system resources should be restricted to individuals or processes that have a legitimate need for this access for the purposes of accomplishing a valid business purpose. For example, access to system software should be restricted to a limited number of personnel who have job responsibilities associated with the use of that software. Responsibilities for using system utilities should be clearly defined and understood by systems programmers. Application programmers and computer operators should be specifically prohibited from accessing system software. Justification and approval by appropriate entity officials for access to system software should be documented and retained. Appropriate entity officials should periodically review the use of privileged system software and utilities to ensure that access permissions correspond with position descriptions and job duties. Further, the use of sensitive/privileged accounts should be adequately monitored. Responsibilities for monitoring use should be clearly defined and understood by entity officials.

Typically, access to operating system software is restricted to a few systems programmers whose job it is to modify the system, when needed, and intervene when the system will not operate properly. In addition, database administrators need access to the system's database management system and a designated senior-level security administrator needs access to security software. However, application programmers and computer operators should not have access to system software, as this would be incompatible with their assigned responsibilities and could allow unauthorized actions to occur. (See section 3.4 for details on segregation of duties.)

The number of personnel authorized to access the system will vary depending on the size and needs of the entity and, therefore, should be determined based on an analysis of the entity's operations. For example, a large entity that must maintain operations on a 24-hour basis will need more operating systems analysts and programmers than a smaller entity that operates on a less intensive schedule. There may be a tendency for entities to authorize access to many individuals so that emergency operating problems can be handled promptly. However, management should balance the need for efficiency with the need for security.

Because of the powerful capabilities at the disposal of those who have access to system software and related tools, use of the tools should be adequately controlled and monitored to identify any inappropriate or unusual behavior. Such behavior may indicate unauthorized access or an individual who is improperly exploiting access privileges. For example, greater than normal use of system software or use at odd hours may indicate that an individual is using the software to search for system weaknesses to exploit or to make unauthorized changes to system or application software or data. For monitoring to be effective in both detecting and deterring inappropriate use, personnel authorized to use system software should understand which uses are appropriate and which are not and also that their activities may be monitored. Such policies should be documented and distributed to all personnel.

Policies and techniques should be implemented for using and monitoring the use of system tools and utilities. Some system utilities are used to perform system maintenance routines that are

frequently required during normal processing operations. Other utilities aid the development and documentation of applications systems. These utilities can aid individuals who have fraudulent or malicious intentions in understanding how the programs or data in an application system operate and in how to make unauthorized modifications.

Following is a listing of some utilities with their intended functions that could be misused without proper monitoring and control:

- Flowcharters, transaction profile analyzers, execution path analyzers, and data dictionaries can be used to understand application systems.
- Data manipulation utilities, data comparison utilities, and query facilities can be used to access and view data, with manipulation utilities also allowing data modification.
- Online debugging facilities permit online changes to program object code leaving no audit trail and can activate programs at selected start points.
- Library copiers can copy source code from a library into a program, text and online editors permit modification of program source code, and online coding facilities permit programs to be coded and compiled in an interactive mode.

To prevent or detect the misuse of systems utilities, policies should be clearly documented regarding their use. In addition, the use of utilities should be monitored. Generally, system software contains a feature that provides for logging and reporting of its use. Such reports should identify when and by whom the software was used. It is important that this software operation work properly and that the reports are reviewed on a regular basis.

The availability of standard usage data may assist the systems manager in identifying unusual activity. Some systems can be designed to compare standard usage data with actual use and report significant variances, thus making it easier for the system manager to identify unusual activity. When questionable activity is identified, it should be investigated. If improper activity is determined to have occurred, in accordance with security violation policies, the

incident(s) should be documented, appropriate disciplinary action taken, and, when appropriate, higher-level management notified. Further, the possibility of damage or alteration to the system software, application software, and related data files should be investigated and corrective action taken if needed. Such action should include notifying the resource owner of the violation.

In addition to controlling access to sensitive system resources, it is also important to control a number of other activities. First, default permissions and rights to system software and network devices should be changed during installation. Second, system libraries should be appropriately controlled. For example, the migration of system software from the testing environment to the production environment may be performed, after approval, by an independent library control group. Outdated versions of system software should be removed from the production environment to preclude their use. Some changes may be made specifically to correct security or integrity vulnerabilities, and using outdated versions allows the entity's data and systems to remain exposed to these vulnerabilities. Third, access to authentication services and directories should also be appropriately controlled. Finally, access to mobile code[85] (see next paragraph) should be appropriately controlled due to its potential to cause damage to the information system if used maliciously.

Mobile code refers to programs (for example, script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics. Being able to download files and electronic documents off the Internet is a useful function and a common practice today. Web pages serve as an electronic counterpart to paper documents; however, unlike paper documents, Web pages can entail active content that is capable of delivering digitally encoded multimedia information enlivened through embedded computer instructions.

[85]Mobile code is a software program or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient. Examples of mobile code include scripts (JavaScript, VBScript), Java applets, Active X controls, and macros embedded within Office documents.

The popularity of the World Wide Web has spurred the trend toward active content. A dynamic weather map, a stock ticker, and live camera views or programmed broadcasts appearing on a Web page are common examples of the use of this technology. Like any technology, active content can provide a useful capability, but can also become a source of vulnerability for an attacker to exploit.

Mobile code controls should include registration, approval, and control procedures to prevent the development, acquisition, or introduction of unacceptable mobile code within the information system. All mobile code or executable content employed should be registered unless otherwise approved by the authorizing official. Uploading of mobile code or executable content from one organizational information system to another should also be similarly authorized.

Sensitive system resources may be further protected by partitioning applications, isolating security functions, and establishing a trusted communication path. First of all, through application partitioning, the information system physically or logically separates user interface services (for example, public Web pages) from information storage and management services (for example, database management). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate. Secondly, it is desirable for the information system to isolate security functions from nonsecurity functions by means of partitions, domains, etc., including control of access to and integrity of the hardware, software, and firmware that perform those security functions. The information system maintains a separate execution domain (for example, address space) for each executing process. Thirdly, the information system should establish a trusted communication path between the user and the security functionality of the system. Technical experts may be needed to examine and test these controls. Finally, as appropriate, controls should be in place over information leakage through electromagnetic signals emanations.

AC-4.2. Adequate media controls have been implemented

Media controls should be implemented to control unauthorized physical access to digital and printed media removed from the information system and during pick up, transport, and delivery to authorized users. Media should also be properly labeled to identify its sensitivity and distribution limitations. Finally, all sensitive information should be removed from media before its disposal or transfer to another use.

As discussed in NIST SP 800-53, information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). Media controls also apply to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones).

NIST SP 800-53 also states that an organizational assessment of risk guides the selection of media and associated information contained on that media requiring restricted access. Organizations document in policy and procedures, the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls where the media resides provide adequate protection.

One sensitive area is the storage of personally identifiable information on portable media. The ability to store and transport substantial volumes of data on portable devices creates an additional exposure to information confidentiality. The entity should have adequate controls in place over such portable media. OMB Memorandum M-06-16 recommends federal agencies encrypt all data on mobile computers/devices which carry agency data unless

the data is determined to be non-sensitive, in writing, by the agency's Deputy Secretary or an individual they may designate in writing.

In addition, as part of the risk assessment process, entities should identify information that is sensitive, including personally identifiable information. Entities should implement controls to adequately protect the confidentiality of such information, including any copies of such data. OMB Memorandum M-06-16 recommends federal agencies to log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required. This OMB Memorandum provides additional guidance on controls over personally identifiable and other sensitive information. Also see AC-1.2 and AC-2.1.

Automated marking and labeling of information helps to enforce information security access policy. Information system outputs should be marked using standard naming conventions to identify any special dissemination, handling, or distribution instructions. Similarly, information in storage, in process, and transmission should be appropriately labeled. Further, a means should be provided for the information system to ensure that the labels a user associates with information provided to the system are consistent with the information that the user is allowed to access. It is important that security parameters are exchanged between systems to authenticate services requested by another system. Security parameters include, for example, security labels and markings. Security parameters may be explicitly or implicitly associated with the information contained within the information system.

The entity should have policies and procedures in place to remove sensitive information[86] and software from computers, disks, and other equipment or media when they are disposed of or transferred to another use. Further, approved equipment and techniques should

[86]The process of removing sensitive information from computer media is often referred to as sanitization. It includes removing all labels, markings, and activity logs. NIST SP 800-36 provides guidance on appropriate sanitization equipment, techniques, and procedures.

be used and periodically tested to ensure correct performance. If sensitive information is not fully cleared, it may be recovered and inappropriately used or disclosed by individuals who have access to the discarded or transferred equipment and media. The responsibility for clearing information should be clearly assigned. Also, standard forms or a log should be used to document that all discarded or transferred items are examined for sensitive information and that this information is cleared before the items are released.

AC-4.3. Cryptographic controls are effectively used

Where appropriate, cryptographic tools help provide access control by rendering data unintelligible to unauthorized users and/or protecting the integrity of transmitted or stored data. In some cases—especially those involving telecommunications—it is not possible or practical to adequately restrict access through either physical or logical access controls. In these cases, cryptographic tools can be used to identify and authenticate users and help protect the integrity and confidentiality of data and computer programs, both while these data and programs are "in" the computer system and while they are being transmitted to another computer system or stored on removable media.

As discussed in FIPS Pub 140-2, cryptographic-based security systems may be utilized in various computer and telecommunication applications (e.g., data storage, access control and personal identification, network communications, radio, facsimile, and video) and in various environments (e.g., centralized computer facilities, office environments, and hostile environments). The cryptographic services (e.g., encryption, authentication, digital signature, and key management) provided by a cryptographic module are based on many factors that are specific to the application and environment. The security level to which a cryptographic module is validated should be chosen to provide a level of security appropriate for the security requirements of the application and environment in which the module will be utilized and the security services that the module will provide. The security requirements for a particular security level include both the security requirements specific to that level

and the security requirements that apply to all modules regardless of the level.

Cryptography involves the use of algorithms (mathematical formulae) and combinations of keys (strings of bits) to do any or all of the following:

- encrypt, or electronically scramble a message or file so that it is unintelligible to those who do not have the secret key needed to decrypt it, thus keeping the contents of the message or file confidential,
- provide an electronic signature that can be used to determine if any changes have been made to the related file, thus ensuring the file's integrity, and
- link a message or document to a specific individual's or group's key, thus ensuring that the "signer" of the file can be identified.

Cryptographic tools are especially valuable for any application that involves "paperless" transactions or for which the users want to avoid relying on paper documents to substantiate data integrity and validity. Examples include

- electronic commerce, where purchase orders, receiving reports, and invoices are created, approved, and transmitted electronically;
- travel administration, where travel orders and travel vouchers are created, approved, and transmitted electronically; and
- protection of documents or digital images, such as contracts, personnel records, or diagrams, which are stored on electronic media.

Cryptographic tools may be linked to an individual application or implemented so that they can be used to sign or encrypt data associated with multiple applications. For example, the personal computers connected to a local area network may each be fitted with hardware and/or software that identifies and authenticates users and allows them to encrypt, sign, and authenticate the messages and files that they send or receive, regardless of the application that they are using.

There are a number of technical issues to consider concerning cryptography. Some of the key considerations are listed here.

- Are the cryptographic tools implemented in software or through the use of a hardware module? (Hardware modules are generally more secure.)
- How is the data transmitted between the computer's memory and the cryptographic module, and is this path protected?
- How strong, or complex, is the algorithm used to encrypt and sign data?
- How are keys managed and distributed?
- Does the entity's use of cryptographic tools comply with related Federal Information Processing Standards issued by NIST?
- Has the entity chosen cryptographic techniques that are appropriate to cost-effectively meet its defined control objectives?

If the auditor encounters cryptographic tools and determines that their reliability is important to his or her understanding of the controls, they should obtain the most recent guidance available from OMB, NIST, and GAO, as well as technical assistance from an auditor experienced in assessing cryptographic tools.

AC-4 Related NIST SP 800-53 Controls	
AC-15	Automated Marking
AC-16	Automated Labeling
IA-7	Cryptographic Module Authentication
MP-2	Media Access
MP-3	Media Labeling
MP-4	Media Storage
MP-5	Media Transport
MP-6	Media Sanitization and Disposal
PE-19	Information Leakage
SC-2	Application Partitioning
SC-3	Security Function Isolation
SC-4	Information Remnance
SC-8	Transmission Integrity
SC-9	Transmission Confidentiality
SC-11	Trusted Path
SC-12	Cryptographic Key Establishment and Management

SC-13	Use of Cryptography
SC-16	Transmission of Security Parameters
SC-18	Mobile Code

Control Techniques and Suggested Audit Procedures for Critical Element AC-4

Table 19. Control Techniques and Suggested Audit Procedures for Critical Element AC-4: Adequately protect sensitive system resources

Control activities	Control techniques	Audit procedures
AC-4.1. Access to sensitive system resources is restricted and monitored.	AC-4.1.1. Access to sensitive/privileged accounts is restricted to individuals or processes having a legitimate need for the purposes of accomplishing a valid business purpose.	Review pertinent policies and procedures. Interview management and systems personnel regarding access restrictions. Identify and test who has access to sensitive/privileged accounts and determine the reason for that access.
	AC-4.1.2. Use of sensitive/privileged accounts is adequately monitored.	Determine if the use of sensitive and privileged accounts is monitored and evaluate the effectiveness of monitoring procedures.
	AC-4.1.3. Logical access to utilities and tools is adequately controlled (for example, remote maintenance).	Determine the last time the access capabilities of staff with special system access privileges (e.g., system programmers) were reviewed. Review security software settings to identify types of activity logged. Observe personnel accessing system software, such as sensitive utilities and note the controls encountered to gain access. Attempt to access the operating system and other system software. Select some application programmers and determine whether they are authorized access.
	AC-4.1.4. Files relied upon by operating systems are appropriately controlled.	Determine if access to files relied upon by operating systems are adequately controlled.
	AC-4.1.5. Passwords/authentication services and directories are appropriately controlled and encrypted when appropriate.	Determine if password files and authentication services are adequately protected from unauthorized access. Determine if password files are encrypted.
	AC-4.1.6. Mobile code is appropriately controlled.	Interview system administrator and perform appropriate procedures to determine if mobile code is adequately controlled.
	AC-4.1.7. Where appropriate, access is restricted based on time and/or location.	Determine if access is appropriately restricted based on time and/or location.

Control activities	Control techniques	Audit procedures
	AC-4.1.8. The information system partitions or separates user functionality (including user interface services) from information system management functionality.	Interview officials and review related system documentation. Coordinate with vulnerability analysis.
	AC-4.1.9. The information system isolates security functions from nonsecurity functions.	Interview officials and review related system documentation. Coordinate with vulnerability analysis.
	AC-4.1.10. The information system establishes a trusted communications path between the user and the security functionality of the system.	Interview officials with system and communication responsibilities and examine appropriate records such as developer design documents.
AC-4.2. Adequate media controls have been implemented.	AC-4.2.1. Only authorized users have access to printed and digital media removed from the information system.	Interview personnel and review procedures. Observe entity practices and review selected access logs.
	AC-4.2.2. The information system automatically identifies how information is to be used • output is marked using standard naming conventions, and • internal data in storage, process and transmission is labeled.	Interview appropriate personnel. For output, identify standard naming conventions and examine the system configuration. For internal data, examine the labeling mechanism and internal data for accurate labels. Test output and internal data for appropriate results.
	AC-4.2.3. The organization controls the pickup, transport, and delivery of information system media (paper and electronic) to authorized personnel.	Interview officials and review appropriate policy and procedures. Observe selected media transport practices and receipts.
	AC-4.2.4. Systems media is securely stored according to its sensitivity.	Determine if media storage practices are adequate and comply with applicable requirements (for federal agencies, FIPS 199 security categories).
	AC-4.2.5. Security parameters are clearly associated with information exchanged between information systems.	Determine if security parameters are clearly associated with information exchanged.
	AC-4.2.6. Approved equipment, techniques, and procedures are implemented to clear sensitive data from digital media before its disposal or release for reuse outside of the organization.	Review written procedures; interview personnel responsible for clearing data from digital media. For a selection of recently discarded or transferred items, examine documentation related to clearing of data and disposal of software. For selected items still in the entity's possession, test to determine whether they have been appropriately sanitized.
AC-4.3. Cryptographic controls are effectively used.	AC-4.3.1. Cryptographic tools have been implemented to protect the integrity and confidentiality of sensitive and critical data and software programs where appropriate.	Determine if cryptographic tools are properly implemented. (See NIST standards for federal agencies) To evaluate the use of cryptographic tools, the auditor should obtain the assistance of a specialist.
	AC-4.3.2. Encryption procedures are implemented in data communications where appropriate based on risk.	Capture passwords transmitted over the network and determine if they are encrypted; for federal system, determine if cryptographic authentication complies with FIPS 140-2. To evaluate cryptographic tools, the auditor should obtain the assistance of a specialist.

Control activities	Control techniques	Audit procedures
	AC-4.3.3. For authentication to a cryptographic module, the information system employs appropriate authentication methods.	Interview appropriate officials and review supporting documentation. For federal agencies, compare the authentication process to FIPS 140-2 requirements.
	AC-4.3.4. The information system employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management.	Compare policy and practices to appropriate guidance, such as NIST guidance in SP 800-56 and SP 800-57 for cryptographic key establishment and management, respectively.

Source: GAO.

Critical Element AC-5. Implement an effective audit and monitoring capability

Audit and monitoring involves the regular collection, review, and analysis of auditable events for indications of inappropriate or unusual activity, and the appropriate investigation and reporting of such activity. Automated mechanisms may be used to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities. Audit and monitoring controls can help security professionals routinely assess computer security, perform investigations during and after an attack, and even recognize an ongoing attack. Audit and monitoring technologies include network and host-based intrusion detection systems, audit logging, security event correlation tools, and computer forensics. Network-based intrusion detection systems (IDSs) capture or "sniff" and analyze network traffic in various parts of a network. On the other hand, host-based IDSs analyze activity on a particular computer or host. Both types of IDS have advantages and disadvantages.

FISMA requires that each federal agency implement an information security program that includes procedures for detecting, reporting, and responding to security incidents. Further, OMB is to ensure the operation of a central federal information security incident center to

- provide timely technical assistance to system operators,
- compile and analyze incident information,
- inform system operators about threats and vulnerabilities, and
- consult with NIST, national security agencies, and other designated agencies such as the Department of Homeland Security.

NIST issued two relevant special publications that provide additional information:

- SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, and
- SP 800-61, Computer Security Incident Handling Guide

SP 800-61 discusses four steps in incident handling:

- preparation,
- detection and analysis,
- containment, eradication, and recovery, and
- post-incident activity.

An IDS detects inappropriate, incorrect, or anomalous activity aimed at disrupting the confidentiality, integrity, or availability of a protected network and its computer systems. An IDS collects information on a network, analyzes the information on the basis of a preconfigured rule set, and then responds to the analysis. A description of the technologies, their effectiveness, and how they work is described in *Technologies to Secure Federal Systems*, GAO-04-467 (Washington, D.C.: March 2004).

AC-5.1. An effective incident response program is documented and approved

An effective incident response program should be implemented. Control techniques include

- documented policies and procedures, including an incident response plan;
- documented testing of the incident response plan;
- a means of prompt centralized reporting;
- active monitoring of alerts and advisories;
- response team members with the necessary knowledge, skills, and abilities;
- training on roles and responsibilities and periodic refresher training;
- links to other relevant groups;
- protection against denial of service attacks; and

- appropriate incident response assistance and consideration of computer forensics.

OMB tasks NIST with coordinating activities governmentwide for agencies sharing information concerning common vulnerabilities and threats. Finally, Appendix III of OMB Circular A-130 directs the Department of Justice to provide appropriate guidance on pursuing legal remedies in the case of serious incidents.

According to NIST, the two main benefits of an incident-handling capability are (1) containing and repairing damage from incidents and (2) preventing future damage. Other, less obvious, benefits of an incident-handling capability include

- improved threat data for use in the risk assessment and control selection process,
- enhanced internal communication and organizational preparedness, and
- enhanced training and awareness programs by providing trainers with better information on users' knowledge and providing real-life illustrations for classes.

Also, according to NIST, the characteristics of a good incident-handling capability include

- an understanding of the constituency being served, including computer users and program managers;
- an educated constituency that trusts the incident-handling team;
- a means of prompt centralized reporting, such as through a hotline;
- a response team with the necessary knowledge, skills, and abilities, including technical expertise with the computer technology used by the entity, and the ability and willingness to respond when and where needed; and
- links to other groups—such as law enforcement agencies, response teams, or security groups external to the entity—and to the entity's public relations office (in case the incident receives media attention).

One aspect of incident response that can be especially problematic is gathering the evidence to pursue legal action. Incident response training and assistance is important for users of information systems to understand the proper handling and reporting of security incidents. Resources should be available to provide adequate computer forensics of security incidents. To gather evidence, an entity may need to allow an intruder or violator to continue his or her inappropriate activities—a situation that puts the system and data at continued risk. However, fear of detection and prosecution can serve as a deterrent to future violations.

The United States Computer Emergency Readiness Team (US–CERT) was established in September 2003 to provide a national incident response capability. US–CERT is a partnership of the Department of Homeland Security and the public and private sectors. Established to protect the nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation. Specifically, it is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities.

As the nation's focal point for preventing, protecting against, and responding to cyber security vulnerabilities, US–CERT interacts with all federal agencies, private industry, the research community, state and local governments, and others on a 24X7 basis to disseminate reasoned and actionable cyber security information. To provide security information to the public, US–CERT

- integrates content contributed by numerous organizations from both the public and private sectors,
- aggregates and analyzes the various types of data provided by contributing organizations,
- serves as the focal point for promoting common and comprehensive analysis of security trends and risks, and
- maintains quality control standards and works to ensure technical accuracy as well as timeliness.

Worldwide, there are more than 250 organizations that use the name CERT or a similar name and deal with cyber security response. US–CERT and the CERT Coordination Center at Carnegie Mellon University work jointly on cyber security activities. When a cyber security problem warrants, US-CERT coordinates a response by working with computer security experts from public and private state and local incident response teams. (See www.us-cert.gov/aboutus.html.)

In addition, the incident response program is affected by and should be responsive to the configuration of the entity's networks. For example, it can affect the placement of intrusion detection systems. Also, the network and related access controls can be designed to aid in containment of security breaches to limited areas of the network.

Also, the incident response program should appropriately consider treatment of privacy information. Specifically, federal entities should comply with applicable statutes and OMB guidance, including the following OMB Memoranda:

- M-06-15, *Safeguarding Personally Identifiable Information* (5/22/06)
- M-06-16, *Protection of Sensitive Agency Information* (6/23/06)
- M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments* (7/12/06)
- *OMB* Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (generally annual OMB memorandums)
- *Recommendations for Identity Theft Related Data Breach Notifications* (9/20/06)
- M-07-04, *Use of Commercial Credit Monitoring Services Blanket Purchase Agreements* (12/22/06)

AC-5.2. Incidents are effectively identified and logged

Entity policies and procedures should establish criteria for the identification of significant system events that should be logged. Based on such criteria, the entity should identify significant system events. At a minimum, all such significant events,[87] including access to and modification of sensitive or critical system resources, should be logged. Also, logging should include appropriate information to facilitate monitoring of access to business process applications and related actions taken by application users. To be effective:

- identification and logging of auditable events should be based on considerations of costs, benefits, and risk;
- this feature should be activated to log critical activity, maintain critical audit trails, and report unauthorized or unusual activity;
- access to audit logs should be adequately controlled; and
- managers should review logs for unusual or suspicious activity and take appropriate action.

Access control software should be used to maintain an audit trail of security access containing appropriate information for effective review to determine how, when, and by whom specific actions were taken. For example, time stamps of audit records should be generated using internal information system clocks that are synchronized systemwide. Such information is critical to monitoring compliance with security policies and when investigating security incidents. The settings of the access control software control the nature and extent of audit trail information provided. Typically, audit trails may include user ID, resource accessed, date, time, terminal location, and specific data modified. The information system should have the capability to determine whether or not a given individual took a particular action (non-repudiation).

The completeness and value of the audit trails maintained will only be as good as the entity's ability to thoroughly identify the critical processes and the related information that may be needed. Procedures for maintaining such audit trails should be based on

[87] The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of auditable events.

- the value or sensitivity of data and other resources affected;
- the processing environment, for example, systems development, testing, or production;
- technical feasibility; and
- legal and regulatory requirements.

Audit trails, including automated logs, need to be retained for an appropriate period of time. Therefore, the entity needs to allocate sufficient audit record storage capacity and configure auditing to prevent the storage capacity from being exceeded. The information system should provide a warning when storage capacity reaches a certain level. If storage capacity is reached, the system should alert appropriate officials and take appropriate, predefined actions such as saving the oldest data offline, shutting down the system, overwriting the oldest audit records, or stop generating audit records.

An effective intrusion detection system (IDS) should be implemented, including appropriate placement of intrusion-detection sensors and setting of incident thresholds. IDS security software generally provides a means of determining the source of a transaction or an attempted transaction and of monitoring users' activities (audit trail).

AC-5.3. Incidents are properly analyzed and appropriate actions taken

Because all of the audit trail and log information maintained is likely to be too voluminous to review on a routine basis, the IDS security software should be implemented to selectively identify unauthorized, unusual, and sensitive access activity, such as

- attempted unauthorized logical and physical access;
- access trends and deviations from those trends;
- access to sensitive data and resources;
- highly-sensitive privileged access, such as the ability to override security controls;
- access modifications made by security personnel; and
- unsuccessful attempts to logon to a system.

Modern information systems may have an audit-reduction and report-generation capability to automatically process audit records for events of interest based on selectable event criteria. The security software should be designed to report such activity and, in some cases, respond by actions such as

- disabling passwords,
- terminating repeated failed attempts to access sensitive resources,
- terminating processing,
- shutting down terminals,
- issuing warning or error messages, and
- writing audit trail records that would not normally be maintained.

Once unauthorized, unusual, or sensitive access activity is identified, it should be reviewed and apparent or suspected violations investigated. If it is determined that a security violation has occurred, appropriate action should be taken to identify and remedy the control weaknesses that allowed the violation to occur, repair any damage that has been done, and determine and discipline the perpetrator. It is important that an entity have formal written procedures for reporting security violations or suspected violations to a central security management office so that multiple related incidents can be identified, other employees can be alerted to potential threats, and appropriate investigations can be performed. Such incidents might include multiple attacks by a common hacker or repeated infections with the same computer virus.

Without prompt and appropriate responses to security incidents, violations could continue to occur and cause damage to an entity's resources indefinitely. Further, violators will not be deterred from continuing inappropriate access activity, which could cause embarrassment to the entity and result in disclosure of confidential information and financial losses.

An entity should have documented procedures in place for responding to security violations. These should include procedures and criteria for

- incident containment, eradication, and recovery
- documenting offenses,
- determining the seriousness of violations,
- reporting violations to higher levels of management,
- investigating violations,
- imposing disciplinary action for specific types of violations,
- notifying the resource owner of the violation,
- sharing incident and threat information with owners of connected systems, and
- notifying and consulting with, as appropriate, law enforcement agencies, and for federal entities, relevant agency IGs and the US-CERT.

Further, access control policies and techniques should be modified when violations, incidents, and related risk assessments indicate that such changes are appropriate.

In addition, the frequency and magnitude of security violations and the corrective actions that have been taken should periodically be summarized and reported to senior management. Such a report can assist management in its overall management of risk by identifying the most attractive targets, trends in types of violations, cost of securing the entity's operations, and any need for additional controls.

Finally, since even the best incident response program may not catch increasingly sophisticated system intrusions, critical system resources should be periodically reviewed for integrity. For example, an organization may employ integrity verification applications on the information system to automatically look for evidence of information tampering, errors, and omissions.

AC-5 Related NIST SP 800-53 Controls	
AC-13	Supervision and Review—Access Control
AT-5	Contacts with Security Groups and Associations
AU-2	Auditable Events
AU-3	Content of Audit Records
AU-4	Audit Storage Capacity
AU-5	Response to Audit Processing Failures
AU-6	Audit Monitoring, Analysis, and Reporting
AU-7	Audit Reduction and Report Generation
AU-8	Time Stamps
AU-9	Protection of Audit Information
AU-11	Audit Record Retention
IR-1	Incident Response Policy and Procedures
IR-2	Incident Response Training
IR-3	Incident Response Testing and Exercises
IR-4	Incident Handling
IR-5	Incident Monitoring
IR-6	Incident Reporting
IR-7	Incident Response Assistance
SC-5	Denial Of Service Protection
SI-4	Information System Monitoring Tools and Techniques
SI-6	Security Functionality Verification

Control Techniques and Suggested Audit Procedures for Critical Element AC-5

Table 20. Control Techniques and Suggested Audit Procedures for Critical Element AC-5: Implement an effective audit and monitoring capability

Control activities	Control techniques	Audit procedures
AC-5.1. An effective incident response program is documented and approved.	AC-5.1.1. An effective incident-response program has been implemented and include • documented policies, procedures, and plans; • documented testing of the incident response plan and follow-up on findings; • a means of prompt centralized reporting; • active monitoring of alerts/advisories; • response team members with the necessary knowledge, skills, and abilities; • training on roles and responsibilities and periodic refresher training; • links to other relevant groups; • protection against denial-of-service attacks (see http://icat.nist.gov); • appropriate incident-response assistance; and • consideration of computer forensics.	Interview security manager, response team members, and system users; review documentation supporting incident handling activities; compare practices to policies, procedures, and related guidance such as NIST SP 800-61 that provides guidance on incident-handling and reporting. Determine qualifications of response team members; review training records; identify training in incident response roles and responsibilities. Identify the extent to which computer forensics is used and compare to applicable guidelines and industry best practices.
AC-5.2. Incidents are effectively identified and logged.	AC-5.2.1. An effective intrusion detection system has been implemented, including appropriate placement of intrusion-detection sensors and incident thresholds.	Obtain the design and justification for the intrusion detection system; determine if the placement of sensors and incident thresholds is appropriate based on cost and risk.
	AC-5.2.2. An effective process has been established based on a risk assessment, to identify auditable events that will be logged.	Interview the security manager to determine the process for determining what actions are logged. Determine if security event correlation tools are used to identify anomalous network activity.
	AC-5.2.3. All auditable events, including access to and modifications of sensitive or critical system resources, are logged.	Review security software settings to identify types of activity logged; compare to NIST SP 800-92 guidance on auditable events.
	AC-5.2.4. Audit records contain appropriate information for effective review including sufficient information to establish what events occurred, when the events occurred (for example, time stamps), the source of the events, and the outcome of the events.	Determine if audit records/logs are reviewed and whether they contain appropriate information; see NIST SP 800-92 for guidance.
	AC-5.2.5. Audit record storage capacity is adequate and configured to prevent such capacity from being exceeded. In the event of an audit failure or audit storage capacity being reached, the information system alerts officials and appropriate action is taken.	Determine the retention period for audit records and logs and whether it complies with applicable guidance. Determine if audit capacity is sufficient and what happens should it be exceeded.
	AC-5.2.6. Audit records and tools are protected from unauthorized access, modification, and deletion. Audit records are effectively reviewed for unusual or suspicious activity or violations.	Determine how access to audit records/logs is controlled; review logs for suspicious activity and evidence of entity follow-up and appropriate corrective action.

Control activities	Control techniques	Audit procedures
	AC-5.2.7. Audit records are retained long enough to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	Determine if audit record retention (for example, logs etc.) meet legal requirements and entity policy for computer forensics. See General Records Schedule 20 and 24 for guidance on requirements for record retention.(http://archives.gov/records-mgmt/ardor/grs20.html and http://archives.gov/records-mgmt/ardor/grs24.html)
AC-5.3. Incidents are properly analyzed and appropriate actions taken.	AC-5.3.1. Security violations and activities, including failed logon attempts, other failed access attempts, and sensitive activity, are reported and investigated.	Review pertinent policies and procedures; review security violation reports; examine documentation showing reviews of questionable activities.
	AC-5.3.2. Security managers investigate security violations and suspicious activities and report results to appropriate supervisory and management personnel.	Test a selection of security violations to verify that follow-up investigations were performed and reported to appropriate supervisory and management personnel.
	AC-5.3.3. Appropriate disciplinary actions are taken.	For the selection reviewed in AC-5.3.2, determine what action was taken against the perpetrator.
	AC-5.3.4. Violations and incidents are analyzed, summarized, and reported to senior management and appropriate government authorities.	Interview senior management and personnel responsible for summarizing violations; review any supporting documentation. Determine if automated tools are used to analyze network activity and whether it complies with security policy.
	AC-5.3.5. Alerts and advisories are issued to personnel when appropriate.	Identify recent alerts and advisories and determine if they are up-to-date; interview entity personnel to determine what actions were taken.
	AC-5.3.6 Incident and threat information is shared with owners of connected systems.	Determine if incident and threat data are shared with owners of connected systems; follow up with owners of connected systems to see if they received this information in a timely manner.
	AC-5.3.7. Access control policies and techniques are modified when violations, incidents, and related risk assessments indicate that such changes are appropriate.	Review policies and procedures and interview appropriate personnel; review any supporting documentation.
	AC-5.3.8. Critical system resources are periodically reviewed for integrity.	Determine how frequently alterations to critical system files are monitored (for example, integrity checkers, etc.).
	AC-5.3.9. Appropriate processes are applied to gather forensic evidence in support of investigations.	Review entity processes to gather forensic information and determine whether they are adequate. Discuss with appropriate entity management.

Source: GAO.

Critical Element AC-6. Establish adequate physical security controls

Adequate physical security controls should be established that are commensurate with the risks of physical damage or access. In evaluating the effectiveness of physical security controls, the auditor should consider the effectiveness of the entity's policies and practices pertaining to both the overall facility and areas housing sensitive information technology components. Consequently, an entity should implement physical security controls in the following areas

- security planning and management (security management),
- securing the perimeter of the facility (perimeter security),
- controlling access into a facility (entry security),
- controlling access within a facility (interior security), and
- protection from emerging physical security threats (emerging threats).

Physical security controls restrict physical access to computer resources and protect them from intentional or unintentional loss or impairment. Computer resources to be protected include

- primary computer facilities,
- cooling system facilities,
- network devices such as routers and firewalls,
- terminals used to access a computer,
- microcomputers and mobile or portable systems,
- devices that display or output information,
- access to network connectivity, such as through "live" network jacks
- computer file storage areas, and
- telecommunications equipment and transmission lines.

In June 1995, the Department of Justice (DOJ) published minimum-security standards for the protection of federal facilities. It identified and evaluated the various types of security measures that could be used to counter potential vulnerabilities. The standards

cover perimeter security, entry security, interior security, and security planning. Because of the considerable differences among facilities and their security needs, physical holdings are divided into five security levels to determine which minimum standards are appropriate for which security levels.[88] For federal entity facilities, appropriate criteria for physical safeguards in place for the overall facility are Justice standards unless the facility has adopted different standards. To illustrate, information technology resources may be housed in a facility that has been designated a national critical asset in accordance with Homeland Security Presidential Directive 7[89] and therefore require physical security measures above those required by DOJ standards. For non-federal entities, appropriate criteria are equivalent guidance or the federal standards.

Physical controls also include environmental controls, such as smoke detectors, fire alarms, extinguishers, and uninterruptible power supplies (see section 3.5, service continuity).

In an IS controls audit being performed as part of a financial audit or data reliability assessment, the auditor should tailor the identification of control techniques and audit procedures related to the entity's physical security management program to the extent necessary to achieve the audit objectives, considering the IS controls identified by the auditor as significant to the audit objectives (e.g., internal control over financial reporting). Generally, this would include consideration of the overall design of the entity's physical security program at relevant facilities.

AC-6.1. Establish a physical security management program based on risk

Risk management is the foundation of an effective physical security program. The approach to good security is fundamentally similar, regardless of the assets being protected—information systems, buildings, or critical infrastructure. Risk management principles for

[88]Department of Justice, *Vulnerability Assessment of Federal Facilities*, (Washington, D.C.: June 28, 1995).

[89]*Critical Infrastructure Identification, Prioritization, and Protection* (Washington, D.C.: December 17, 2003).

an effective security program are discussed in section 3.1. In addition, the testimonies *Technologies to Secure Federal Buildings* (GAO-02-687T) and *Key Elements of a Risk Management Approach* (GAO-02-150T) elaborate on specific risk management steps that may be applied to the protection of any critical asset.

The effectiveness of physical security controls depends on the effectiveness of the entity's policies and practices pertaining to the overall facility and to areas housing sensitive information technology components, including

- granting and discontinuing access authorizations,
- controlling badges, ID cards, smartcards, passkeys, and other entry devices,
- controlling entry during and after normal business hours,
- controlling the entry and removal of computer resources (for example, equipment and storage media) from the facility,
- managing emergencies,
- controlling reentry after emergencies,
- establishing compensatory controls when restricting physical access is not feasible, as is often the case with telecommunications lines, and
- storing computer assets such as equipment and sensitive documents.

In some instances an entity may not be able to fully control their physical security posture. For example, leased space in a building managed by another organization. In this case, the entity should consider compensating controls and ensure that contingency planning adequately considers their lack of control over physical security.

As with any type of business activity, physical security should be monitored to ensure that controls are accomplishing their intended purpose. FISMA specifically requires that federal agencies periodically test and evaluate information security controls and techniques to ensure that they are effectively implemented.

Visitors should be controlled. On occasion, persons other than regularly authorized personnel may be granted access to sensitive areas or facilities, such as employees from another facility, maintenance personnel, contractors, and the infrequent or unexpected visitor. None of these visitors should be granted unrestricted access.[90] Controls should include

- preplanned appointments,
- identification checks,
- controlling the reception area,
- logging in visitors,
- escorting visitors while in sensitive areas, and
- periodically changing entry codes to prevent reentry by previous visitors who might have knowledge of the code.

AC-6.2. Establish adequate perimeter security based on risk

Perimeter security is the first line of defense against threats that can cause catastrophic damages to facilities and internal computer resources. Considerations for perimeter security include

- controlling vehicle and pedestrian traffic around the facility,
- controlling employee and visitor parking,
- monitoring the perimeter with closed circuit TV (CCTV),
- providing emergency backup power supply, and
- extending perimeter barriers to prevent unauthorized access and reduce exposure to explosions.

Perimeter security includes protective controls such as fencing around sensitive buildings, concrete and earthen and other barriers,

[90]Also see Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, (Washington, D.C.: August 27, 2004); and NIST Federal Information Processing Standard Publication (FIPS PUB) 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, (Washington, D.C.: March 2006).

appropriate gates and locks, exterior lighting, guard posts, security patrols, and detection and monitoring systems.

AC-6.3. Establish adequate security at entrances and exits based on risk

Access to facilities should be limited to personnel having a legitimate need for access to perform their duties. Management should regularly review the list of persons authorized to have physical access to sensitive facilities, including contractors and other third parties. In addition, procedures should be implemented to terminate access privileges for terminated or separated employees or contractors.

Physical security controls at entrances and exits vary, but may include

- manual door or cipher key locks,
- magnetic door locks that require the use of electronic keycards,
- biometrics authentication,
- security guards,
- photo IDs,
- entry logs, and
- electronic and visual surveillance systems.

Unissued keys or other entry devices should be secure. Issued keys or other entry devices should be regularly inventoried.

AC-6.4. Establish adequate interior security based on risk

The effectiveness of physical security controls over sensitive and critical IT resources within a facility include consideration of whether the entity has

- identified all sensitive areas—such as individual rooms or equipment, software and tape libraries, or telecommunication closets and lines—that are susceptible to physical access, loss, or impairment;
- identified all physical access points and threats to the sensitive areas; and

- developed cost-effective security controls over all physical access points and addressed all significant threats to sensitive areas.

In addition, the entity should have controls to prevent or detect surreptitious entry into sensitive areas. For example, could unauthorized persons gain entry by

- observing lock combinations entered by authorized personnel?
- obtaining unsecured keycards?
- going over the top of a partition that stops at the underside of a suspended ceiling when the partition serves as a wall for a sensitive facility?
- cutting a hole in a plasterboard wall in a location hidden by furniture?

Many of the control techniques for interior security are similar to those for perimeter and entry security (for example, locks, surveillance systems, as well as using and controlling badges, ID cards, smartcards, passkey, and other entry devices). Additional considerations include

- logs and authorization for removal and return of tapes and other storage media to the library,
- computer terminal locks,
- controlled access to powerful consoles in data centers, and
- segregation of duties (discussed in section 3.4).

AC-6.5. Adequately protect against emerging threats based on risk

In addition to traditional physical security considerations, it may be important to protect building environments from new threats such as airborne chemical, biological, and radiological (CBR) attacks. Such protective measures may include the installation of early warning sensors, the location and securing of air intakes, and plans and procedures to mitigate the effect of a CBR release. The decisions concerning which protective measures should be implemented for any building should be based on several factors,

including the perceived risk associated with the building and its tenants, engineering and architectural feasibility, and cost.

Appropriate audit procedures related to emerging threats include:

- Interview appropriate officials to identify the level of physical security controls needed for the facility.
- Review the facility risk and independent assessments (for example, internal audit, internal office of physical security, outside consultants) to identify their assessment of risk and the adequacy of controls in place.
- Observe and document the controls in place. Assess the organization's preparations based on what the organization has stated it needs based on risk, including an evacuation plan for a possible CBR attack.
- Identify any planned projects to enhance physical security controls in this area through discussions with physical security and building management/operations staff.

Control Techniques and Suggested Audit Procedures for Critical Element AC-6

AC-6 Related NIST SP 800-53 Controls	
PE-2	Physical Access Authorizations
PE-3	Physical Access Control
PE-4	Access Control for Transmission Medium
PE-5	Access Control for Display Medium
PE-6	Monitoring Physical Access
PE-7	Visitor Control
PE-8	Access Records
PE-16	Delivery and Removal

Table 21. Control Techniques and Suggested Audit Procedures for Critical Element AC-6: Establish adequate physical security controls

Control activities	Control techniques	Audit procedures
AC-6.1. Establish an effective physical security management program based on risk.		Coordinate AC-6 procedures with sections SM-2 (assess and validate risks), SM-3 (policies and procedures), SD-1 (segregation of duties), and CP-2 (environmental controls).
	AC-6.1.1. Use a risk management approach to identify the level of physical security needed for the facility and implement measures commensurate with the risks of physical damage or access.	Interview entity officials to discuss how their physical security program is organized and whether they use a risk management approach. Obtain and review any facility risk assessments performed by the entity or by independent entities.
	AC-6.1.2. Facilities and areas housing sensitive and critical resources have been identified. The following generally constitute sensitive areas: computer rooms, tape libraries, telecommunication closets, mechanical/ electrical rooms, cooling facilities and data transmission and power lines.	Review diagram of physical layout of the computer network, telecommunications, and cooling system facilities (for example, HVAC); Inspect these areas for physical access control weaknesses.
	AC-6.1.3. All significant threats to the physical well-being of these resources have been identified and related risks determined.	Interview entity officials. Review risk analysis to ensure that it includes physical threats to employees and assets. Review any recent audit reports or other evaluations of the facility's physical security.
	AC-6.1.4. Establish law enforcement security liaisons that facilitate the accurate flow of timely security information between appropriate government agencies, provide procedures for the timely receipt and dissemination of threat information, and implement a standardized security/threat classifications and descriptions (for example, alert levels).	Check if the organization has established law enforcement security liaisons that facilitate the accurate flow of timely security information between appropriate government agencies. Review how the organization receives and disseminates security alerts. Identify governmental agencies involved in the flow of security information and interview appropriate officials. Review procedures and nomenclature for threat information.
	AC-6.1.5. Conduct annual employee physical security awareness training. Coordinate this step with SM-4.	Review information (for example, individual training records, training program content) on security awareness training and its frequency.
	AC-6.1.6. Security control procedures (for example, trusted vendors/suppliers, background checks, etc.) are established for non-employees (contractors, custodial personnel).	Review security control procedures for scope and adequacy.

Control activities	Control techniques	Audit procedures
	AC-6.1.7. Periodic monitoring and independent evaluations of the physical security program are conducted. Physical security incidents are effectively monitored and appropriate countermeasures are implemented.	Check if the entity evaluates its physical security program and controls. Obtain and review the entity's most recent self assessments and compliance review report. Determine if security incidents are recorded, effectively analyzed, and result in appropriate countermeasures. Coordinate with SM-5: Monitor the effectiveness of the security program, and AC-5: Implement an effective audit and monitoring capability.
	AC-6.1.8. When possible, do not co-locate high risk operations with non-essential support organizations (for example, cafeteria, day care, banks, news media). If not possible, place appropriate security between such support organizations and critical facilities.	Identify co-located operations and their respective risk levels. Determine if the entity co-locates high risk operations with support operations and assess the security impact.
	AC-6.1.9. Visitors, contractors, and maintenance personnel are authenticated through the use of preplanned appointments and identification checks.	Review appointment and verification procedures for visitors, contractors, and maintenance personnel. Compare actual practices to procedures.
AC-6.2. Establish adequate perimeter security based on risk.	AC-6.2.1. Control/restrict vehicle and pedestrian traffic around the facility based on the facility's risk level. Specific measures include fences, gates, locks, guard posts, perimeter patrols and inspections.	Determine if vehicle and pedestrian traffic around the facility is adequately controlled for the risk level. Inspect the perimeter for physical security and access control weaknesses. Assess the effectiveness of perimeter guard procedures and practices for controlling access to facility grounds.
	AC-6.2.2. Control employee and visitor parking. For example, restrict access to facility parking and parking adjacent to the facility (including leases), use ID systems and procedures for authorized parking (for example, placard, decal, card key), have signs and arrangements for towing of unauthorized vehicles and adequate lighting for parking areas.	Observe parking area and related controls. Check if identification systems and procedures for authorized parking are in place. Determine what is done about unauthorized vehicles (e.g. towing).
	AC-6.2.3. Monitor the perimeter with closed circuit television (CCTV) including cameras with time lapse video recording and warning signs advising of 24 hour video surveillance.	Inspect the facility surveillance camera system to assess its capacity and ability to assist in protecting the facility's perimeter.
	AC-6.2.4. Lighting is adequate for effective surveillance and evacuation operations. Emergency power backup exists for lighting (as well as for alarm and monitoring systems).	Observe perimeter and exterior building lighting to determine its adequacy. Also, determine if emergency power is available for security systems. Request test results.
	AC-6.2.5. Extend perimeter barriers (for example, concrete, steel) and parking barriers, as needed, to prevent unauthorized access and reduce exposure to explosions.	Determine if perimeter barriers are used and extended if appropriate.
AC-6.3. Establish adequate security at entrances and exits based on risk.	AC-6.3.1. All employee access is authorized and credentials (for example, badges, identification cards, smart cards) are issued to allow access.	Observe and document all access control devices used to secure the facility.

Control activities	Control techniques	Audit procedures
	AC-6.3.2. Access is limited to those individuals who routinely need access through the use of guards, identification badges, or entry devices such as key cards.	Observe entries to and exits from facilities during and after normal business hours. Obtain a list of employees and contractors with badged access and check the justification for such access. Check whether terminated employees/contractors have turned in their badge.
	AC-6.3.3. Management conducts regular reviews of individuals with physical access to sensitive facilities to ensure such access is appropriate.	Review procedures used by management to ensure that individuals accessing sensitive facilities are adequately restricted. Evaluate support for physical access authorizations and determine appropriateness.
	AC-6.3.4. Intrusion detection systems with central monitoring capability are used to control access outside of normal working hours (for example, nights and weekends).	Determine if an intrusion detection system is used and test its use for appropriate exterior and interior apertures.
	AC-6.3.5. Visitor access logs are maintained and reviewed.	Compare entries in the log to a list of personnel authorized access.
	AC-6.3.6. X-ray and magnetometer equipment is used to screen people, possessions, and packages.	Observe how this equipment is used and test its effectiveness.
	AC-6.3.7. The entity controls information system-related items (i.e., hardware, firmware, software) entering and exiting the facility and maintains appropriate records of those items.	Review procedures and interview officials. Attempt to enter and exit the facility with information systems items at various entry points and times.
	AC-6.3.8. Entry and exit points are monitored by using CCTV capability. Also, high security locks and alarm systems are required for all doors that are not guarded.	Observe use of these devices and test as appropriate. Inspect the building(s) for physical access control weaknesses.
	AC-6.3.9. Emergency exit and re-entry procedures ensure that only authorized personnel are allowed to reenter the facility after fire drills, etc.	Review written emergency procedures. Examine documentation supporting prior fire drills. Observe a fire drill.
AC-6.4. Establish adequate interior security based on risk.	AC-6.4.1. An ID badge should generally be displayed at *all* times. [All individuals must display an ID at all times.]	Observe use of employee and visitor IDs. See what happens if you do not display your own ID.
	AC-6.4.2. Visitors such as vendors, contractors, and service personnel who need access to sensitive areas are prescreened, formally signed in, badged and escorted.	Review visitor entry logs. Observe entries to and exits from sensitive areas during and after normal business hours. Interview guards at facility entry.

Control activities	Control techniques	Audit procedures
	AC-6.4.3. Sensitive information technology and infrastructure resources are adequately secured (for example, using keys, alarm systems, security software and other access control devices), including • the badging system, • computer room, master consoles, and tape libraries, • display and output devices, • data transmission lines, • power equipment and power cabling, • mobile or portable systems, and • utility and mechanical areas (HVAC, elevator, water).	Interview officials. Walk through facilities and observe potential vulnerabilities and security controls [measures] used to protect sensitive information technology resources. Observe entries to and exits from sensitive areas during and after normal business hours. Review security software features and settings. Evaluate the badging system: who has access to the badging system and how it is protected; how is physical control maintained over unissued and visitor badges. Test the controls.
	AC-6.4.4. Management conducts regular reviews of individuals with physical access to sensitive areas to ensure such access is appropriate.	Review procedures used by management to ensure that individuals accessing sensitive areas are adequately restricted. Determine if there is a periodic (e.g. annual) auditing and reconciliation of ID cards. Evaluate support for physical access authorizations and determine appropriateness.
	AC-6.4.5. As appropriate, physical access logs to sensitive areas are maintained and routinely reviewed.	Compare entries in the logs to a list of personnel authorized access.
	AC-6.4.6. Unissued keys, badges, or other entry devices are secured. Issued keys or other entry devices are regularly inventoried.	Observe practices for safeguarding keys, badges, and other devices.
	AC-6.4.7. Entry codes are changed periodically.	Review documentation of entry code changes.
	AC-6.4.8. All deposits and withdrawals of storage media from the library are authorized and logged.	Review procedures for the removal and return of storage media to and from the library. Select from the log some returns and withdrawals, verify the physical existence of the tape or other media, and determine whether proper authorization was obtained for the movement.
	AC-6.4.9. Documents/equipment are appropriately stored and are subject to maintenance and accountability procedures.	Examine and verify maintenance and accountability procedures for storage of documents and equipment.
	AC-6.4.10. Critical systems have emergency power supplies (for example, all alarm systems, monitoring devices, entry control systems, exit lighting, communication systems).	Verify that critical systems, (e.g., alarm systems, monitoring devices, entry control systems, exit lighting, and communication systems) have emergency power supplies. Identify back up systems and procedures and determine the frequency of testing. Review testing results.

Control activities	Control techniques	Audit procedures
AC-6.5. Adequately protect against emerging threats, based on risk	AC-6.5.1. Appropriate plans have been developed and controls implemented based on a risk assessment such as a shelter in place plan and/or evacuation plan for a potential CBR attack. A plan is in place and tested to respond to emerging threats such as a CBR attack (e.g. an appropriate shelter in place and/or evacuation plan.)	Interview officials, review planning documents, and related test results. Observe and document the controls in place to mitigate emerging threats.
	AC-6.5.2. Outdoor areas such as air intakes, HVAC return air grilles, and roofs have been secured by restricting public access and relocating or protecting critical entry points (for example, air intake vents, protective grills, etc.)	Observe location of these devices and identify security measures that have been implemented.
	AC-6.5.3. All outdoor air intakes are monitored by CCTV, security lighting, and/or intrusion detection sensors.	Verify that all outdoor air intakes are monitored by CCTV or other similar security.
	AC-6.5.4. The ventilation and air filtration system has been evaluated for vulnerabilities to CBR agents and remedial action taken based on cost and risks.	Interview officials and review the results of any evaluations.

Source: GAO.

3.3. Configuration Management (CM)

Configuration management (CM) involves the identification and management of security features for all hardware, software, and firmware components of an information system at a given point and systematically controls changes to that configuration during the system's life cycle. At an entitywide level, management develops security policies that establish the entity's configuration management process and may establish the configuration settings for the organization. Policy enforcement applications can be used to help administrators define and perform centralized monitoring and enforcement of an entity's security policies. These tools examine desktop and server configurations that define authorized access to specified devices and they compare these settings against a baseline policy. At a system level, network management provides system administrators with the ability to control and monitor a computer network from a central location. Network management systems obtain status data from network components, enable network managers to make configuration changes, and alert them of problems. For each critical control point, at each system sublevel (for example, network, operating systems, and infrastructure applications), the entity should have configuration management controls to ensure that only authorized changes are made to such critical components. At a business process application level, all applications and changes to those applications should go through a formal, documented systems development process that identifies all changes to the baseline configuration. Also, procedures should ensure that no unauthorized software is installed.

In some instances, the entity may not have an effective entitywide configuration management process, but may nonetheless have configuration management controls at the systems and business process application level. Therefore, evaluation of configuration controls at all levels is important to determine whether they are effective.

FISMA requires each federal agency to determine minimally acceptable system configuration requirements and ensure compliance with them. Systems with secure configurations have less vulnerability and are better able to thwart network attacks. In

response to both FISMA and the Cyber Security Research and Development Act, NIST developed a central repository for information technology security configuration checklists: http://checklists.nist.gov. Typically, checklists are created by information technology vendors for their own products; however, checklists are also created by other entities such as consortia, academia, and government agencies. Security configuration checklists are a series of instructions for configuring a product to a particular operational environment. Some examples of the types of devices and software for which security checklists are intended are as follows:

- general purpose operating systems
- common desktop applications such as e-mail clients, Web browsers, word processing, personal firewalls, and antivirus software
- infrastructure devices such as routers, firewalls, virtual private network (VPN) gateways, intrusion detection systems (IDS), wireless access points (WAP), and telecom systems
- application servers such as domain name system (DNS) servers, dynamic host configuration protocol (DHCP) servers, Web servers, simple mail transfer protocol (SMTP) servers, file transfer protocol (FTP) servers, and database servers
- other network devices such as mobile devices, scanners, printers, copiers, and fax appliances

Industry best practices, NIST, and DOD guidance[91] all recognize the importance of configuration management when developing and maintaining a system or network. Through configuration management, the composition of a system is formally defined and tracked to ensure that an unauthorized change is not introduced. Changes to an information system can have a significant impact on the security of the system. Documenting information system changes and assessing the potential impact on the security of the system on an ongoing basis is an essential aspect of maintaining the

[91] See, for example, IEEE Standard 1200-1998, SEI CMMI (ver. 1.1), NIST SP 800-64, and Military Handbook 61A(SE).

security posture. An effective entity configuration management and control policy and associated procedures are essential to ensuring adequate consideration of the potential security impact of specific changes to an information system. Configuration management and control procedures are critical to establishing an initial baseline of hardware, software, and firmware components for the entity and subsequently controlling and maintaining an accurate inventory of any changes to the system.

An effective configuration management process consists of four primary concepts, each of which should be described in a configuration management plan and implemented according to the plan. The four are:

- *configuration identification:* procedures for identifying, documenting, and assigning unique identifiers (for example, serial number and name) to a system's hardware and software component parts and subparts, generally referred to as configuration items
- *configuration control:* procedures for evaluating and deciding whether to approve changes to a system's baseline configuration; decision makers such as a configuration control board evaluate proposed changes on the basis of costs, benefits, and risks, and decide whether to permit a change
- *configuration status accounting:* procedures for documenting and reporting on the status of configuration items as a system evolves. Documentation, such as historical change lists and original designs or drawings, are generated and kept in a library, thereby allowing entities to continuously know the state of a system's configuration and be in a position to make informed decisions about changing the configuration.
- *configuration auditing:* procedures for determining alignment between the actual system and the documentation describing it, thereby ensuring that the documentation used to support decision making is complete and correct. Configuration audits are performed when a significant system change is introduced and help to ensure that only authorized changes are being made and that systems are operating securely and as intended.

Establishing controls over the modification of information system components and related documentation helps to ensure that only authorized systems and related program modifications are implemented. This is accomplished by instituting policies, procedures, and techniques that help make sure all hardware, software, and firmware programs and program modifications are properly authorized, tested, and approved, and that access to and distribution of computer assets is carefully controlled. Without proper controls, there is a risk that security features could be inadvertently or deliberately omitted or turned off or that processing irregularities or malicious code could be introduced. For example,

- a knowledgeable programmer could modify program code to provide a means of bypassing controls to gain access to sensitive data;
- the wrong version of a program could be implemented, thereby perpetuating outdated or erroneous processing that is assumed to have been updated; or
- a virus could be introduced, inadvertently or on purpose, that disrupts processing.

Effective configuration management prevents unauthorized changes to information system resources (for example, software programs and hardware configurations) and provides reasonable assurance that systems are configured and operating securely and as intended.

The absence of effective system-level configuration management is a serious risk that jeopardizes an entity's ability to support current and potential requirements. Without effective configuration management, users do not have adequate assurance that the system and network will perform as intended and to the extent needed to support their missions.

Assessing controls over configuration management involves evaluating the entity's success in performing each of the critical elements listed in table 22. Also, NIST SP 800-100 provides guidance in related configuration management programmatic areas of capital planning and investment control, and security services and product acquisition. This publication discusses practices designed to help security managers identify funding needs to secure systems and

provide strategies for obtaining the necessary funding. In addition, it provides guidance to entities in applying risk management principles to assist in the identification and mitigation of risks associated with security services acquisitions.

Table 22. Critical Elements for Configuration Management

Number	Description
CM-1.	Develop and document CM policies, plans, and procedures
CM-2.	Maintain current configuration identification information
CM-3.	Properly authorize, test, approve, and track all configuration changes
CM-4.	Routinely monitor the configuration
CM-5.	Update software on a timely basis to protect against known vulnerabilities
CM-6.	Appropriately document and approve emergency changes to the configuration

Source: GAO

Critical Element CM-1. Develop and document CM policies, plans, and procedures

Configuration management policies, plans, and procedures should be developed, documented, and implemented at the entitywide, system, and application levels to ensure an effective configuration management process. Such procedures should cover employee roles and responsibilities, change control and system documentation requirements, establishment of a decision-making structure, and configuration management training. CM should be a key part of an entity's Systems Development Life Cycle (SDLC) methodology.[92]

An effective entitywide SDLC methodology details the procedures that are to be followed when systems and applications are being designed and developed, as well as when they are subsequently modified. The SDLC should provide a structured approach for identifying and documenting needed changes to computerized operations; assessing the costs and benefits of various options, including the feasibility of using off-the-shelf software; and designing, developing, testing, and approving new systems and system modifications. It is especially important that, for new

[92]A Systems Development Life Cycle (SDLC) methodology consists of the policies and procedures that govern software development and modification as a software product goes through each phase of its life cycle.

systems being developed or for major enhancements to existing systems, SDLC require approving design features at key points during the design and development process. For the methodology to be properly applied, it should be sufficiently documented to provide staff with clear and consistent guidance. Also, personnel involved in designing, developing, and implementing new systems and system modifications should be appropriately trained. This includes program staff who initiate requests for modifications and staff involved in designing, programming, testing, and approving changes.

Information system controls should be integrated into the SDLC to reasonably ensure appropriate protection for the information that the system is intended to support. Implementing information system controls early in the development of a system should reduce the risk of introducing vulnerabilities to the environment. This will also generally result in less expensive and more effective security than adding information system controls to an operational system. Information system controls should be considered in each phase of the SDLC. The SDLC typically will include the following phases: initiation, design/development, implementation, and operations/maintenance.

During the initiation phase, the entity establishes the need for a specific system and documents its purpose. In this phase the entity should define high-level information security policy requirements, including the development of the system security plan.

The design/development phase, includes efforts directed to designing, programming, developing, and testing the system. In this phase, the entity should define the system's security and functional requirements. These requirements should include technical features (e.g., access controls), assurances (e.g., background checks for system developers), or operational practices (e.g., security awareness training). This phase should also include testing the technical and system control features to ensure that they perform as intended.

In the implementation phase, the entity configures and enables information system control features, tests the functionality of these features, installs the system, and tests system prior to placing it into

operation to ensure that it meets all required security specifications. Tests should include user acceptance testing and related documentation of this test. Design reviews and system tests should be fully documented, updated, as new reviews or tests are performed, and maintained.

In the operation and maintenance phase, systems are in place and operating, enhancements and/or modifications to the system are developed and tested, and software is added or replaced. Documenting information system control changes and assessing the potential impact of these changes on the security of a system is an essential part of the continuous monitoring and key to avoiding a lapse in the system security.

Information system controls in the business process environment may be manual or automated. Automated controls are system-based, and may be used to control such things as the correctness or accuracy of data, such as edits and validations. Manual controls are procedures that require human intervention, such as the approval of a transaction, and are typically used to assure the reasonableness or propriety of transactions. Automated and manual controls can be preventive or detective. Automated controls can keep invalid data from being processed, and they can report transactions that fail to meet reasonableness criteria. Manual controls performed prior to input can identify problems before data is processed, while monitoring controls performed after processing can identify errors.

Information system controls should be considered throughout the SDLC process. In addition, in this process safeguarding provisions for personally identifiable information should be reviewed, including conducting privacy impact assessments when new IT systems are under development or significant modifications are made as required by OMB.

NIST SP 800-64, dated October 2003, identifies security considerations in the information system development life cycle. In addition, NIST SP 800-27 provides guidance on engineering principles for designing security into information systems.

Configuration management policies and procedures should describe the configuration management process and address purpose, scope, roles, responsibilities, compliance, and implementation of security controls. Security controls include the following.

- A baseline configuration of the information system and an inventory of the system's constituent components.
- A process to document and control changes to the system.
- Monitoring system changes and analysis of their impact to determine the effect of the changes.
- Access restrictions over changes to the system and auditing of the enforcement actions.
- Configuring the security settings of information technology products to the most restrictive mode consistent with operational requirements.
- Configuring the information system to provide only essential capabilities and specifically prohibiting or restricting the use of unnecessary or dangerous functions, ports, protocols, and services.

Good configuration management provides strict control over the implementation of system changes and thus minimizes corruption to information systems.

Also, CM policies should address the introduction of software developed outside of the entity's normal software development process, including the outsourced development of software and commercial or other software acquired by individual users. Specific configuration management policy considerations for systems that are internet accessible (inbound or outbound) should address software quality controls designed to prevent security flaws from being introduced.

Configuration management plans should address configuration management in terms of the following:[93]

[93]Based on IEEE Standard for Software Configuration Management Plans (IEEE Std. 828-1998), the Institute of Electrical and Electronic Engineers, June 25, 1998.

- responsibilities and authorities for accomplishing the planned activities (who)
- activities to be performed (what)
- required coordination of configuration management activities with other activities (when)
- tools and physical and human resources required for the execution of the plan as well as how the plan will be kept current (how)

The CM plan should describe the allocation of responsibilities and authorities for CM activities to entities and individuals within the project structure. Organizational units may consist of a vendor and customer, a prime contractor and subcontractors, or different groups within one entity. The name of the organizational unit or job title to perform this activity is provided for each activity listed within CM activities. A matrix that relates these entities to CM functions, activities, and tasks is useful for documenting CM activities. CM activities identify all functions and tasks required to mange the configuration as specified in the scope of the CM plan. CM activities are traditionally grouped into four functions: configuration identification, configuration control, configuration status accounting, and configuration audits and reviews.

Configuration management procedures should describe the configuration management system used to maintain and change controlled work products. A configuration management system includes the storage media, the procedures, and the tools for accessing the configuration system. The procedures should describe how configuration items are stored and retrieved; shared between control levels; recovered; protected by access controls; and stored, updated, and retrieved. Configuration management plans should be integrated at all levels.

CM-1 Related NIST SP 800-53 Controls CM-1 Configuration Management Policy and Procedures

Control Techniques and Suggested Audit Procedures for Critical Element CM-1

Table 23. Control Techniques and Suggested Audit Procedures for Critical Element CM-1: Develop and document CM policies, plans, and procedures

Control activities	Control techniques	Audit procedures
CM-1.1. CM policies, plans, and procedures have been developed, documented, and implemented.	CM-1.1.1. An effective configuration management process is documented and implemented, including: • a CM plan that identifies roles, responsibilities, procedures, and documentation requirements; • guidance that is appropriate for personnel with varying levels of skill and experience; • trained personnel who are familiar with the organization's configuration management process; • permitting only essential capabilities and restricting the use of dangerous functions, ports, protocols, and services; • regular review and approval of configuration changes by management (for example, Configuration Control Board (CCB)); • appropriate representation on CCB from across the entity; • a formal SDLC methodology that includes system-level security engineering principles to be considered in the design, development, and operation of an information system. • appropriate systems documentation.	Review CM policies, plans, and procedures to identify roles, responsibilities, procedures, and documentation requirements. Determine if a CCB exists and is operating effectively. Review organizational chart to ensure that the CCB has appropriate representation from across the entity. Interview hardware and software managers to identify the currency and completeness of CM policies, plans, procedures, and documentation. Review CM documentation and test whether recent changes are incorporated. Review the SDLC methodology and ensure that security is adequately considered throughout the life cycle. Review a selection of system documentation to verify that the SDLC methodology was followed and complies with appropriate guidance, such as NIST SP 800-64 and SP 800-27.

Source: GAO.

Critical Element CM-2. Maintain current configuration identification information

Configuration identification activities involve identifying, naming, and describing the physical and functional characteristics of a controlled item (for example, specifications, design, IP address, code, data element, architectural artifacts, and documents). The CM plan should describe how each configuration item and its versions are uniquely named. It should also describe the activities performed to define, track, store, manage, and retrieve configuration items. Configuration items should be associated with development and production baselines.

The entity should maintain current configuration information in a formal configuration baseline that contains the configuration information formally designated at a specific time during a product's or product component's life. Configuration baselines, plus approved changes from those baselines, constitute the current configuration information. There should be a current and comprehensive baseline inventory of hardware, software, and firmware, and it should be routinely validated for accuracy. Backup copies of the inventory should be maintained and adequately protected. There should also be information system diagrams and documentation on the set up of routers, switches, guards, firewalls, and any other devices facilitating connections to other systems[94] FISMA requires federal entity compliance with system configuration requirements, as determined by the entity. In addition, OMB Memorandum M-07-11 [95] requires agencies that upgrade to the Microsoft Vista™ operating system to adopt the security configurations developed by the National Institute of Standards and Technology (NIST), the Department of Defense (DoD) and the Department of Homeland Security (DHS).

CM-2 Related NIST SP 800-53 Controls	
CM-2	Baseline Configuration
CM-6	Configuration Settings
CM-8	Information System Component Inventory
SA-5	Information System Documentation

[94] See OMB M-08-22, *Guidance on the Federal Desktop Core configuration (FDCC)* (Washington, DC:. August 11, 2008).

[95] OMB, Implementation of Commonly Accepted Security Configurations for Windows Operating Systems (Washington, D.C.: March 22, 2007).

Control Techniques and Suggested Audit Procedures for Critical Element CM-2

Table 24. Control Techniques and Suggested Audit Procedures for Critical Element CM-2: Maintain current configuration identification information

Control activities	Control techniques	Audit procedures
CM-2.1. Current configuration identification information is maintained.	CM-2.1.1. A current and comprehensive baseline inventory of hardware, software, and firmware is documented, backed up, and protected. Information system documentation describes security controls in sufficient detail to permit analysis and testing of controls. For Federal entities, baseline meets minimum configuration management standards as required by NIST standards and OMB.	Request an inventory of all computer assets and determine if the inventory is accurate, complete, and whether duplicate copies are adequately protected. Select items in the inventory and trace to the asset and verify that the configuration (model, settings, etc.) is accurate. Select assets at the entity and verify that they are accurately recorded in the inventory. (Note: Selections should be focused on areas that are most relevant to the audit.)
	CM-2.1.2. Hardware, software, and firmware are mapped to application it supports.	Determine whether management has mapped the hardware, software and firmware to the application it supports.
	CM-2.1.3. Configuration settings optimize the system's security features.	Determine if key component security settings conform with NIST SP 800-70 and vendor recommendations.

Source: GAO.

Critical Element CM-3. Properly authorize, test, approve, track, and control all configuration changes

An entity should properly control all configuration changes; not only changes made by internal developers but also changes made by external developers or contractors (see SM-7 for activities performed by external third parties). This includes a wide range of activities starting with the establishment of a formal change management process. Management should authorize and approve all configuration changes. Test plan standards should be developed for all levels of testing and test plans should be documented and approved by all responsible parties. Testing should be comprehensive and appropriately consider security and impacts on interfacing systems. An audit trail should be made to clearly document and track the configuration changes. Also, see Section AS-3 for additional business process application level considerations.

Authorizations for system and application software modifications should be documented and maintained. Policies and procedures should be in place that detail who can authorize a modification and how these authorizations are to be documented. Generally, the application users have the primary responsibility for authorizing system changes; however, users should be required to discuss their proposed changes with systems developers to confirm that the change is feasible and cost effective. For this reason, an entity may require a senior systems developer to co-authorize a change. The use of standardized change request forms helps ensure that requests are clearly communicated and approvals are documented. Authorization documentation should be maintained for at least as long as a system is in operation in case questions arise regarding why or when system modifications were made. Authorization documents may be maintained in either paper or electronic form as long as their integrity is protected.

Configuration control activities involve activities that request, evaluate, approve, disapprove, or implement changes to baseline configuration items. Changes encompass both error correction and enhancements. The configuration management plan should identify each level of decision making (for example, CCB[96]) and its level of authority for approving proposed system and application changes and its management of development and production baselines.

The configuration status accounting process records and reports the status of configuration items. The following are minimum data elements to be tracked for a configuration item: (1) its initial approved version, (2) the status of requested changes, and (3) the implementation status of approved changes. The level of detail and specific data required may vary according to the information needs of the project and the customer.

A disciplined process for testing and approving new and modified systems before their implementation is essential to make sure systems hardware and related programs operate as intended and

[96] A configuration control board evaluates and approves or disapproves proposed changes to configuration items and ensures implementation of approved changes.

that no unauthorized changes are introduced. Test plans should appropriately consider security. The extent of testing varies depending on the type of modification. For new systems being developed or major system enhancements, testing will be extensive, generally progressing through a series of test stages that include (1) testing individual program modules (unit testing), (2) testing groups of modules that must work together (integration testing), and (3) testing an entire system (system testing). Minor modifications may require less extensive testing; however, changes should still be carefully controlled and approved since relatively minor program code changes, if performed incorrectly, can have a significant impact on security and overall data reliability.

Once a change has been authorized, it should be implemented, written into the program code, and tested in a disciplined manner. Because testing is an iterative process that is generally performed at several levels, it is important that the entity adhere to a formal set of configuration management procedures or standards for prioritizing, scheduling, testing, and approving changes. These procedures should be described in the entity's configuration management plan and should include requirements for

- ranking and scheduling configuration changes so that authorized change requests are not lost and are implemented efficiently and in accordance with user needs;
- preparing detailed specifications for the configuration change, which are approved by an individual responsible for supervising programming activities to confirm that the specifications correspond to the user's authorized requirements;
- developing a detailed test plan for each modification that defines the levels and types of tests to be performed;
- defining responsibilities for each person involved in testing and approving software (for example, systems analysts, programmers, quality assurance staff, auditors, library control personnel, and users—who should participate in testing and approve test results before implementation), including determining that testing is performed by parties independent of development;

- developing related configuration changes to system documentation, including hardware documentation, operating procedures, and user procedures;
- supervisory review and documented approvals by appropriate personnel, including programming supervisors, database administrators, and other technical personnel before and after testing;
- maintaining controlled libraries of software in different stages of development to ensure that programs being developed or tested are not interchanged with each other or with production software;
- documenting configuration/software changes so that they can be traced from authorization to the final approved code and facilitating "trace-back" of code to design specifications and functional requirements by system testers; and
- obtaining final user acceptance only after testing is successfully completed and reviewed by the user.

To ensure that approved software programs are protected from unauthorized changes or impairment and that different versions are not misidentified, copies should be maintained in carefully controlled libraries. Further, adequately controlled software libraries help ensure that there is (1) a copy of the official approved version of a program available in case the integrity of an installed version is called into question and (2) a permanent historical record of old program versions.

Separate libraries should be established for programs being developed or modified, programs being tested by users, and programs approved for use (production programs). Access to these libraries should be limited and movement of programs and data among them should be controlled.

Inadequately controlled software libraries increase the risk that unauthorized changes could be made either inadvertently or deliberately for fraudulent or malicious purposes. In addition, inadequate controls over programs being developed or modified could make it difficult to determine which version of the program is the most recent. Such an environment can result in inefficiencies

and could lead to interruptions of service and monetary losses. For example,

- an unauthorized program could be substituted for the authorized version;
- test programs could be labeled as production programs;
- two programmers could inadvertently access and work on the same test program version simultaneously, making it difficult or impossible to merge their work; or
- unauthorized changes to either test or production programs could be made and remain undetected.

Copies of software programs should be maintained in libraries where they are labeled, dated, inventoried, and organized in a way that diminishes the risk that programs will be misidentified or lost. Library management software provides an automated means of inventorying software (ensuring that differing versions are not accidentally misidentified) and maintaining a record of software changes. Specifically, such software can be used to

- produce audit trails of program changes and maintain version number control,
- record and report program changes made,
- automatically number program versions,
- identify creation date information,
- maintain copies of previous versions, and
- control concurrent updates so that multiple programmers are prevented from making changes to the same program in an uncontrolled manner.

The movement of programs and data among libraries should be controlled by an entity group or person that is independent of both the user and the programming staff. This group should be responsible for

- moving programs from development/maintenance to user testing and from user testing to production;

- supplying data from the production library for testing and creating test data; and
- controlling different program versions, especially when more than one change is being performed on a program concurrently.

Before transferring a tested program from the user test library to the production library, the independent library control group should (1) generate a report that shows all changed source code (lines added, changed, and deleted) and (2) compare this report to the user request to ensure that only approved changes were made.

Many federal agencies have data processing operations that involve multiple locations and require a coordinated effort for effective and controlled distribution and implementation of new or revised software. For example, an entity may have a central software design, development, and maintenance activity, but have two or more regional data processing centers running the same software. Once a modified software program has been approved for use, the change should be communicated to all affected parties and distributed and implemented in a way that leaves no doubt about when it is to begin affecting processing. To accomplish these objectives, an entity should have and follow established procedures for announcing approved changes and their implementation dates and for making the revised software available to those who need to begin using it.

Source code programs (the code created by programmers) are compiled into object or production code programs that are machine-readable and become the versions that are actually used during data processing. Source code programs should be closely controlled at a central location and compiled into production programs before being distributed. Source code should not be distributed to other locations. This helps protect the source code from unauthorized changes and increases the integrity of the object or production code, which is much more difficult for programmers to change without access to the source code. Inadequately controlling software distribution and implementation increases the risk that data could be improperly processed due to

- implementation of unapproved and possibly malicious software,

- continued use of outdated versions of software, and
- inconsistent implementation dates resulting in inconsistent processing of similar data at different locations.

With independent processing sites, each site is responsible for implementing the correct version of the software at the predetermined date and time and maintaining the documentation authorizing such implementation. Conversely, implementing new software through one or more central computers or servers minimizes the risk that the software will be inconsistently implemented.

The use of public domain and personal software should be restricted. It is important that an entity have clear policies regarding the use of personal and public domain software by employees at work. Allowing employees to use their own software or even diskettes for data storage that have been used elsewhere increases the risk of introducing viruses. It also increases the risk of violating copyright laws and making bad decisions based on incorrect information produced by erroneous software. As mentioned in section CM-5, virus identification software can help contain damage from viruses that may be introduced from unauthorized use of public domain, from personal software, or from corrupted diskettes.

CM-3 Related NIST SP 800-53 Controls
CM-3 Configuration Change Control
SA-2 Allocation of Resources
SA-3 Life Cycle Support
SA-4 Acquisitions
SA-8 Security Engineering Principles
SA-10 Developer Configuration Management
SA-11 Developer Security Testing

Control Techniques and Suggested Audit Procedures for Critical Element CM-3

Table 25. Control Techniques and Suggested Audit Procedures for Critical Element CM-3: Properly authorize, test, approve, and track all configuration changes

Control activities	Control techniques	Audit procedures
CM-3.1. All configuration changes are properly managed (authorized, tested, approved, and tracked).		Where appropriate, these audit procedures should be applied to both internal and external developers and coordinated with section SM-7. (Ensure that activities performed by external third parties are adequately secure.)
	CM-3.1.1. An appropriate formal change management process is documented.	Review the change management methodology for appropriateness. Review system documentation to verify that the change management methodology was followed.
	CM-3.1.2. Configuration changes are authorized by management. Configuration management actions are recorded in sufficient detail so that the content and status of each configuration item is known and previous versions can be recovered.	Review system logs for configuration changes. Determine whether these changes have been properly authorized. Examine a selection of CM and software change request forms for approvals and sufficiency of detail. Interview CM management and software development staff. Review a selection of configuration exceptions identified by the entity in its configuration audit (Refer to CM 4.1) or through other audit procedures to identify any weaknesses in the entity's configuration change process.
	CM-3.1.3. Relevant stakeholders have access to and knowledge of the configuration status of the configuration items.	Interview users and ensure that they have ready access to software change requests, test reports, and configuration items associated with the various baselines being managed.
	CM-3.1.4. Detailed specifications are prepared by the programmer and reviewed by a programming supervisor for system and application software changes.	For the software change requests selected for control activity CM-3.1.2: • review specifications and related documentation for evidence of supervisory review.
	CM-3.1.5. Test plan standards have been developed for all levels of testing that define responsibilities for each party (for example, users, system analysts, programmers, auditors, quality assurance, library control).	Review test plan standards.
	CM-3.1.6. Test plans are documented and approved that define responsibilities for each party involved (for example, users, systems analysts, programmers, auditors, quality assurance, library control).	Perform the following procedures to determine whether control techniques CM-3.1.6 through 3.1.12 are achieved.

Control activities	Control techniques	Audit procedures
	CM-3.1.7. Test plans include appropriate consideration of security.	For the software change requests selected for control activity CM-3.1.2: • review test plans; • compare test documentation with related test plans; • review test transactions and data; • review test results; • review documentation for appropriate supervisory or management reviews; • verify user acceptance; and • review updated documentation. Determine whether operational systems experience a high number of system failures (for example, bends) and, if so, whether they indicate inadequate testing before implementation. Examine a selection of program changes to determine whether they were approved by management prior to being moved to production.
	CM-3.1.8. Unit, integration, and system testing are performed and approved in accordance with the test plan and apply a sufficient range of valid and invalid conditions.	
	CM-3.1.9. A comprehensive set of test transactions and data is developed that represents the various activities and conditions that will be encountered in processing.	
	CM-3.1.10. Live data are not used in testing of program changes, except to build test data files.	
	CM-3.1.11. Test results are documented and appropriate responsive actions are taken based on the results.	
	CM-3.1.12. Program changes are moved into production only when approved by management and by persons independent of the programmer.	
	CM-3.1.13. Standardized procedures are used to distribute new software for implementation.	Examine procedures for distributing new software.
	CM-3.1.14. Appropriate tools (for example, library mgt. software and manual techniques) are used to: • produce audit trails of program changes, • maintain program version numbers, • record and report program changes, • maintain creation/date information for production modules, • maintain copies of previous versions, and • control concurrent updates.	Review pertinent policies and procedures. Interview personnel responsible for appropriate tools and library control. Examine a selection of programs maintained in the library and assess compliance with prescribed procedures. Determine whether documentation is maintained on program changes, program version numbers, creation/date information, and copies of prior versions. Review procedures for controlling concurrent updates. Assess the adequacy of access controls over CM tools (e.g., library management software) to ensure segregation of duties is adequately enforced. (Coordinate with audit procedures in AC 4.1).
	CM-3.1.15. Configuration/software changes are documented so that they can be traced from authorization to the final approved code and they facilitate “trace-back” of code to design specifications and functional requirements by system testers.	For the software change requests selected for control activity CM-3.1.2: • trace changes from authorization to the final approved code; and, • trace changes back from code to design specifications and functional requirements.

Control activities	Control techniques	Audit procedures
	CM-3.1.16. Program development and maintenance, testing, and production programs are maintained separately (for example, libraries) and movement between these areas is appropriately controlled, including appropriate consideration of segregation of duties (see the Segregation of Duties control category.	Review pertinent policies and procedures and interview library control personnel. Examine libraries in use. Test access to each program library (e.g., development, test, production) by examining security system parameters. Review program changes procedures for adherence to appropriate segregation of duties between application programming and movement of programs into production. For a selection of program changes, examine related documentation to verify that (1) procedures for authorizing movement among libraries were followed and (2) before and after images were compared to ensure that unauthorized changes were not made to the programs.
	CM-3.1.17. Access to all programs, including production code, source code, and extra program copies, are adequately protected.	For critical software production programs, determine whether access control software rules are clearly defined. Test access to program libraries by examining security system parameters.
	CM-3.1.18. Configuration changes to network devices (for example, routers and firewalls) are properly controlled and documented.	Review a selection of configuration settings to key devices and determine if configuration changes are adequately controlled and documented.
	CM-3.1.19. Clear policies restricting the use of personal and public domain software and prohibiting violations of software licensing agreements have been developed and are enforced.	Review pertinent policies and procedures. Interview users and data processing staff. Review and test management enforcement process.

Source: GAO.

Critical Element CM-4. Routinely monitor the configuration

Current configuration information should be routinely monitored for accuracy. Monitoring should address the current baseline and operational configuration of the hardware, software, and firmware that comprise the information system. Information technology products should comply with applicable standards and the vendors' good security practices. The entity should have the capability to monitor and test that it is functioning as intended. Also, networks should be appropriately configured and monitored to adequately protect access paths between information systems.

Monitoring, sometimes called configuration audits, should be periodically conducted to determine the extent to which the actual configuration item reflects the required physical and functional characteristics originally specified by requirements. The configuration plan should identify the frequency of configuration audits. A configuration audit should be performed on a configuration item before its release and it should be routinely tested thereafter. Configuration audits establish that the functional and performance requirements defined in the configuration documentation have been achieved by the design and that the design has been accurately documented in the configuration document. The purpose and benefits of the process include the following:

- Ensures that the product design provides the agreed-to performance capabilities
- Validates the integrity of the configuration documentation
- Verifies the consistency between a product and its configuration documentation
- Determines that an adequate process is in place to provide continuing control of the configuration
- Provides confidence in establishing a product baseline
- Ensures a known configuration as the basis for operation and maintenance instructions, and training.

Security settings for network devices, operating systems, and infrastructure applications need to be monitored periodically to ensure that they have not been altered and that they are set in the most restrictive mode consistent with the information system operational requirements. NIST SP 800-70 provides guidance on configuration settings (for example, checklists) for information technology products.

A process and related procedures needs to be established to document the results from monitoring configuration items and ensure that discrepancies are properly corrected. For example, network and host environments should be scanned on a regular basis to determine whether patches have been effectively applied. A formal process with central management helps to ensure patch

compliance with the network configuration. Audit results need to be recorded indicating

- each discrete requirement,
- method of verification,
- verification procedures,
- verification results, and
- corrective actions.

CM-4 Related NIST SP 800-53 Controls
CM-4 Monitoring Configuration Changes
CM-5 Access Restrictions for Change
SI-7 Software and Information Integrity

Control Techniques and Suggested Audit Procedures for Critical Element CM-4

Table 26. Control Techniques and Suggested Audit Procedures for Critical Element CM-4: Routinely monitor the configuration

Control activities	Control techniques	Audit procedures
CM-4.1. The configuration is routinely audited and verified.	CM-4.1.1. Routinely validate that the current configuration information is accurate, up-to-date, and working as intended for networks, operating systems, and infrastructure applications.	Identify the standards and procedures used to audit and verify the system configuration. Determine when and how often the configuration is verified and audited. Review a selection of the configuration verifications and audits for compliance with applicable standards. Verify that vendor-supplied system software is still supported by the vendor. Evaluate adequacy of the configuration audits based on the results of the IS control audit tests performed.
	CM-4.1.2. The verification and validation criteria for the configuration audit is appropriate and specifies how the configuration item will be evaluated in terms of correctness, consistency, necessity, completeness, and performance.	Review evaluation criteria for selected releases to determine whether verification and validation criteria for the configuration audit addresses the correctness, consistency, necessity, completeness, and performance of the configuration items. Identify all configuration items, deviations and waivers, and the status of tests. Determine if configuration items have gaps in the documentation or if there are defects in the change management process.

Control activities	Control techniques	Audit procedures
	CM-4.1.3. Confirm compliance with applicable configuration management policy, plans, standards, and procedures.	Compare configuration policy, plans, standards, and procedures with observations.
	CM-4.1.4. The information system periodically verifies the correct operation of security functions—on system start up and restart, on command by user with appropriate privilege—(providing system audit trail documentation) and takes appropriate action (for example, notifies system administrator, shuts the system down, restarts the system) when anomalies are discovered.	Interview officials and review related system documentation. Observe or test this system capability to determine that procedures are followed and related system documentation is generated and reviewed by entity security staff.

Source: GAO.

Critical Element CM-5. Update software on a timely basis to protect against known vulnerabilities

Software should be scanned and updated frequently to guard against known vulnerabilities. In addition to periodically looking for software vulnerabilities and fixing them, security software should be kept current by establishing effective programs for patch management, virus protection, and other emerging threats. Also, software releases should be adequately controlled to prevent the use of noncurrent software.

Vulnerability scanning

Using appropriate vulnerability scanning tools and techniques, entity management should scan for vulnerabilities in the information system or when significant new vulnerabilities affecting the system are identified and reported. Audit procedures include review of the scanning methodology and related results to ensure that significant vulnerabilities are remediated in a timely manner. (See section SM-5.1, table 9, for a description of vulnerability scanning.)

Patch management[97]

Patch management is a critical process used to help alleviate many of the challenges involved with securing computing systems from attack. A component of configuration management, it includes acquiring, testing, applying, and monitoring patches to a computer system. Flaws in software code that could cause a program to malfunction generally result from programming errors that occur during software development. The increasing complexity and size of software programs contribute to the growth in software flaws. While most flaws do not create security vulnerabilities, the potential for these errors reflects the difficulty and complexity involved in delivering trustworthy code.

The federal government has taken several steps to address security vulnerabilities that affect entity systems, including efforts to improve patch management. For example, OMB FISMA reporting instructions have indicated that maintaining up-to-date patches is part of FISMA's system configuration management requirements. Also, the US-CERT is intended to aggregate and disseminate cybersecurity information to improve warning and response to incidents, increase coordination of response information, reduce vulnerabilities, and enhance prevention and protection. Services include notification of software vulnerabilities and information on applicable patches.

Common patch management practices in security-related literature from several groups, including NIST, Microsoft, patch management software vendors, and other computer security experts include the following elements:

- centralized patch management support and clearly assigned responsibilities;
- senior executive support and assurance that appropriate patches are deployed;

[97]Patch management is the process of applying software patches to correct flaws. A patch is a piece of software code that is inserted into a program to temporarily fix a defect. Patches are developed and released by software vendors when vulnerabilities are discovered.

- standardized patch management policies, procedures, and tools;
- skills, knowledge, and training to perform patch management responsibilities;
- current technology inventory of all hardware, software, and services that are used;
- risk assessment based on the criticality of the vulnerability and importance of the system;
- thorough testing before the patch is applied in a production environment;
- monitoring through network and host vulnerability scanning; and
- timely notification of relevant vulnerabilities and distribution of critical patches.

Virus protection

Protecting information systems from malicious computer viruses and worms[98] is a serious challenge. Computer attack tools and techniques are becoming increasingly sophisticated; viruses are spreading faster as a result of the increasing connectivity of today's networks; commercial-off-the-shelf products can be easily exploited for attack by all their users; and there is no "silver bullet" solution such as firewalls or encryption to protect systems. To combat viruses and worms specifically, entities should take steps such as ensuring that security personnel are adequately trained to respond to early warnings of attacks and keeping antivirus programs up-to-date. Strengthening intrusion detection capabilities and effective patch management programs also help.

According to NIST, the information system (including servers, workstations, and mobile computing devices) should implement malicious code protection that includes a capability for automatic updates. Virus definitions should be kept up-to-date. Virus-scanning software should be provided at critical entry points, such as remote-access servers and at each desktop system on the network. Anti-

[98]Worms propagate through networks; viruses destroy files and replicate by manipulating files.

viral mechanisms should be used to detect and eradicate viruses in incoming and outgoing e-mail and attachments.

Emerging threats

Entities are facing a set of emerging cybersecurity threats that are the result of changing sources of attack, increasingly sophisticated social engineering techniques designed to trick the unsuspecting user into divulging sensitive information, new modes of covert compromise, and the blending of once distinct attacks into more complex and damaging exploits. Advances in antispam measures have caused spammers to increase the sophistication of their techniques to bypass detection; the frequency and sophistication of phishing[99] attacks have likewise increased, and spyware[100] has proven to be difficult to detect and remove.

The risks that entities face are significant. Spam consumes employee and technical resources and can be used as a delivery mechanism for malware[101] and other cyberthreats. Entities and their employees can be victims of phishing scams, and spyware puts the confidentiality, integrity, and availability of entity systems at serious risk. Other emerging threats include the increased sophistication of worms, viruses, and other malware, and the increased attack capabilities of blended threats and botnets.[102]

The transition to the new Internet protocol version 6 (IPv6) creates new security risks. The Internet protocol provides the addressing mechanism that defines how and where information moves across

[99]Phishing is tricking individuals into disclosing sensitive personal information through deceptive computer-based means.

[100]Spyware is software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.

[101]Malware (malicious software) is defined as programs that are designed to carry out annoying or harmful actions. They often masquerade as useful programs or are embedded into useful programs so that users are induced into activating them. Malware can include viruses, worms, and spyware (GAO-05-231).

[102]Botnets are compromised computers that can be remotely controlled by attackers to automatically launch attacks. Bots (short for robots) have become a key automation tool to speed the infection of vulnerable systems (GAO-05-231).

interconnected networks. The key characteristics of IPv6 are designed to increase address space, promote flexibility and functionality, and enhance security. However, as IPv6-capable software and devices accumulate in entity networks, they could be abused by attackers if not managed properly. Specifically, some existing firewalls and intrusion detection systems do not provide IPv6 detection or filtering capability, and malicious users might be able to send IPv6 traffic through these security devices undetected. Configuration management can mitigate this threat by tightening firewalls to deny direct outbound connections and tuning intrusion detection systems to detect IPv6 traffic.

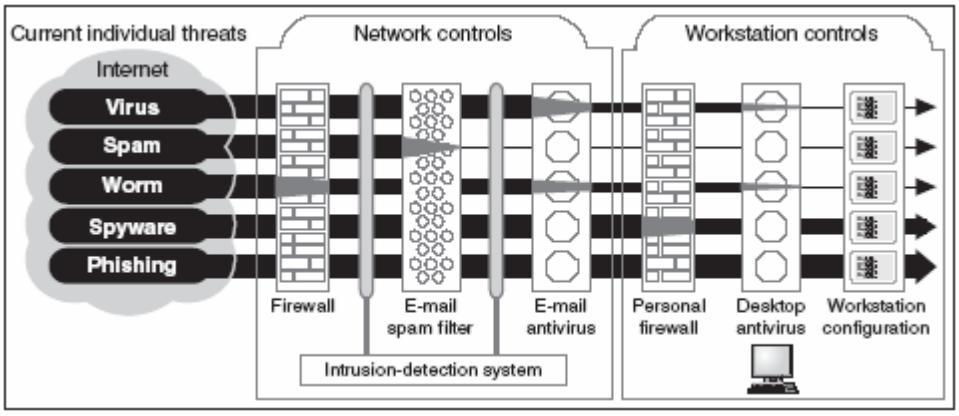
Voice over Internet Protocol (VoIP) technologies may also cause damage to the information system if used maliciously. Because of the integration of voice and data in a single network, establishing a secure VoIP and data network is a complex process that requires greater effort than that required for data-only networks. For example, typical firewall security configurations need to be reexamined when VoIP systems are implemented because of operational aspects required by this type of system that may in turn reduce the effectiveness of normally applied firewall security configurations. To mitigate this threat, the entity should establish usage restrictions and implementation guidance for VoIP, and document and control the use of VoIP. In addition, monitor and review procedures should be established to ensure security effectiveness. NIST SP 800-58 provides guidance on security considerations for VOIP technologies employed in information systems.

An effective security program can assist in entity efforts to mitigate and respond to these emerging cybersecurity threats. First of all, the risks of emerging cybersecurity threats should be addressed as part of required entitywide information security programs, which include performing periodic assessments of risk. Secondly, security controls commensurate with the identified risk should be implemented. Thirdly, ensuring security awareness training for entity personnel is critical. Comprehensive procedures for detecting, reporting, and responding to security incidents should be implemented. An effective security program, related control techniques, and proposed

audit procedures are discussed in the security management section of FISCAM.

As part of the entity security program, effective configuration of layered security (Defense-in-Depth) mitigates the risks from individual cybersecurity threats. Layered security implemented within an entity's security architecture includes the use of strong passwords, patch management, antivirus software, firewalls, software security settings, backup files, vulnerability assessments, and intrusion detection systems. Figure 5 depicts an example of how entities can use layered security controls to mitigate the risks of individual cybersecurity threats.

Figure 5. Layered Security Mitigates the Risk of Individual Cybersecurity Threats



Source: GAO.

Note: Excerpt from GAO, *Cybersecurity Issues Threaten Federal Information Systems*, GAO-05-231 (Washington, D.C.: May 2005).

Noncurrent software

Procedures should ensure that only current software releases are installed in information systems. Noncurrent software may be vulnerable to malicious code such as viruses and worms.

As mentioned previously under CM-3, many federal agencies have data processing operations that involve multiple locations and require a coordinated effort for effective and controlled distribution and implementation of new or revised software. This can include virus protection software and operating system patches. Once a modified software program has been approved for use, the change

should be communicated to all affected parties and distributed and implemented in a way that leaves no doubt about when it is to begin affecting processing. Inadequately controlling virus software distribution and system patches increases the risk that data could be improperly processed or lose its confidentiality due to computer viruses and hackers breaking into the database.

Software usage

Policies and procedures should be implemented to reasonably assure that the entity complies with software usage restrictions. In addition, the entity should have policies and procedures implemented that address the installation of software by users and procedures to determine that such policies and procedures are adhered to. In addition, policies and procedures should be implemented to address the use of collaborative web technologies and peer-to-peer file sharing[103]. This may include, for example, procedures for reviewing firewall rules to ensure compliance with the entity's policies for using these techniques.

CM-5 Related NIST SP 800-53 Controls	
RA-5	Vulnerability Scanning
SA-6	Software Usage Restrictions
SA-7	User Installed Software
SC-19	Voice Over Internet Protocol
SI-2	Flaw Remediation
SI-3	Malicious Code Protection
SI-5	Security Alerts and Advisories
SI-8	Spam Protection

[103]Peer-to-peer file sharing refers to providing and receiving files over a network, where files are stored on and served by workstations and involves both downloading and uploading of files.

Control Techniques and Suggested Audit Procedures for Critical Element CM-5

Table 27. Control Techniques and Suggested Audit Procedures for Critical Element CM-5: Update software on a timely basis to protect against known vulnerabilities

Control activities	Control techniques	Audit procedures
CM-5.1. Software is promptly updated to protect against known vulnerabilities.	CM-5.1.1. Information systems are scanned periodically to detect known vulnerabilities.	Interview entity officials. Identify the criteria and methodology used for scanning, tools used, frequency, recent scanning results, and related corrective actions. Coordinate this work with the AC section.
	CM-5.1.2. An effective patch management process is documented and implemented, including: • identification of systems affected by recently announced software vulnerabilities; • prioritization of patches based on system configuration and risk; • appropriate installation of patches on a timely basis, including testing for effectiveness and potential side effects on the entity's systems; and • verification that patches, service packs, and hotfixes were appropriately installed on affected systems.	Review pertinent policies and procedures. Interview users and data processing staff.
	CM-5.1.3. Software is up-to-date; the latest versions of software patches are installed.	Compare vendor recommended patches to those installed on the system. If patches are not up-to-date, determine why they have not been installed.
	CM-5.1.4. An effective virus, spam, and spyware protection process is documented and implemented, including: • appropriate policies and procedures; • effective protection software is installed that identifies and isolates suspected viruses, spam, and spyware; and • virus, spam, and spyware definitions are up-to-date.	Review pertinent policies and procedures. Interview users and data processing staff. Verify that actual software is installed and up-to-date.
	CM-5.1.5. The entity: (1) establishes usage restrictions and implementation guidance for IPv6 technology based on the potential to cause damage to the information system if used maliciously and (2) documents, monitors, and controls the use of IPv6 within the information system. Appropriate organizational officials authorize the use of IPv6.	Review policies and procedures for IPv6. Determine if known security vulnerabilities are mitigated by appropriate protective measures.
	CM-5.1.6. The entity: (1) establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously and (2) documents, monitors, and controls the use of VoIP within the information system. Appropriate organizational officials authorize the use of VoIP.	Review policies and procedures for VoIP. Determine if security considerations in NIST SP 800-58 are used in the information system.
	CM-5.1.7. Noncurrent software releases are adequately secure, given the risk.	Review pertinent policies and procedures. Interview users and data processing staff.

Control activities	Control techniques	Audit procedures
	CM-5.1.8. Appropriate software usage controls (software restrictions, user-installed software) are implemented and exceptions are identified.	Assess the adequacy of software usage controls.

Source: GAO.

Critical Element CM-6. Appropriately document and approve emergency changes to the configuration

Emergency changes to the information system should be documented and approved by appropriate entity officials, either before the change or after the fact. In addition, appropriate personnel should be notified to provide analysis and follow-up.

It is not uncommon for program changes to be needed on an emergency basis to keep a system operating. Some applications, such as payroll processing, are performed in cycles that must be completed by a deadline. Other systems must be continuously available so that the operations they support are not interrupted. In these cases, the risk of missing a deadline or disrupting operations may pose a greater risk than that of temporarily suspending program change controls. However, because of the increased risk that errors or other unauthorized modifications could be implemented, emergency changes should be kept to a minimum.

It is important that an entity follow established procedures to perform emergency software changes and reduce the risk of suspending or abbreviating normal controls. Generally, emergency procedures should specify

- when emergency software changes are warranted,
- who may authorize emergency changes,
- how emergency changes are to be documented, and
- within what period after implementation the change must be tested and approved.

Making emergency changes often involves using sensitive system utilities or access methods that grant much broader access than would normally be needed. It is important that such access is strictly controlled and that their use be promptly reviewed.

Shortly after an emergency change is made, the usual configuration management controls should be applied retroactively. That is, the change should be subjected to the same review, testing, and approval process that apply to scheduled changes. In addition, logs of emergency changes and related documentation should be periodically reviewed by data center management or security administrators to determine whether all such changes have been tested and have received final approval.

CM-6 Related NIST SP 800-53 Controls
CM-3 Configuration Change Control

Control Techniques and Suggested Audit Procedures for Critical Element CM-6

Table 28. Control Techniques and Suggested Audit Procedures for Critical Element CM-6: Appropriately document and approve emergency changes to the configuration

Control activities	Control techniques	Audit procedures
CM-6.1. Adequate procedures for emergency changes are documented and implemented.	CM-6.1.1. Appropriately document and implement procedures for emergency changes.	Review procedures to determine whether they adequately address emergency change requirements.
CM-6.2. Emergency changes to the configuration are documented and approved.	CM-6.2.1. Appropriately document and approve emergency changes to the configuration and notify appropriate personnel for analysis and follow-up.	For a selection of emergency changes recorded in the emergency change log, review related documentation and approval.

Source: GAO.

3.4. Segregation of Duties (SD)

Effective segregation of duties starts with effective entitywide policies and procedures that are implemented at the system and application levels. Work responsibilities should be segregated so that one individual does not control all critical stages of a process. For example, while users may authorize program changes, programmers should not be allowed to do so because they are not the owners of the system and do not have the responsibility to see that the system meets user needs. Similarly, one computer programmer should not be allowed to independently write, test, and approve program changes. Often, segregation of duties is achieved by splitting responsibilities between two or more organizational groups. Dividing duties this way diminishes the likelihood that errors and wrongful acts will go undetected because the activities of one group or individual will serve as a check on the activities of the other.

Inadequately segregated duties, conversely, increase the risk that erroneous or fraudulent transactions could be processed, that improper program changes could be implemented, and that computer resources could be damaged or destroyed. For example:

- An individual who is independently responsible for authorizing, processing, and reviewing payroll transactions could inappropriately increase payments to selected individuals without detection.
- A computer programmer responsible for authorizing, writing, testing, and distributing program modifications could either inadvertently or deliberately implement computer programs that did not process transactions in accordance with management's policies or that included malicious code.

The extent to which duties are segregated depends on the size of the entity and the risk associated with its facilities and activities. A large entity will have more flexibility in separating key duties than will a small entity that must depend on only a few individuals to perform its operations. These smaller entities may rely more extensively on supervisory review to control activities. Similarly, activities that

involve extremely large dollar transactions or are otherwise inherently risky should be divided among several individuals and be subject to relatively extensive supervisory review.

Key areas of concern during a general controls review involve the segregation of duties among major operating and programming activities, including duties performed by users, application programmers, and data center staff. For example, where possible, the following types of activities should be separated: development versus production, security versus audit, accounts payable versus accounts receivable, and encryption key management versus the changing of keys. Entitywide policies outlining the responsibilities of groups and related individuals pertaining to incompatible activities should be documented, communicated, and enforced.

Because of the nature of computer operations, segregation of duties alone will not ensure that personnel perform only authorized activities, especially computer operators. Preventing or detecting unauthorized or erroneous personnel actions requires effective supervision and review by management and formal operating procedures.

Determining whether duties are adequately segregated and that the activities of personnel are adequately controlled involves assessing the entity's efforts in performing each of the critical elements listed in table 29.

SD Related NIST SP 800-53 Controls	
AC-5	Separation of Duties
PS-2	Position Categorization
PS-6	Access Agreements

Table 29. Critical Elements for Segregation of Duties

Number	Description
SD-1.	Segregate incompatible duties and establish related policies
SD-2.	Control personnel activities through formal operating procedures, supervision, and review

Source: GAO

Critical Element SD-1. Segregate incompatible duties and establish related policies

The first steps in determining if duties are appropriately segregated are to analyze the entity's operations, identify incompatible duties, and assign these duties to different organizational units or individuals. Federal internal control standards specify that key duties and responsibilities for authorizing, processing, recording, and reviewing transactions should be separated. This concept can also be applied to the authorization, testing, and review of computer program changes.

Segregating duties begins by establishing independent organizational groups with defined functions, such as a payroll unit responsible for preparing payroll transaction input and a data processing unit responsible for processing input prepared by other units. Functions and related tasks performed by each unit should be documented for the unit and written in job descriptions and should be clearly communicated to personnel assigned the responsibilities.

Both physical and logical access controls can be used to enforce many entity policies regarding segregation of duties and should be based on organizational and individual job responsibilities. (Access control is discussed in detail in section 3.2.) For example, logical access controls can preclude computer programmers from using applications software or accessing computerized data associated with applications. Similarly, physical access controls, such as key cards and a security guard, can be used to prevent unauthorized individuals from entering a data processing center.

SD-1.1. Incompatible duties have been identified and policies implemented to segregate these duties

Management should have analyzed operations and identified incompatible duties that are then segregated through policies and

organizational divisions. Although incompatible duties may vary from one entity to another, the following functions are generally performed by different individuals: information security management, systems design, applications programming, systems programming, quality assurance and testing, library management/ change management, computer operations, production control and scheduling, data security, data administration, network administration, and configuration management. A brief description of these functions follows.

Information security management includes the personnel who direct or manage the activities and staff of the information security department and its various organizational components.

Systems design is the function of identifying and understanding user information needs and translating them into a requirements document that is used to build a system.

Applications programming involves the development and maintenance of programs for specific applications, such as payroll, inventory control, accounting, and mission support systems.

Systems programming involves the development and maintenance of programs that form the system software, such as operating systems, utilities, compilers, and security software.

Quality assurance/testing involves the review and testing of newly-developed systems and modifications to determine whether they function as specified and perform in accordance with functional specifications. Testing may also determine whether appropriate procedures, controls, and documentation have been developed and implemented before approval is granted to place the system into operation.

Library management/change management is the control over program and data files that are either kept on-line or are on tapes and disks that are loaded onto the computer as needed. Software programs are generally used to assist in management of these files. This function also is often responsible for controlling

documentation related to system software, application programs, and computer operations.

Computer operations involves performing the various tasks to operate the computer and peripheral equipment, including providing the tape, disk, or paper resources as requested by the applications systems.

Production control and scheduling involves monitoring the information into, through, and as it leaves the computer operations area, and for determining the succession of programs to be run on the computer. Often, an automated scheduling package is used in this task. An entity may have a separate data control group that is responsible for seeing that all data necessary for processing are present and that all output is complete and distributed properly. This group is usually also responsible for reconciling record counts and control totals submitted by users with similar counts and totals generated during processing.

The data security function in an IT department involves the development and administration of an entity's information security program. This includes development of security policies, procedures, and guidelines and the establishment and maintenance of a security awareness and education program for employees. This function is also concerned with the adequacy of access controls and service continuity procedures.

Data administration involves planning for and administering the data used throughout the entity. This function is concerned with identifying, cataloging, controlling, and coordinating the information needs of the entity. Database administration is a narrower function concerned with the technical aspects of installing, maintaining, and using an entity's databases and database management systems.

Network administration involves maintaining a secure and reliable on-line communications network and serving as liaison with user departments to resolve network needs and problems.

Configuration management involves controlling and documenting changes made to a system's hardware, software, firmware, and

documentation throughout the development and operational life of the system.

The following include examples of restrictions that are generally addressed in policies about segregating duties and are achieved through organizational divisions and access controls:

- Application users should not have access to operating systems or applications software.
- Programmers should not be responsible for moving programs into production or have access to production libraries or data.
- Access to operating system documentation should be restricted to authorized systems programming personnel.
- Access to applications system documentation should be restricted to authorized applications programming personnel.
- Access to production software libraries should be restricted to library management personnel.
- Persons other than computer operators should not set up or operate the production computer.
- Only users—not computer staff—should be responsible for transaction origination or correction and for initiating changes to application files.
- Computer operators should not have access to program libraries or data files.

Some steps involved in processing a transaction also need to be separated among different individuals. For example, the following combinations of functions should not be performed by a single individual:

- Data entry and verification of data.
- Data entry and its reconciliation to output.
- Input of transactions for incompatible processing functions (for example, input of vendor invoices and purchasing and receiving information).
- Data entry and supervisory authorization functions (for example, authorizing a rejected transaction to continue processing that exceeds some limit requiring a supervisor's review and approval).

Organizations with limited resources to segregate duties should have compensating controls, such as supervisory review of transactions performed.

SD-1.2. Job descriptions have been documented

Documented job descriptions should exist that clearly describe employee duties and prohibited activities. These should include responsibilities that may be assumed during emergency situations. The documented job descriptions should match employees' assigned duties. Also, they should include definitions of the technical knowledge, skills, and abilities required for successful performance in the relevant position, and should be useful for hiring, promoting, and performance evaluation purposes. In addition, the organization should assign a risk designation to all positions and establish screening criteria for individuals filling those positions.

SD-1.3. Employees understand their duties and responsibilities

Employees and their supervisors should understand their responsibilities and the activities that are prohibited. Ultimate responsibility for this rests with senior managers. They should provide the resources and training so that employees understand their responsibilities and ensure that segregation-of-duties principles are established, enforced, and institutionalized within the organization.

Control Techniques and Suggested Audit Procedures for Critical Element SD-1

Table 30. Control Techniques and Suggested Audit Procedures for Critical Element SD-1: Segregate incompatible duties and establish related policies

Control activities	Control techniques	Audit procedures
SD-1.1. Incompatible duties have been identified and policies implemented to segregate these duties.	SD-1.1.1. Policies and procedures for segregating duties exist and are up-to-date.	Review pertinent policies and procedures. Interview selected management and information security personnel regarding segregation of duties.

Control activities	Control techniques	Audit procedures
	SD-1.1.2. Distinct system support functions where possible are performed by different individuals, including the following: • information security management • systems design • applications programming • systems programming • quality assurance/testing • library management/change management • computer operations • production control and scheduling • data control • data security • data administration • network administration • configuration management	Review an entity organization chart showing information security functions and assigned personnel. Interview selected personnel and determine whether functions are appropriately segregated. Determine whether the chart is current and each function is staffed by different individuals. Review relevant alternate or back up assignments and determine whether the proper segregation of duties is maintained. Observe activities of personnel to determine the nature and extent of the compliance with the intended segregation of duties.
	SD-1.1.3. No individual has complete control over incompatible transaction processing functions. Specifically, the following combination of functions are not performed by a single individual: • data entry and verification of data • data entry and its reconciliation to output • input of transactions for incompatible processing functions (for example, input of vendor invoices and purchasing and receiving information) • data entry and supervisory authorization functions (for example, authorizing a rejected transaction to continue processing that exceeds some limit requiring a supervisor's review and approval)	Review the organizational chart and interview personnel to determine that assignments do not result in a single person being responsible for the indicated combinations of functions. Observe activities of personnel to determine the nature and extent of the compliance with the intended segregation of duties.
	SD-1.1.4. Organizations with limited resources to segregate duties have compensating controls, such as supervisory review of transactions performed.	Interview management, observe activities, and test transactions. Note: Perform this in conjunction with SD-2.2.
	SD-1.1.5. Data processing personnel are not users of information systems. They and security managers do not initiate, input, or correct transactions.	Determine through interview and observation whether data processing personnel and security managers are prohibited from these activities.
	SD-1.1.6. Day-to-day operating procedures for the data center are adequately documented and prohibited actions are identified.	Review the adequacy of documented operating procedures for the data center.
	SD-1.1.7. Access controls enforce segregation of duties.	Audit procedures are found in section AC-3.1, but this item is listed here as a reminder. Logical and physical access controls should enforce segregation of duties.

Control activities	Control techniques	Audit procedures
SD-1.2. Job descriptions have been documented.	SD-1.2.1. Documented job descriptions accurately reflect assigned duties and responsibilities and segregation of duty principles.	Review job descriptions for several positions in organizational units and for user security administrators. Determine whether duties are clearly described and prohibited activities are addressed. Review the effective dates of the position descriptions and determine whether they are current. Compare these descriptions with the current responsibilities and duties of the incumbents in these positions to determine the accuracy of these statements.
	SD-1.2.2. Documented job descriptions include definitions of the technical knowledge, skills, and abilities required for successful performance in the relevant position and can be used for hiring, promoting, and performance evaluation purposes.	Review job descriptions and interview management personnel to determine if all job positions have documented technical knowledge, skills, and ability requirements that can be used for hiring, promoting, and performance evaluations.
SD-1.3. Employees understand their duties and responsibilities.	SD-1.3.1. All employees fully understand their duties and responsibilities and carry out those responsibilities in accordance to their job descriptions.	Interview personnel filling positions for the selected job descriptions (see SD-1.2). Determine if the descriptions match their understanding of their duties and responsibilities and whether additional duties are undertaken that are not listed in their job descriptions.
	SD-1.3.2. Senior management is responsible for providing adequate resources and training to ensure that segregation of duty principles are understood and established, enforced, and institutionalized within the organization.	Determine from interviewing personnel whether senior management has provided adequate resources and training to establish, enforce, and institutionalize the principles of segregation of duties.
	SD-1.3.3. Responsibilities for restricting access by job positions in key operating and programming activities are clearly defined, understood, and followed.	Interview management personnel in these activities.

Source: GAO.

Critical Element SD-2. Control personnel activities through formal operating procedures, supervision, and review

Control over personnel activities requires formal operating procedures and active supervision and review of these activities. This is especially relevant for computer operators and system administrators. Some information system officials have extensive access rights in order to keep the systems running efficiently so their activities need to be monitored closely. Inadequacies in this

area could allow mistakes to occur and go undetected and facilitate unauthorized use of the computer.

SD-2.1. Formal procedures guide personnel in performing their duties

Detailed, written instructions should be followed to guide personnel in performing their duties. These instructions are especially important for computer operators. For example, computer operator instruction manuals should provide guidance on system start up and shut down procedures, emergency procedures, system and job status reporting, and operator-prohibited activities. Application-specific manuals (commonly called run manuals) should provide additional instructions for operators specific to each application, such as instructions on job setup, console and error messages, job checkpoints, and restart and recovery steps after system failures. Operators should be prevented from overriding file label or equipment error messages.

SD-2.2. Active supervision and review are provided for all personnel

Supervision and review of personnel computer systems activities help make certain that these activities are performed in accordance with prescribed procedures, that mistakes are corrected, and that the computer is used only for authorized purposes. To aid in this oversight, all user activities on the computer system should be recorded on activity logs, which serve as an audit trail. Supervisors should routinely review these activity logs for incompatible actions and investigate any abnormalities.

Periodic management reviews of computer systems activities are essential to ensure that employees are performing their duties in accordance with established policies and to identify the need to update policies when operational processes change. In particular, management should periodically review activities that cannot be controlled by physical or logical access controls. Such activities are typically controlled instead by supervisory oversight and documentation showing approvals and authorizations.

Control Techniques and Suggested Audit Procedures for Critical Element SD-2

Table 31. Control Techniques and Suggested Audit Procedures for Critical Element SD-2: Control personnel activities through formal operating procedures, supervision, and review

Control activities	Control techniques	Audit procedures
SD-2.1. Formal procedures guide personnel in performing their duties.	SD-2.1.1. Detailed, written instructions exist and are followed for the performance of work.	Perform the following procedures for SD-2.1.1 to SD-2.1.3.
	SD-2.1.2. Instruction manuals provide guidance on system operation.	Review manuals to determine whether formal procedures exist to guide personnel in performing their work.
	SD-2.1.3. Application run manuals provide instruction on operating specific applications.	Interview supervisors and personnel. Observe processing activities.
SD-2.2. Active supervision and review are provided for all personnel.	SD-2.2.1. Personnel are provided adequate supervision and review, including each shift for computer operations.	Interview supervisors and personnel. Observe processing activities.
	SD-2.2.2. Access authorizations are periodically reviewed for incompatible functions.	Review a selection of access authorizations for incompatible functions and evidence of supervisory review.
	SD-2.2.3. Management reviews are performed to determine that control techniques for segregating incompatible duties are functioning as intended and that the control techniques in place are maintaining risks within acceptable levels (for example, periodic risk assessments).	Determine which reviews are conducted to assess the adequacy of duty segregation. Obtain and review results of such reviews. Note: This audit step should be performed in conjunction with audit steps in critical elements SM-2 (Periodically assess and validate risks) and SM-5 (Monitor the effectiveness of the security program).
	SD-2.2.4. Staff performance is monitored on a periodic basis and controlled to ensure that objectives laid out in job descriptions are carried out.	Interview management and subordinate personnel. Select documents or actions requiring supervisory review and approval for evidence of such performance (for example, approval of input of transactions, software changes).
	SD-2.2.5. Supervisors routinely review user activity logs for incompatible actions and investigate any abnormalities.	Interview supervisors and review user activity logs for incompatible actions. Check for evidence of supervisory review.

Source: GAO.

3.5. Contingency Planning (CP)

Losing the capability to process, retrieve, and protect electronically maintained information can significantly affect an entity's ability to accomplish its mission. If contingency planning controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information. For some operations, such as those involving health care or safety, system interruptions could even result in injuries or loss of life.

Given these severe implications, it is critical that an entity have in place (1) procedures for protecting information resources and minimizing the risk of unplanned interruptions and (2) a plan to recover critical operations should interruptions occur. Such plans should consider the activities performed at general support facilities, such as data processing centers and telecommunications facilities, as well as those performed by users of specific applications. To determine whether recovery plans will work as intended, they should be tested periodically in disaster-simulation exercises. FISMA requires that each federal agency implement an information security program that includes "plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency."

Although often referred to as disaster recovery or contingency plans, controls to ensure service continuity should address the entire range of potential disruptions. These may include relatively minor interruptions, such as temporary power failures, as well as major disasters, such as fires, natural disasters, and terrorism, that would require reestablishing operations at a remote location; it might also include errors, such as writing over a file. If controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data.

To mitigate service interruptions, it is essential that the related controls be understood and supported by management and staff throughout the entity. Senior management commitment is especially important to ensuring that adequate resources are devoted to

emergency planning, training, and related testing. Also, the involvement of data and process owners is integral to contingency planning, as they have first-hand knowledge of their data and processes and of the impact of a loss of availability. In addition, all staff with contingency planning responsibilities, such as those responsible for backing up files, should be fully aware of the risks of not fulfilling those duties.

Assessing contingency planning controls involves evaluating the entity's performance in each of the critical elements listed in table 32.

Table 32. Critical Elements for Contingency Planning

Number	Description
CP-1.	Assess the criticality and sensitivity of computerized operations and identify supporting resources
CP-2.	Take steps to prevent and minimize potential damage and interruption
CP-3.	Develop and document a comprehensive contingency plan
CP-4.	Periodically test the contingency plan and adjust it as appropriate

Source: GAO

Critical Element CP-1. Assess the criticality and sensitivity of computerized operations and identify supporting resources

At most entities, the continuity of certain automated operations is more important than for other operations, and it is not cost effective to provide the same level of continuity for all operations. For this reason, it is important that management analyze data and operations to determine which are the most critical and what resources are needed to recover and support them. This is the first step in determining which resources merit the greatest protection and what contingency plans need to be made.

As explained in SM-2, FISMA required NIST to develop standards and guidelines for agencies to use in categorizing federal information and information systems so agencies can provide the appropriate level of information security according to a range of risks. This information is useful in assessing risks and the criticality and sensitivity of computerized operations, and in identifying

supporting resources. It is also very important to link this information to the entity's mission and critical business processes.

According to NIST, the definition of an organization's critical mission or business functions is often called a business plan, and it is used to support contingency planning.[104] Part of business planning involves the development of a business continuity plan that focuses on sustaining an organization's business functions during and after a disruption. A business continuity plan can be written for a specific business process or it may address all key business processes. Because there is an inherent relationship between an IT system and the business process it supports, there should be coordination between each plan, and ultimately an entity may use a suite of plans for its IT systems, business processes, and the facility.[105] In addition, a business impact analysis should be conducted to (1) identify critical information technology resources, (2) identify outage impact and allowable outage times, and (3) develop recovery priorities. The purpose of the business impact analysis is to correlate specific system components with the critical services that they provide and, based on that information, to characterize the consequences if system components were to be disrupted.

CP-1.1. Critical data and operations are identified and prioritized

The criticality and sensitivity of various data and operations should be determined and prioritized based on security categorizations and an overall risk assessment of the entity's operations. As discussed in section 3.1, Entitywide Security Management Program, such a risk assessment should serve as the foundation of an entity's security plan. Factors to be considered include the importance and sensitivity of the data and other organizational assets handled or protected by the individual operations, and the cost of not restoring data or operations promptly. For example, a 1-day interruption of major tax or fee-collection systems or a loss of related data could

[104]NIST, *An Introduction to Computer Security: The NIST Handbook*, Special Publication (SP) 800-12, October 1995.

[105]NIST, *Contingency Planning Guide for Information Technology Systems*, Special Publication (SP) 800-34, June 2002.

significantly slow or halt receipt of revenues, diminish controls over millions of dollars in receipts, and reduce public trust. Conversely, a system that monitors employee training could be out of service for perhaps as much as several months without serious consequences. Further, sensitive data, such as personal information on individuals or information related to contract negotiations, may require special protection during a suspension of normal service, even if such information is not needed on a daily basis to carry out critical operations.

Generally, critical data and operations should be identified and ranked by those personnel involved in the entity's business or program operations. For example, managers should predict the negative effects of lost data and interrupted operations and determine how long specific operations can be suspended or postponed. However, it is also important to obtain senior management's agreement with such determinations, as well as concurrence from affected groups.

The prioritized listing of critical information resources and operations should be periodically reviewed to determine whether current conditions are reflected in it. Such reviews should occur whenever there is a significant change in the entity's mission and operations or in the location or design of the systems that support these operations.

CP-1.2. Resources supporting critical operations are identified and analyzed

Once critical data and operations have been determined, the minimum resources needed to support them should be identified and their roles analyzed. The resources to be considered include computer resources, such as hardware, software, and data files; networks, including components such as routers and firewalls; supplies, including paper stock and preprinted forms; telecommunications services; and any other resources that are necessary to the operation, such as people, office facilities and supplies, and noncomputerized records. For example, an analysis should be performed to identify the maximum number of disk drives needed at one time and the specific requirements for telecommunications lines and devices.

Because essential resources are likely to be held or managed by a variety of groups within an entity, it is important that program and information security support staff work together to identify the resources needed for critical operations.

CP-1.3. Emergency processing priorities are established

In conjunction with identifying and ranking critical functions, the entity should develop a plan for restoring critical operations. The plan should clearly identify the order in which various aspects of processing should be restored, who is responsible, and what supporting equipment or other resources will be needed. A carefully developed processing restoration plan can help employees immediately begin the restoration process and make the most efficient use of limited computer resources during an emergency. Both system users and information security support staff should be involved in determining emergency processing priorities. (See critical element CP-3 for additional information on contingency planning.)

CP-1 Related NIST SP 800-53 Controls
RA-2 Security Categorization

Control Techniques and Suggested Audit Procedures for Critical Element CP-1

Table 33. Control Techniques and Suggested Audit Procedures for Critical Element CP-1: Assess the criticality and sensitivity of computerized operations and identify supporting resources

Control activities	Control techniques	Audit procedures
CP-1.1. Critical data and operations are identified and prioritized.	CP-1.1.1. The entity categorizes information systems in accordance with appropriate guidance, such as FIPS 199, and documents the results in the system security plan.	Perform the following procedures for CP-1.1.1 to CP-1.1.2.
	CP-1.1.2 A list of critical operations and data has been documented that • identifies primary mission or business functions, • prioritizes data and operations, • is approved by senior program managers, and • reflects current conditions including system interdependencies and technologies.	Review the policies and methodology used to categorize systems and create the critical operations list. This list should identify each system and its criticality in supporting the entity's primary mission or business functions. Review how systems are categorized and the critical operations list. Determine if the justifications have been documented and that they (1) prioritize data and operations by primary mission or business functions; (2) are approved by senior management; and (3) reflect current operating conditions, including key system interdependencies. Determine if technology supporting critical operations is identified and appropriately considered in processing priorities. Interview program, information technology, and security administration officials. Determine their input and assessment of the reasonableness of priorities established.
CP-1.2. Resources supporting critical operations are identified and analyzed.	CP-1.2.1. Resources supporting critical operations and functions have been identified and documented. Types of resources identified should include • computer hardware, • computer software, • computer supplies, • network components, • system documentation, • telecommunications, • office facilities and supplies, and • human resources.	Interview program and security administration officials responsible for developing the critical operations listing. Review documentation supporting the critical operations listing to verify that the following resources have been identified for each critical operation: • computer hardware and software, • computer supplies, • network components, • system documentation, • telecommunications, • office facilities and supplies, and • human resources. Appropriate documentation may include contingency-related plans in NIST SP 800-34.

Control activities	Control techniques	Audit procedures
	CP-1.2.2. Critical information technology resources have been analyzed to determine their impact on operations if a given resource were disrupted or damaged. This analysis should evaluate the impact of the outages over time and across related resources and dependent systems.	Determine if a current business impact analysis has been conducted that identifies critical information technology resources, disruption impacts, allowed outage times, and recovery priorities.
CP-1.3. Emergency processing priorities are established.	CP-1.3.1. Emergency processing priorities have been documented and approved by appropriate program and data processing managers.	Review related policies, plans, and procedures for emergency processing and ensure: • recovery priorities have been developed, • management has approved priorities, and • priorities are documented. • Request a copy of the continuity of operations plan. Interview program and security administration officials to determine whether they are aware of all policies and procedures for emergency processing priorities and maintain copies of the continuity of operations plan.

Source: GAO.

Critical Element CP-2. Take steps to prevent and minimize potential damage and interruption

There are a number of steps that an entity should take to prevent or minimize the damage to automated operations that can occur from unexpected events. These can be categorized as

- routinely duplicating or backing up data files, computer programs, and critical documents with off-site storage;
- arranging for remote backup facilities that can be used if the entity's usual facilities are damaged beyond use;
- establishing an information system recovery and reconstitution capability so that the information system can be recovered and reconstituted to its original state after a disruption or failure;
- installing environmental controls, such as fire-suppression systems or backup power supplies; and
- ensuring that staff and other system users understand their responsibilities during emergencies.

Such steps, especially implementing thorough backup procedures and installing environmental controls, are generally inexpensive ways to prevent relatively minor problems from becoming costly disasters. In particular, an entity should maintain an ability to restore data files, which may be impossible to recreate if lost. In addition, effective maintenance, problem management, and change management for hardware equipment will help prevent unexpected interruptions.

In an IS controls audit being performed as part of a financial audit or data reliability assessment, the auditor should tailor the identification of control techniques and audit procedures related to environmental controls (CP-2.2) and hardware maintenance (CP-2.4) to achieve the audit objectives, considering the IS controls identified by the auditor as significant to the audit objectives (e.g., internal control over financial reporting).

CP-2.1. Data and program backup procedures have been implemented

Routinely copying data files and software and storing these files at a secure, remote location are usually the most cost-effective actions that an entity can take to mitigate service interruptions. Although equipment can often be readily replaced, the cost could be significant and reconstructing computerized data files and replacing software can be extremely costly and time consuming. And, data files cannot always be reconstructed. In addition to the direct costs of reconstructing files and obtaining software, the related service interruptions could lead to significant financial losses.

A program should be in place for regularly backing up computer files, including master files, transaction files, application programs, system software, and database software, and for storing these backup copies securely at an off-site location. Choosing a location depends on the particular needs of the entity, but in general, the location should be far enough away from the primary location that it will be protected from events such as fires, storms, electrical power outages, and terrorism that may occur to the primary location. In addition, it should be protected from unauthorized access and from environmental hazards.

The frequency with which files should be backed up depends on the volume and timing of transactions that modify the data files. Generally, backing up files on a daily basis is adequate. However, if a system accounts for thousands of transactions per day, it may be appropriate to back up files several times a day. Conversely, if only a few transactions are recorded every week, then weekly backing up of files may be adequate.

File back up procedures should be designed so that a recent copy is always available. For example, new data file versions should be received at the off-site storage location before the disks or tapes containing prior versions are returned to the data center for reuse.

Generally, data center personnel are responsible for routinely backing up files. However, if critical data are routinely maintained on computers that are not under the control of data center personnel, then responsibility for backing up this information should be clearly defined.

In addition to data files and software programs, copies of any other information and supplies that may be needed to maintain operations should be maintained at a remote location. Examples of such documents are system and application documentation, unique preprinted computer paper, and essential legal files. Although a review of computer-related controls focuses on electronically maintained data, it is important that critical paper documents also be copied and stored remotely so that they are available when needed to support automated operations.

CP-2.2. Adequate environmental controls have been implemented

Environmental controls prevent or mitigate potential damage to facilities and interruptions in service. Examples of environmental controls include

- fire extinguishers and fire-suppression systems;
- fire alarms;
- smoke detectors;
- water detectors;

- emergency lighting;
- redundancy in air cooling systems;
- backup power supplies;
- existence of shut-off valves and procedures for any building plumbing lines that may endanger processing facilities;
- processing facilities built with fire-resistant materials and designed to reduce the spread of fire; and
- policies prohibiting eating, drinking, and smoking within computer facilities.

Environmental controls can diminish the losses from some interruptions such as fires or prevent incidents by detecting potential problems early, such as water leaks or smoke, so that they can be remedied. Also, uninterruptible or backup power supplies can carry a facility through a short power outage or provide time to back up data and perform orderly shut-down procedures during extended power outages.

CP-2.3. Staff have been trained to respond to emergencies

Staff should be trained in and aware of their responsibilities in preventing, mitigating, and responding to emergency situations. For example, information security support staff should receive periodic training in emergency fire, water, and alarm incident procedures, as well as in their responsibilities in starting up and running an alternate data processing site. Also, if outside users are critical to the entity's operations, they should be informed of the steps they may have to take as a result of an emergency.

Generally, information on emergency procedures and responsibilities can be provided through training sessions and by distributing written policies and procedures. Training sessions should be held at least once a year and whenever changes to emergency plans are made. Further, if staff could be required to relocate or significantly alter their commuting routine in order to operate an alternate site in an emergency, it is advisable for an entity to incorporate into the contingency plan steps for arranging lodging and meals or any other facilities or services that may be needed to accommodate essential personnel.

CP-2.4. Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions

Unexpected service interruptions can occur from hardware equipment failures or from changing equipment without adequate advance notification to system users. To prevent such occurrences requires an effective program for maintenance, problem management, and change management for hardware equipment.

Routine periodic hardware maintenance should be scheduled and performed to help reduce the possibility and impact of equipment failures. Vendor-supplied specifications normally prescribe the frequency and type of preventive maintenance to be performed. Such maintenance should be scheduled in a manner to minimize the impact on overall operations and on critical or sensitive applications. Specifically, peak workload periods should be avoided. All maintenance performed should be documented, especially any unscheduled maintenance that could be analyzed to identify problem areas warranting additional action for a more permanent solution. Flexibility should be designed into the data processing operations to accommodate the required preventive maintenance and reasonably expected unscheduled maintenance. For critical or sensitive applications that require a high level of system availability, the acquisition and use of spare or backup hardware may be appropriate.

Effective problem management requires tracking service performance and documenting problems encountered. Goals should be established by senior management on the availability of data processing and on-line service. Records should be maintained on the actual performance in meeting service schedules. Problems and delays encountered, the reasons for the problems or delays, and the elapsed time for resolution should be recorded and analyzed to identify any recurring pattern or trend. Senior management should periodically review and compare the service performance achieved with the goals and survey user departments to see if users' needs are being met.

Changes to hardware equipment and related software should be scheduled to minimize the impact on operations and users and allow for adequate testing to demonstrate that they will work as expected.

Advance notification should be given to users so that service is not unexpectedly interrupted.

CP-2 Related NIST SP 800-53 Controls	
CP-3	Contingency Training
CP-6	Alternative Storage Site
CP-7	Alternate Processing Site
CP-9	Information System Backup
CP-10	Information System Recovery and Reconstitution
MA-2	Controlled Maintenance
MA-3	Maintenance Tools
MA-5	Maintenance Personnel
MA-6	Timely Maintenance
PE-9	Power Equipment and Power Cabling
PE-10	Emergency Shutoff
PE-11	Emergency Power
PE-12	Emergency Lighting
PE-13	Fire Protection
PE-14	Temperature and Humidity Controls
PE-15	Water Damage Protection
PE-16	Delivery and Removal
PE-17	Alternate Work Site
PE-18	Location of Information System Components
SA-5	Information System Documentation

Control Techniques and Suggested Audit Procedures for Critical Element CP-2

Table 34. Control Techniques and Suggested Audit Procedures for Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption

Control activities	Control techniques	Audit procedures
CP-2.1. Information system back up and recovery procedures have been implemented.	CP-2.1.1. Backup files are created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are lost or damaged.	Review written policies and procedures for backing up and transporting files. Determine how often files are backed up and rotated off site, retention periods, and security involved in transport. Compare inventory records with the files maintained off-site and determine the age of these files. For a selection of critical files, locate and examine the backup files. Verify that backup files can be used to recreate current reports. Determine whether backup files are created and rotated off-site as prescribed and are sent before prior versions are returned. Determine if the technology is implemented in such a manner as to provide appropriate availability, including consideration of backup procedures, system configuration, redundancy, environmental controls, staff training, and routine maintenance.
	CP-2.1.2. System and application documentation is maintained at the off-site storage location.	Locate and examine documentation.
	CP-2.1.3. The backup storage site is • geographically removed from the primary site (for example, not subject to the same hazards), and • protected by environmental controls and physical access controls.	Examine the backup storage site. Determine if there are accessibility problems between the storage and processing sites in the event of an area wide disaster.
	CP-2.1.4. The information system back up and recovery procedures adequately provide for recovery and reconstitution to the system's original state after a disruption or failure including • system parameters are reset; • patches are reinstalled; • configuration settings are reestablished; • system documentation and operating procedures are available; • application and system software is reinstalled; • information from the most recent backup is available; and • the system is fully tested.	Interview entity officials and determine whether comprehensive procedures and mechanisms exist to fully restore the information security to its original state. Determine if this recovery capability has been tested and, if so, review the test plan and test results.

Control activities	Control techniques	Audit procedures
CP-2.2. Adequate environmental controls have been implemented.		Audit procedures for CP-2.2 should be performed in conjunction with Section AC-6 regarding physical access controls. Perform the following procedures to determine whether control techniques CP-2.2.1 through 2.2.10 are achieved. - Examine the entity's facilities. - Interview site managers.
	CP-2.2.1. Fire detection and suppression devices have been installed and are working, for example, smoke detectors, fire extinguishers, and sprinkler systems.	Observe that operations staff are aware of the locations of fire alarms, fire extinguishers, regular and auxiliary electrical power switches, water shut-off valves, breathing apparatus, and other devices that they may be expected to use in an emergency. Observe fire detection and suppression devices. Determine whether the activation of heat and smoke detectors will notify the fire department.
	CP-2.2.2. Controls have been implemented to mitigate other disasters, such as floods, earthquakes, terrorism, etc.	Review the entity's assessment of environmental risks and related controls.
	CP-2.2.3. Redundancy exists in critical systems (for example, power and air cooling systems).	Observe the operation, location, maintenance, and access to critical systems.
	CP-2.2.4. Building plumbing lines do not endanger the computer facility or, at a minimum, shut-off valves and procedures exist and are known.	Observe whether water can enter through the computer room ceiling or whether pipes are running through the facility and that there are water detectors on the floor.
	CP-2.2.5. An uninterruptible power supply or backup generator has been provided so that power will be adequate for orderly shut down.	Observe power backup arrangements and results of testing.
	CP-2.2.6. Humidity, temperature, and voltage are controlled within acceptable levels.	Determine whether humidity, temperature, and voltage are appropriately controlled.
	CP-2.2.7. Emergency lighting activates in the event of a power outage and covers emergency exits and evacuation routes.	Observe that emergency lighting works and that power and other cabling is protected.
	CP-2.2.8. A master power switch or emergency shut-off switch is present and appropriately located.	Observe power shut-off arrangements.
	CP-2.2.9. Environmental controls are periodically tested at least annually for federal agencies	Review test policies. Review documentation supporting recent tests of environmental controls and followup actions.

Control activities	Control techniques	Audit procedures
	CP-2.2.10. Eating, drinking, and other behavior that may damage computer equipment is prohibited.	Review policies and procedures regarding employee behavior. Observe employee behavior.
CP-2.3. Staff have been trained to respond to emergencies.	CP-2.3.1. Operational and support personnel have received training and understand their emergency roles and responsibilities.	Interview security personnel and appropriate operational and support staff and ensure that they understand their roles and responsibilities.
	CP-2.3.2. Personnel receive periodic environmental controls training including emergency fire, water, and alarm incident procedures.	Review training records and training course documentation. Determine whether all personnel have received up-to-date training and that the scope of the training is adequate.
	CP-2.3.3. Emergency response procedures are documented.	Review emergency response procedures for completeness and determine whether roles and responsibilities are clearly defined.
	CP-2.3.4. Emergency procedures are periodically tested.	Review test policies. Review test documentation. Interview operational and data center staff.
CP-2.4. Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions.	CP-2.4.1. Policies and procedures exist and are up-to-date.	Review policies and procedures.
	CP-2.4.2. Routine periodic hardware preventive maintenance is scheduled and performed in accordance with vendor specifications and in a manner that minimizes the impact on operations.	Perform the following procedures to determine whether control techniques CP-2.4.2 through 2.4.4 are achieved. Interview information security, data processing, and user management. Review maintenance documentation. Determine when maintenance is performed, if it is in accordance with vendor specifications, and if there is minimal impact on system availability.
	CP-2.4.3. Regular and unscheduled maintenance performed is documented.	
	CP-2.4.4. Flexibility exists in the data processing operations to accommodate regular and a reasonable amount of unscheduled maintenance.	
	CP-2.4.5. Spare or backup hardware is used to provide a high level of system availability for critical and sensitive applications.	Interview information security and data center management.
	CP-2.4.6. Goals are established by senior management on the availability of data processing and on-line services.	Perform the following procedures to determine whether control techniques CP-2.4.6 through 2.4.8 are achieved. Interview senior management, information security management, data processing management, and user management. Review supporting documentation, including system performance metrics.
	CP-2.4.7. Records are maintained on the actual performance in meeting service schedules.	
	CP-2.4.8. Problems and delays encountered, the reason, and the elapsed time for resolution are recorded and analyzed to identify recurring patterns or trends.	

Control activities	Control techniques	Audit procedures
	CP-2.4.9. Senior management periodically reviews and compares the service performance achieved with the goals and surveys of user departments to see if their needs are being met.	Interview senior management, information security management, data processing management, and user management. Review supporting documentation such as user surveys, service goals, metric measuring system availability, service schedules, and test plans.
	CP-2.4.10. Changes of hardware equipment and related software are scheduled to minimize the impact on operations and users, thus allowing for adequate testing.	For control techniques CP-2.4.10 and CP-2.4.11, review supporting documentation for scheduling of hardware changes, including staff notifications.
	CP-2.4.11. Advance notification of hardware changes and related software changes is given to users so that service is not unexpectedly interrupted.	

Source: GAO.

Critical Element CP-3. Develop and document a comprehensive contingency plan

A contingency plan or suite of related plans should be developed for restoring critical applications; this includes arrangements for alternative processing facilities in case the usual facilities are significantly damaged or cannot be accessed. Agency/entity-level policies and procedures define the contingency planning process and documentation requirements. Furthermore, an entitywide plan should identify critical systems, applications, and any subordinate or related plans. It is important that these plans be clearly documented, communicated to affected staff, and updated to reflect current operations. Testing the plan is addressed in critical element CP-4. In addition, the plan should address entity systems maintained by a contractor or other entity (e.g., through service level agreements).

According to NIST, contingency planning represents a broad scope of activities designed to sustain and recover critical IT services following an emergency. IT contingency planning fits into a much broader emergency preparedness environment that includes organizational and business process continuity and recovery planning. Ultimately, an organization may use a suite of plans to properly prepare response, recovery, and continuity activities for disruptions affecting the organization's IT systems, business processes, and the facility. Because there is an inherent relationship between an IT system and the business process it supports, there

should be coordination between each plan during development and updates to ensure that recovery strategies and supporting resources neither negate each other nor duplicate efforts.

The NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, discusses the types of contingency plans that an organization might use and how they relate to each other. Since there is no standard definition for these plans, they may vary from organization to organization. To provide a common basis of understanding for IT contingency planning, NIST developed the descriptions shown in the table below.

Table 35: Types of Contingency-Related Plans

Plan	Purpose	Scope
Business Continuity Plan (BCP)	Provide procedures for sustaining essential business operations while recovering from a significant disruption	Addresses business processes; IT addressed based only on its support for business process
Business Recovery (or Resumption) Plan (BRP)	Provide procedures for recovering business operations immediately following a disaster	Addresses business processes; not IT-focused; IT addressed based only on its support for business process
Continuity of Operations Plan (COOP)	Provide procedures and capabilities to sustain an organization's essential, strategic functions at an alternate site for up to 30 days	Addresses the subset of an organization's missions that are deemed most critical; usually written at headquarters level; not IT-focused
Continuity of Support Plan/IT Contingency Plan	Provide procedures and capabilities for recovering a major application or general support system	Same as IT contingency plan; addresses IT system disruptions; not business process focused
Crisis Communications Plan	Provides procedures for disseminating status reports to personnel and the public	Addresses communications with personnel and the public; not IT focused

Plan	Purpose	Scope
Cyber Incident Response Plan	Provide strategies to detect, respond to, and limit consequences of malicious cyber incident	Focuses on information security responses to incidents affecting systems and/or networks
Disaster Recovery Plan (DRP)	Provide detailed procedures to facilitate recovery of capabilities at an alternate site	Often IT-focused; limited to major disruptions with long-term effects
Occupant Emergency Plan (OEP)	Provide coordinated procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat	Focuses on personnel and property particular to the specific facility; not business process or IT system functionality based

Source: NIST Contingency Planning Guide for Information Technology Systems (SP 800-34).

In addition, NIST addresses technical contingency planning considerations and solutions for specific information technology platforms: (1) desktop computers and portable systems, (2) servers, (3) Web sites, (4) local area networks, (5) wide area networks, (6) distributed systems, and (7) mainframe systems.

Note that incident handling can be considered that portion of contingency planning that responds to malicious technical threats. An incident response capability is addressed in critical element AC-5.1.

CP-3.1. An up-to-date contingency plan is documented

Contingency plans should be documented, agreed on by both users and information security departments, and communicated to affected staff. As noted above, FISMA requires that each federal agency develop, document, and implement an agencywide information security program that includes plans to ensure continuity of operations for information systems.

The plan should reflect the risks and operational priorities that the entity has identified. It should be designed so that the costs of contingency planning do not exceed the costs associated with the risks that the plan is intended to reduce. The plan should also be detailed enough so that its success does not depend on the

knowledge or expertise of one or two individuals. It should identify and provide information on

- supporting resources that will be needed;
- roles and responsibilities of those who will be involved in recovery activities;
- arrangements for an off-site disaster recovery location and travel and lodging for necessary personnel, if needed;
- off-site storage location for backup files; and
- procedures for restoring critical applications and their order in the restoration process. (See section CP-1.3 for additional information on emergency processing priorities.)

Multiple copies of the contingency plan should be available, with some stored at off-site locations to make sure they are not destroyed by the same events that made the primary data processing facilities unavailable.

CP-3.2. Arrangements have been made for alternate data processing, storage, and telecommunications facilities

Depending on the degree of service continuity needed, choices for alternative facilities will range from an equipped site ready for immediate backup service, referred to as a "hot site," to an unequipped site that will take some time to prepare for operations, referred to as a "cold site." In addition, various types of services can be prearranged with vendors. These include making arrangements with suppliers of computer hardware and telecommunications services as well as with suppliers of business forms and other office supplies.

As with all emergency preparations, costs and risks should be considered in deciding what type of alternate site is needed. However, it should be geographically removed from the original site so that it is protected from the same events. In addition, the site should have ready access to the basic utilities needed to resume operations, such as electricity, water, and telecommunications services. In some cases, two or more entities may share the same

alternate site in order to reduce the cost. However, this may cause problems if two or more entities need the site at the same time.

Whatever options are determined to be the most appropriate, the entity should have a formal agreement or contract detailing the emergency arrangements. Further, the arrangements should be periodically reviewed to determine whether they remain adequate to meet the entity's needs.

CP-3 Related NIST SP 800-53 Controls
CP-2 Contingency Plan
CP-5 Contingency Plan Update
CP-8 Telecommunications Services

Control Techniques and Suggested Audit Procedures for Critical Element CP-3

Table 36. Control Techniques and Suggested Audit Procedures for Critical Element CP-3: Develop and document a comprehensive contingency plan

Control activities	Control techniques	Audit procedures
CP-3.1. An up-to-date contingency plan is documented.	CP-3.1.1. A contingency plan has been documented that • is based on clearly defined contingency planning policy; • reflects current conditions, including system interdependencies; • has been approved by key affected groups, including senior management, information security and data center management, and program managers; • clearly assigns responsibilities for recovery; • includes detailed instructions for restoring operations (both operating system and critical applications); • identifies the alternate processing facility and the back up storage facility; • includes procedures to follow when the data/service center is unable to receive or transmit data; • identifies critical data files; • is detailed enough to be understood by all entity managers; • includes computer and telecommunications hardware compatible with the entity's needs; • includes necessary contact numbers; • includes appropriate system-recovery instructions; • has been distributed to all appropriate personnel; and • has been coordinated with related plans and activities.	Review contingency planning policy and determine if it documents the entity's overall contingency objectives and establishes the organizational framework and responsibilities for contingency planning. Obtain contingency plans (see NIST SP 800-34) and compare their provisions with the most recent risk assessment and with a current description of automated operations. Compare the contingency plans to security-related plans, facility-level plans, and agency/entity-level plans such as those in NIST contingency planning guidance. Determine if the contingency plans include • appropriate consideration of the technology, including alternative processing requirements, • recovery of the security infrastructure, and • interdependencies with other systems (i.e., other component, federal, state, or local agencies) that could affect the contingency operations.

Control activities	Control techniques	Audit procedures
	CP-3.1.2. Contingency plans are reevaluated before proposed changes to the information system are approved to determine if major modifications have security ramifications that require operational changes in order to maintain adequate risk mitigation.	Interview senior management, information security management, and program managers.
	CP-3.1.3. Procedures allow facility access in support of restoration of lost information under the contingency plans in the event of an emergency.	Determine whether emergency and temporary access authorizations are properly approved, documented, controlled, communicated, and automatically terminated after a predetermined period. These procedures should be performed in conjunction with Section AC-3.1.8 and AC-6.1.8 regarding access controls.
	CP-3.1.4. The plan provides for backup personnel so that it can be implemented independent of specific individuals.	Review the contingency plan.
	CP-3.1.5. User departments have developed adequate manual/peripheral processing procedures for use until operations are restored.	Interview senior management, information security management, and program managers.
	CP-3.1.6. Several copies of the current contingency plan are securely stored off-site at different locations.	Observe copies of the contingency and related plans held off-site.
	CP-3.1.7. The contingency plan is periodically reassessed and revised as appropriate. At a minimum, the plan is reassessed when there are significant changes in the entity mission, organization, business processes, and IT infrastructures (e.g. hardware, software, personnel).	Review the plan and any documentation supporting recent plan reassessments.
CP-3.2. Arrangements have been made for alternate data processing, storage, and telecommunications facilities.	CP-3.2.1. Contracts or interentity agreements have been established for backup processing facilities that • are in a state of readiness commensurate with the risks of interrupted operations, • have sufficient processing and storage capacity, and • are likely to be available for use.	Interview officials and review contracts and agreements including processing priorities for the backup site. Determine if the back up site is properly configured and ready to be used as an operational site.
	CP-3.2.2. Alternate network and telecommunication services have been arranged.	Interview officials and review contracts and agreements including the priority of service provisions for the backup service provider. Determine if the backup service provides separate failure points and is geographically removed from the primary provider.
	CP-3.2.3. Arrangements are planned for travel, lodging, and protection of necessary personnel, if needed.	Interview officials and review the plan.

Source: GAO.

Critical Element CP-4. Periodically test the contingency plan and adjust it as appropriate

Testing contingency plans is essential to determining whether they will function as intended in an emergency situation. According to OMB, federal managers have reported that testing revealed

important weaknesses in their plans, such as backup facilities that could not adequately replicate critical operations as anticipated. Through the testing process, these plans were substantially improved.[106]

The most useful scenarios involve simulating a disaster situation to test overall service continuity. Such an event would include testing whether the alternative data processing site will function as intended and whether critical computer data and programs recovered from off-site storage are accessible and current. In executing the plan, managers will be able to identify weaknesses and make changes accordingly. Moreover, tests will assess how well employees have been trained to carry out their roles and responsibilities in a disaster situation.

CP-4.1. The plan is periodically tested

The frequency of contingency plan testing will vary depending on the criticality of the entity's operations. Generally, contingency plans for very critical functions should be fully tested about once every year or two, whenever significant changes to the plan have been made, or when significant turnover of key people has occurred. It is important for top management to assess the risks of contingency plan problems and develop and document a policy on the frequency and extent of such testing.

CP-4.2. Test results are analyzed and the contingency plan is adjusted accordingly

Contingency test results provide an important measure of the feasibility of the contingency plan. As such, they should be reported to top management so that the need for modification and additional testing can be determined and so that top management is aware of

[106] *Observations of Agency Computer Security Practices and Implementation of OMB Bulletin No.90-08: Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information*, February 1993. OMB Bulletin 90-08 was superseded by NIST Special Publication (SP) 800-18, dated December 1998, *Guide for Developing Security Plans for Information Technology Systems.* [OMB Circular A-130, Appendix III, directs NIST to update and expand security planning guidance.]

the risks of continuing operations with an inadequate contingency plan.

Any testing of contingency plans is likely to identify weaknesses in the plan, and it is important that the plan and related supporting activities, such as training, be revised to address these weaknesses. Otherwise, the benefits of the testing will be mostly lost.

Control Techniques and Suggested Audit Procedures for Critical Element CP-4

CP-4 Related NIST SP 800-53 Controls
CP-4 Contingency Plan Testing
CP-5 Contingency Plan Update

Table 37. Control Techniques and Suggested Audit Procedures for Critical Element CP-4: Periodically test the contingency plan and adjust it as appropriate

Control activities	Control techniques	Audit procedures
CP-4.1. The plan is periodically tested.	CP-4.1.1. The contingency plan is periodically tested under conditions that simulate a disaster. Disaster scenarios tested may be rotated periodically. Typically, contingency plans are tested annually or as soon as possible after a significant change to the environment that would alter the assessed risk.	Review testing policies and methodology used to select disaster scenarios. Determine when and how often contingency plans are tested. Determine if technology is appropriately considered in periodic tests of the contingency plan and resulting adjustments to the plan. Review test results. Observe a disaster recovery test.
CP-4.2. Test results are analyzed and the contingency plan is adjusted accordingly.	CP-4.2.1. Test results are documented and a report, such as a lessons learned report, is developed and provided to senior management.	Review final test report. Interview senior managers to determine if they are aware of the test results.
	CP-4.2.2. The contingency plan and related agreements and preparations are adjusted to correct any deficiencies identified during testing.	Review any documentation supporting contingency plan adjustments.

Source: GAO.

Chapter 4. Evaluating and Testing Business Process Application Controls

4.0 Overview

Business processes are the principal functions used by the entity to accomplish its mission. Examples of typical business processes in government entities include:

- Mission-related processes, typically at the program or sub-program level, such as education, public health, law enforcement, or income security;
- Financial management processes, such as collections, disbursements, or payroll; and
- Other support processes, such as human resources, or property management, and security.

A business process application is a combination of hardware and software that is used to process business information in support of a specific business process.

Business process application level controls, commonly referred to as “application level controls” or “application controls”, are those controls over the completeness, accuracy, validity, confidentiality, and availability of transactions and data during application processing. The effectiveness of application level controls is dependent on the effectiveness of entitywide and system level general controls. Weaknesses in entitywide and system level general controls can result in unauthorized changes to business process applications and data that can circumvent or impair the effectiveness of application level controls.

If entitywide and system level controls are relevant to the audit objectives, the auditor should coordinate the planning and testing of such controls with application level controls. For example, if a data management system is a critical control point, the auditor would

coordinate the planning of testing of the entitywide, system, and application level controls associated with the data management system.

In this chapter, application level controls are divided into the following four control categories, which are described in more detail below:

(1) Application level general controls;

(2) Business Process controls;

(3) Interface controls; and

(4) Data Management System controls.

The auditor should assess the effectiveness of controls in each of the four control categories to the extent they are significant to the audit objectives.

Application level general controls (referred to herein as "application security" or AS)consist of general controls operating at the business process application level, including those related to security management, access controls, configuration management, segregation of duties, and contingency planning. In this chapter, the general control activities discussed in Chapter 3, as well as related suggested control techniques and audit procedures, are tailored to the business process application level.

Business Process (BP) controls are the automated and/or manual controls applied to business transaction flows. They relate to the completeness, accuracy, validity and confidentiality of transactions and data during application processing. They typically cover the structure, policies, and procedures that operate at a detailed business process (cycle or transaction) level and operate over individual transactions or activities across business processes. Specific control areas of business process controls are:

- **Transaction Data Input** relates to controls over data that enter the application (e.g., data validation and edit checks).

- **Transaction Data Processing** relates to controls over data integrity within the application (e.g., review of transaction processing logs).

- **Transaction Data Output** relates to controls over data output and distribution (e.g., output reconciliation and review).

- **Master Data Setup and Maintenance** relates to controls over master data, the key information that is relatively constant and shared between multiple functions or applications (e.g., vendor file).

Interface controls (IN) consist of those controls over the a) timely, accurate, and complete processing of information between applications and other feeder and receiving systems on an on-going basis, and b) complete and accurate migration of clean data during conversion.

Data management system (DA) controls are relevant to most business process applications because applications frequently utilize the features of a data management system to enter, store, retrieve or process information, including detailed, sensitive information such as financial transactions, customer names, and social security numbers. Data management systems include database management systems, specialized data transport/communications software (often called middleware), data warehouse software, and data extraction/reporting software. Data management system controls enforce user authentication/authorization, availability of system privileges, data access privileges, application processing hosted within the data management systems, and segregation of duties. Chapter 3 addresses general controls over data management systems as part of system level controls. This chapter discusses their use within the application level.

For each of the four application control categories, this chapter identifies several critical elements—tasks that are essential for establishing adequate controls within the category. For each critical element, there is a discussion of the associated objectives, risks, and control activities, as well as potential control techniques and

suggested audit procedures. For each critical element, the auditor should make a summary determination as to the effectiveness of the entity's related controls in achieving the critical element. If the controls for one or more of each category's critical elements are ineffective, then the controls for the entire category are not likely to be effective. The auditor should use professional judgment in making such determinations.

To facilitate the auditors' evaluation, tables identifying commonly used control techniques and related suggested audit procedures are included after the discussion of each critical element. These tables can be used for both the preliminary evaluation and the more detailed evaluation and testing of controls. For the preliminary evaluation, the auditor can use the tables to guide and document preliminary inquiries and observations. For the more detailed evaluation and testing, the auditor can use the suggested audit procedures in developing and carrying out a testing plan. Such a testing plan would include more extensive inquiries; observation of control procedures; inspection of application configurations, design documents, policies and written procedures; and tests of key control techniques, which may include using audit or system software auditing tools.

The discussion of control elements and control techniques apply to all application environments, which include mainframe, client-server, integrated enterprise resource planning (ERP)[107] and web environments. The nature of evidence obtained by the auditor will be different based on the environment. Auditors' knowledge of the business processes and application level security in different environments is, therefore, critical to identifying and testing business process application level controls.

As noted earlier, the effectiveness of application level controls is dependent on the effectiveness of entitywide and system level

[107]An enterprise resource planning (ERP) system is a commercial software package that integrates all the information flowing through the entity. ERP systems contain functional modules (e.g., financial, accounting, human resources, and supply chain and customer information) that are integrated within the core system or interfaced to external systems.

general controls. Weaknesses in entitywide and system level general controls can result in unauthorized changes to business process applications and data (confidentiality, integrity, and availability) that can circumvent or impair the effectiveness of business process application controls. More specifically,

- Weaknesses in security management can result in inadequate assessment of and response to information security risks related to the business process applications and the systems on which they depend, as well as significantly increase the risk that application level and other controls are not consistently applied in accordance with management's policies.

- Weaknesses in access controls can result in unauthorized access to and modifications of

    - applications, including the operation of the related controls,

    - application data, including after the control(s) were applied, and/or

    - system components, which can lead to unauthorized changes to data and applications.

- Weaknesses in configuration management can result in unauthorized modifications or additions to the applications and to system components, leading to unauthorized access to data and applications.

- Weaknesses in segregation of duties can result in unauthorized access to applications, application data, and/or system components. In addition, such weaknesses can allow fraudulent transactions and control overrides to occur.

- Weaknesses in contingency planning can result in unavailability of applications and/or loss of application data.

The following table illustrates the relationship between business process application level controls and general controls at the entitywide and system level.

Table 38. General and Application Control Categories Applicable at Different Levels of Audit

	Control Categories	Entitywide/ Component Level	System Level			Business Process Application Level
			Network	Operating Systems	Infrastructure Applications	
General Controls	Security Management	→	→	→	→	→
	Access Controls	→	→	→	→	→
	Configuration Management	→	→	→	→	→
	Segregation of Duties	→	→	→	→	→
	Contingency Planning	→	→	→	→	→
Business Process Application Controls	Business Process Controls					→
	Interfaces					→
	Data Management Systems					→

Source: GAO.

4.0.1 The Auditor's Consideration of Business Process Control Objectives

The overall objectives of business process application level controls are to provide reasonable assurance about the completeness, accuracy, validity and confidentiality of transactions and data during application processing. Each specific business process control technique is designed to achieve one or more of these objectives. The effectiveness of business process controls depends on whether all of these overall objectives are achieved. Each objective is described in more detail below.

Completeness (C) controls should provide reasonable assurance that all transactions that occurred are input into the system, accepted for processing, processed once and only once by the system, and properly included in output. Completeness controls include the following key elements:

- transactions are completely input,
- valid transactions are accepted by the system,
- duplicate postings are rejected by the system,
- rejected transactions are identified, corrected and re-processed; and
- all transactions accepted by the system are processed completely.

The most common completeness controls in applications are batch totals, sequence checking, matching, duplicate checking, reconciliations, control totals and exception reporting.

Accuracy (A) controls should provide reasonable assurance that transactions are properly recorded, with the correct amount/data, and on a timely basis (in the proper period); key data elements input for transactions are accurate; and data elements are processed accurately by applications that produce reliable results; and output is accurate.

Accuracy control techniques include programmed edit checks (e.g., validations, reasonableness checks, dependency checks, existence checks, format checks, mathematical accuracy, range checks, etc.), batch totals and check digit verification.

Validity (V) controls should provide reasonable assurance (1) that all recorded transactions actually occurred (are real), relate to the organization, and were properly approved in accordance with management's authorization; and (2) that output contains only valid data. A transaction is valid when it has been authorized (for example, buying from a particular supplier) and when the master data relating to that transaction is reliable (for example, the name, bank account and other details on that supplier). Validity includes the concept of authenticity. Examples of validity controls are one-for-one checking and matching.

Confidentiality (CF) controls should provide reasonable assurance that application data and reports and other output are protected against unauthorized access. Examples of confidentiality controls include restricted physical and logical access to sensitive business process applications, data files, transactions, and output, and adequate segregation of duties. Confidentiality also includes restricted access to data reporting/extraction tools as well as copies or extractions of data files.

Availability controls should provide reasonable assurance that application data and reports and other relevant business information are readily available to users when needed. These controls are principally addressed in application security controls (especially contingency planning) and therefore, are not included as specific business process controls.

The completeness, accuracy, and validity controls relate to the overall integrity objective. The availability objective is addressed as part of application level general controls in AS-5.

4.0.2 Steps in Assessing Business Process Application Level Controls

The assessment of business process application level controls is incorporated into the audit approach discussed in Chapter 2. This

section provides supplemental implementation guidance with respect to planning the assessment of business process application level controls and should be applied in conjunction with Chapter 2. Consistent with Chapter 2, the assessment of business process application level controls includes the following steps:

- Plan the information system controls audit
- Perform information system controls audit tests
- Report audit results

4.0.3 Plan the Information System Controls Audit of Business Process Application Level Controls

Although planning continues throughout the audit, the objectives of the initial planning phase are to identify significant issues, assess risk, and design efficient and effective audit procedures. To accomplish this, the auditor performs the following steps, which are discussed in more detail in Chapter 2:

- Understand the overall audit objectives and related scope of the business process application control assessment
- Understand the entity's operations and key business processes
- Obtain a general understanding of the structure of the entity's networks
- Identify key areas of audit interest (files, applications, systems, locations)
- Assess information system risk on a preliminary basis
- Identify critical control points
- Obtain a preliminary understanding of business process application level controls
- Perform other audit planning procedures

The following discussion provides additional audit considerations as they apply to application level controls.

4.0.3.A Understand the overall audit objectives and related scope of the business process application control assessment

The auditor should obtain an understanding of the objectives of the application control assessment. The nature, timing and extent of the auditor's procedures to assess the effectiveness of application controls vary depending upon the audit objectives.

The audit objectives for an application control assessment could include:

- Assessment as part of a broad assessment of information system controls (including entitywide, system, and application level controls), either as part of a financial statement or performance audit, or as a standalone assessment;
- A comprehensive assessment of application level controls related to a specific application or applications, with or without an assessment of related entitywide and system level controls;
- An assessment of specific aspects of application level controls, such as:
    a. Evaluating the efficiency of business process applications;
    b. Assessing business process application level controls for applications under development;
    c. Assessing selected business application level control categories, such as business process controls or application level general controls;
    d. Assessing conversion of data to a new application; or
    e. Assessing access controls to assess whether access granted is appropriately identified, evaluated, and approved.

As noted in Chapter 2, if achieving the audit objectives does not require an overall conclusion on IS controls or relates only to certain components or a subset of controls, the auditor's assessment would not necessarily identify all significant IS control weaknesses that may exist. Consequently, if the audit objectives only relate to a subset of controls, such as only business process controls for a

specific application, the auditor should evaluate the potential limitations of the auditor's work on the auditor's report and the needs and expectations of users. The auditor may determine that, because the limitations are so significant, the auditor will (1) communicate the limitations to the management of the audited entity, those charged with governance, and/or those requesting the audit, and (2) clearly report such limitations on the conclusions in the audit report. For example, in reporting on an audit limited to business process controls within a business process application, the auditor may determine that it is appropriate to clearly report that the scope of the assessment was limited to those business process controls and that, consequently, additional information system control weaknesses may exist that could impact the effectiveness of IS controls related to the application and to the entity as a whole.

4.0.3.B Understand the entity's operations and key business processes

Understanding the entity's operations and business processes includes understanding how business process applications are used to support key business processes, as it tends to vary from entity to entity. The auditor should obtain and review documentation, such as design documents, blueprints, business process procedures, user manuals, etc., and inquire of knowledgeable personnel to obtain a general understanding of each significant business process application that is relevant to the audit objectives. This includes a detailed understanding of

- business rules (e.g. removing all transactions that fail edits or only selected ones based on established criteria),
- transaction flows (detailed study of the entity's internal controls over a particular category of events that identifies all key procedures and controls relating to the processing of transactions), and
- application and software module interaction (transactions leave one system for processing by another, e.g. payroll time card interfaces with pay rate file to determine salary information).

Obtaining this understanding is essential to assessing information system risk, understanding application controls, and developing relevant audit procedures.

The concept of materiality/significance, discussed in Chapter 2, can help the auditor determine which applications are significant, or key, to the audit objectives.

4.0.3.C Obtain a general understanding of the structure of the entity's networks

The auditor should obtain an understanding of the specific networks and systems that are used to support the key business process applications. Information obtained during this step is important to

(1) Assist in the identification of the critical control points (see Chapter 2) over which entitywide and system level controls need to be effective for the related application level controls to be effective. Based on the results of audit procedures, the auditor may modify the listing of critical control points, or identify additional critical control points. In the testing phase, the auditor assesses entitywide and system level controls (as outlined in Chapter 3) over each critical control point identified, unless not part of the objectives of the audit.

(2) Provide a foundation for understanding where application level general controls are applied. For example, application level general controls may be applied as part of the application itself, through access control software, data management systems, ERP systems, and/or in conjunction with operating system and network security. Obtaining such an understanding is important to identify those controls that are necessary to reasonably assure that unauthorized access to key applications and data files are prevented or detected.

4.0.3.D Identify key areas of audit interest (files, applications, systems, locations)

Based on the audit objectives and the auditor's understanding of the business processes and networks, the auditor should identify key areas of audit interest, including:

- key business process applications and where each key business process application is processed,
- key data files used by each key business application, and
- relevant general controls at the entitywide and system levels, upon which application level controls depend.

Chapter 2 provides additional information on identifying key areas of audit interest.

4.0.3.E Assess information system risk on a preliminary basis

Based on the auditor's understanding obtained in the previous steps, the auditor should assess, on a preliminary basis, the nature and extent of IS risk related to the key applications. The auditor may classify security risks according to the definitions explained in Chapter 2.

Chapter 2 provides a description of risk factors that are relevant to an assessment of IS risk, including nature of the hardware and software used, the configuration of the network, and the entity's IT strategy. The auditor should evaluate such risk factors in relation to the specific key business process applications. For example, Internet accessible applications, and applications that provide access to assets, such as payment or inventory systems, generally present a higher degree of risk.

4.0.3.F Identify critical control points

As discussed in Chapter 2, the auditor should identify and document critical control points in the entity's information systems and key applications, based on the auditor's understanding of such systems and applications, key areas of audit interest, and IS risk. Based on information obtained during audit planning, the auditor identifies critical control points related to the entity's key applications (applications that are significant to the audit objectives and key areas of audit interest). Critical control points at the application level (in addition to critical control points at the system levels) are those points, which if compromised, could significantly affect the integrity, confidentiality, or availability of key business process applications or related data. Critical control points at the business process application level typically include application level general

controls, and interface controls among several applications. Typical critical control points also include network components where business process application level controls are applied. As the audit testing proceeds and the auditor gains a better understanding of the applications, application functionality, controls within and outside each application, control weaknesses, and related risks, the auditor should reassess and reconsider the critical control points.

4.0.3.G Obtain a preliminary understanding of application controls

Within each key business process application, the auditor should obtain an understanding of the particular types of application level controls that are significant to the audit objectives. If the audit objectives relate to a comprehensive assessment of the effectiveness of application controls within one or more applications, the auditor should obtain an understanding of controls implemented by the entity to achieve each of the critical elements for each key application. If the assessment of application controls is performed in connection with a financial audit, the auditor should assess the effectiveness of those controls that are identified by the financial auditor (controls identified in the Specific Control Evaluation (SCE) Worksheet in federal financial audits) and other related controls upon which the effectiveness of these controls depend. The responsibility to identify financial reporting controls rests primarily with the financial auditor, but the information systems auditor should be consulted in this process. Financial reporting controls generally include both IS controls and non-IS controls. The SCE Worksheet is more fully discussed in section 395 H of the Financial Audit Manual (FAM).

The auditor should obtain a preliminary understanding of business process application controls in each of the following control categories to the extent they are significant to the audit objectives:

- Application level general controls;
- Business Process;
- Interface controls; and
- Data management systems.

Frequently each type of control occurs within a business process and such controls are interdependent. The auditor should consider the interaction between each of these types of controls. For example, interface and data management controls are inter linked since many of the feeder systems reside on some type of data management system whose controls must be effective to ensure the integrity of the data it maintains, including social security numbers, vendor names, and other sensitive information. Further, interface and business process controls are linked in that controls should be established that ensure the timely, accurate and complete processing of information between the feeder and receiving systems and the mainline business processes they support.

To document the auditor's understanding, the auditor may complete the control tables in Appendices II and III on a preliminary basis. The auditor generally should review available application documentation that explains processing of data within the application. The auditor generally should inspect any narratives, flowcharts, and documentation related to system and application, including error reporting.

As part of this step, the auditor should determine whether application level controls are effectively designed. In considering whether controls are effectively designed, the auditor considers the type of control. The effectiveness of business process application controls, and the nature, timing, and extent of assessment procedures, depend on the nature of the control.

As discussed in Chapter 1, information system (IS) controls consist of those internal controls that are dependent on information systems processing and include general controls (entitywide, system, and business process application levels), business process application controls (input, processing, output, master file, interface, and data management system controls), and user controls (controls performed by people interacting with information systems). General and business process application controls are always IS controls. A user control is an IS control if its effectiveness depends on information systems processing or the reliability (accuracy, completeness, and validity) of information processed by information systems. Conversely, a user control is not an IS control if its effectiveness does not depend on information systems

processing or the reliability of information processed by information systems.

Application controls can be automated or manual (sometimes referred to as user controls). The auditor will find that most business processes will have a combination of automated and manual controls that balance resource requirements and risk mitigation. Also, management may use manual controls as effective monitoring controls. It is important to understand how these types of controls inter-relate when assessing application controls. The auditor should evaluate the adequacy of controls, both automated and manual, to determine whether or not management has appropriately mitigated risks and achieved its control objectives.

Automated business process controls can provide a higher level of consistency in application, and can also be timelier in preventing an undesired outcome. Automated controls have greater consistency because once designed and implemented, they will continue to operate as designed, assuming the presence of effective general controls (at all levels). Automated controls can also be designed to block a transaction from proceeding through the process, making them timelier in preventing an undesired outcome. For example, a vendor invoice can be blocked for payment automatically if the goods or services are not received or if the payment exceeds a specific threshold and requires additional review and approval. Manual controls, such as the review of reports or payments over a certain amount, could effectively detect an invoice payment without goods receipt, or a high-dollar payment, but may not occur in time to stop the payment.

The operating effectiveness of an automated application control during the audit period also depends on the operating effectiveness of related general controls (at the entitywide, system and applications levels). For example, effective general controls are necessary to prevent or detect management overrides or other unauthorized changes to computer applications or data that could preclude or impair the operation of the automated control.

Automated controls can be further subdivided into

- **Inherent Controls** are those that have been hard coded and built into the application logic and cannot be changed by end users. The self-balancing capability provided by some applications is an example of an inherent control (e.g., in a financial application, the transaction will not post until debits = credits.

- **Configurable Controls** are those that have been designed into the system during application implementation and address the features most commonly associated with options available to guide end users through their assigned tasks. Workflow to approve purchase requisition and purchase orders, commitments not to exceed obligations, and dollar value threshold to process transactions are examples of configurable controls.

ERP systems by design are Extensible Business Reporting Language (XBRL) compliant, which means that they can be configured to prepare reports based upon standard rules or “taxonomies.” The auditor should understand the nature and extent of any XBRL use and evaluate the controls surrounding such reporting processes.

Automated controls cannot contemplate and reasonably forecast the outcome of every type of uncertainty, nor can it prevent or detect every possible error or intentional misuse of application functionality. For example, well-designed segregation of duty controls could be compromised by collusion. Manual controls, therefore, may be used either in situations where ideal controls, such as complete segregation of duties, can't be implemented to prevent something from occurring, or when manual controls offer an effective, cost-effective control option.

Manual controls require human involvement, usually by way of approval of a critical step in a business process (example: signed purchase requisition) or reviewing for exceptions and compliance by reviewing system output. Generally, the auditor considers and tests manual controls along with automated controls. Testing only one type of application control may lead to incorrect assessment of key controls management may be relying on.

When the effectiveness of a manual control that is significant to the audit objectives depends on the reliability of computer-processed information, it is considered an IS control and, the auditor should assess the effectiveness of relevant general (at the entitywide, system, and application levels) and business process application, controls over the reliability of the information used. Also, the effectiveness of manual controls is dependent on how consistently and effectively the control is applied. The auditor considers the following when reviewing manual controls:

- The competence of the individuals performing control activities (reviewing the reports or other documents). They should have an adequate level of business knowledge and technical expertise and be familiar with the entity's operations.
- The authority of the individuals performing the reviews to take corrective action. They should be adequately positioned within the entity to act effectively.
- The objectivity of the individuals performing the reviews. The individuals should be independent of those who perform the work, both functionally (that is, there should be adequate segregation of duties) and motivationally (for example, a review would be less effective if the reviewer's compensation is based on operating results being reviewed).
- The nature and quality of the information reviewed by management.
- The frequency and timeliness of performance of reviews.
- The extent of follow-up performed by management.
- The extent to which controls can be tested (i.e., the auditor's ability to corroborate management's responses to inquiries).

In addition to automated and manual controls performed prior to or during transaction processing, monitoring controls may be applied by management after the processing has taken place. Their objective is to identify any errors that have not been prevented or detected by other controls. Examples of monitoring controls include:

- Review of a report of revenue with overall knowledge of the volume of goods shipped.

- Monitoring of capital expenditures via a quarterly report that analyzes expenditures by department with comparisons to budgeted levels.
- Monitoring of budget versus actual program cost.

4.0.3.H Perform other audit planning procedures

As discussed in more detail in Chapter 2, the auditor should address the following issues during the planning phase that could affect the application control audit:

- relevant laws and regulations
- staffing and other resources needed to perform the audit
- multi-year planning
- communication to management officials concerning the planning and performance of the audit, and to others as applicable;
- use of service organizations;
- using the work of others; and
- preparation of an audit plan.

4.0.4 Perform Information System Controls Audit Tests of Business Process Application Level Controls

The auditor's assessment of application controls has two main aspects: testing the effectiveness of controls, and evaluating the results of testing. The process of testing and evaluation are planned and scoped during the planning phase, as discussed in Chapter 2. As the auditor obtains additional information during control testing, the auditor should periodically reassess the audit plan and consider whether changes are appropriate.

The auditor should perform the following procedures as part of testing and evaluating the effectiveness of application level controls:

- Understand information systems relevant to the audit objectives, building on identification of key areas of audit interest and critical control points.
- Determine which IS control techniques are relevant to the audit objectives. The control categories, critical elements, and control activities in Chapters 3 and 4 are generally relevant to all audits.

However, if the auditor is not performing a comprehensive audit, for example, an application review, then there may be no need to assess controls in Chapter 3.

- For each relevant IS control technique, determine whether it is suitably designed to achieve the critical activity and has been implemented — placed in operation (if not done earlier);
- Perform tests to determine whether such control techniques are operating effectively;
- Identify potential weaknesses in IS controls (weaknesses in design or operating effectiveness); and
- For each potential weakness, consider the impact of compensating controls or other factors that mitigate or reduce the risks related to the potential weakness.

The auditor considers the following in designing the tests of application level controls:

- The nature of the control;
- The significance of the control in achieving the control objective(s);
- The risk of the control not being properly applied. [also see FAM 340];
- All of the key controls that management is relying on to address the risks for a specific business process or a sub-process, which may include automated and manual controls;
- The key controls outside the application under audit, as the business process may involve other applications for a downstream or upstream sub-process; and
- The strength or weakness of the entitywide and system level controls. The depth of the testing is based on the level of risk of the entity under review and the audit objectives. In the absence of effective general controls, the auditor may conclude that business process application level controls are not likely to be effective.

4.0.5 Report Audit Results

As a final step of the audit of application level controls, the auditor should conclude on the individual aggregate effect of identified application control weaknesses on the audit objectives and report the results of the audit. Such conclusions generally should include the effect of any weaknesses on the entity's ability to achieve each of the critical elements in Chapters 3 and 4, and on the risk of unauthorized access to key systems or files. The auditor's conclusions should be based upon the potential interdependencies of application controls (i.e., controls which effectiveness depends on the effectiveness of other controls).

Prior to developing an audit report, it is generally appropriate to communicate identified weaknesses to management to obtain their concurrence with the facts and to understand whether there are additional factors that are relevant to the auditor's evaluation of the effect of the weaknesses. Communication of identified weaknesses to management typically includes the following information:

- Nature and extent of risks
- Control Objectives
- Control Activity
- Findings (including condition, criteria, and where possible, cause and effect), and
- Recommendations

Chapter 2 provides additional guidance on reporting audit results.

4.1. Application Level General Controls (AS)

Application level general controls consist of general controls operating at the business process application level, including those related to security management, access controls, configuration management, segregation of duties, and contingency planning. In this chapter, the general control activities discussed in Chapter 3, as well as related suggested control techniques and audit procedures, are tailored to the application level. Understanding business processes or events is necessary to determine the role of application level general controls in the assessment of business process application controls.

Chapter 3 addresses controls at the entitywide and system levels, such as those related to networks, servers, general support systems and databases that support one or more business and financial systems. Additional security considerations specific to applications are discussed in this section.

Application level general controls are dependent on general controls operating at the entitywide and system levels. The application is generally a subset of the infrastructure that includes one or more operating systems, networks, portals, LDAPs, and data management systems. For example, the system level access controls discussed in Chapter 3 apply to the users of the application. In addition, applications themselves require another level of access requirements that restrict users to application functionality that aligns with the user's role in the organization. The objective of application level general controls is to help entity management assure the confidentiality, integrity, and availability of information assets, and provide reasonable assurance that application resources and data are protected against unauthorized:

– Modification,
– Disclosure,
– Loss, and
– Impairment

Weaknesses in application level general controls can result in unauthorized access, use, disclosure, disruption, modification, or destruction of applications and application data. Consequently, weaknesses in application level general controls can affect the achievement of all of the control objectives (completeness, accuracy, validity, and confidentiality) related to applications data. Therefore, the control activities in the control tables for application level general controls do not contain reference to specific control objectives.

The evaluation of application level general controls is comprised of critical elements in the following areas: Security Management, Access Control, Configuration Management, Segregation of Duties and Contingency Planning. Application-specific technical knowledge is essential to assess the application level general controls.

The critical elements for application level general controls are:

- AS-1 - Implement effective application security management
- AS-2 - Implement effective application access controls
- AS-3 - Implement effective application configuration management
- AS-4 - Segregate application user access to conflicting transactions and activities and monitor segregation
- AS-5 - Implement effective application contingency planning

The related NIST SP 800-53 controls are identified in Chapter 3.

Critical Element AS-1. Implement effective application security management.

Effective application security management provides a foundation for entity management to obtain reasonable assurance that the application is effectively secure. Application security management provides a framework for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's application-related controls. Without effective security management over the application, there is an increased risk that entity management, IT staff, and application owners and users will not properly assess risk and will, consequently, implement

inappropriate and/or inadequate information security over the application. Effective application security management controls, consistent with Section 3.1, Security Management (SM), include the following steps:

- Establish an application security plan
- Periodically assess and validate application security risks
- Document and implement application security policies and procedures
- Implement effective security awareness and other security-related personnel policies
- Monitor the effectiveness of the security program
- Effectively remediate information security weaknesses
- Ensure that activities performed by external third parties are adequately secure

Establish an application security plan

An application security plan serves as a roadmap during the entire security development and maintenance lifecycle of the application, and is therefore critical to the auditor in gaining a high-level understanding of the entity's application security. The lack of a comprehensive, documented security design increases the risk of inappropriate system access and compromised data confidentiality, integrity, and availability. Risks of not having a security program at the application level include the following:

- The process to gather design requirements may be compromised without clear guidelines on approval and sign off procedures for security roles.
- Ongoing requirements for business process owners to provide authorization specifications to the security design team (e.g., field-level security, role testing, etc.) may be compromised without a guideline to drive the joint-effort process.
- Security roles could be defined inappropriately resulting in users being granted excessive or unauthorized access.

For federal systems, NIST Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems*, provides guidance on documenting information system security

controls. The general guidance in SP 800-18 is augmented by SP 800-53 with recommendations for information and rationale to be included in the system security plan.

Periodically assess and validate application security risks

Chapter 3 (SM-2) discusses comprehensive risk assessment, and provides guidance on risk assessment. The guidance includes requirements contained in various laws, such as FISMA and FMFIA, OMB Circular A-130, and standards developed by NIST[108]. Risk assessments should consider risks to data confidentiality, integrity, and availability, and the range of risks that an entity's systems and data may be subject to, including those posed by internal and external users. The Security Management section of Chapter 3 addresses the entitywide and system level security risk assessments. Risk assessments also should be conducted for applications, and documented in the security plan, as discussed in NIST SP 800-18. In assessing business processing controls, the auditor should consider management's own assessment of risks to know the risks identified by them and the extent to which each have been mitigated.

Document and implement application security policies and procedures

Based on the application security plan, the entity should document and implement specific policies and procedures that govern the operation of application controls. Policies and procedures should address all business process application level controls, be documented and reflect current application configurations.

In defining policies and procedures for application controls, the following should also be considered:

- High risk business processes – Procurement, Asset Management, Treasury, etc.
- Functionality that should not be widely distributed - For example, limiting vendor master data maintenance to a few

[108]In addition, agency-specific requirements should be addressed.

users is critical to ensure master data integrity and reliable transaction processing.

- Segregating master data and transactional data (Contrary to master data, transactional data result from a single event, and often use several field values of the master data.) – For example, combining vendor creation and payment authorization could result in payments to unauthorized vendors.
- Cross-business unit access - Should be limited to users who have a specific business need.

Implement effective security awareness and other security-related personnel policies

It is important that application owners and users are aware of and understand the application security policies and procedures so that they may be properly implemented. Improper implementation could result in ineffective controls and increased information security risks. Awareness programs should be coordinated with the entitywide training program to reasonably assure that the training is appropriate and consistent for all applications.

In addition, entitywide security-related personnel policies and procedures (see critical element SM-6) should be properly implemented with respect to the application. For example, controls should be in place to reasonably assure that (1) application users are appropriately trained, and (2) risks related to confidentiality, integrity, and availability are considered in approving user access (e.g., security clearances) and in applying personnel policies.

Monitor the effectiveness of the security program

Policies and procedures for monitoring application security should be integrated with monitoring performed as part of the entitywide information security program. Changes related to people, processes, and technology, often make policies and procedures inadequate. Periodic management evaluation not only identifies the need to change the policies and procedures, when appropriate, but also demonstrates management's commitment to an application security plan that is appropriate to the entity's mission. The basic components of an effective monitoring program are discussed in

Chapter 3 (Critical element SM-5), which provides guidelines for monitoring the policies and procedures relevant to application security. Management should have an adequate plan for monitoring policy effectiveness, and should test and document application security controls on a regular basis.

Management should consider ways to effectively coordinate monitoring efforts with work performed to comply with applicable laws and regulations and should consider them in developing an application security monitoring assessment plan. Examples of such requirements for federal entities include: FISMA, OMB Circular A-130 and OMB Circular A-123. FISMA requires that security of all major systems is tested by management annually, which would include applications. The depth and breadth of the testing may vary based on the following factors:

- The potential risk and magnitude of harm to the application or data;
- The criticality of the application to the entity's mission;
- The relative comprehensiveness of the prior year's review; and
- The adequacy and successful implementation of corrective actions for weaknesses identified in previous assessments.

OMB Circular A-130 requires that Federal agencies assess and test the security of major applications at least once every 3 years, as part of the certification and accreditation (C&A) process; sooner if significant modifications have occurred or where the risk and magnitude of harm are high.

OMB Circular A-123 requires agencies and individual Federal managers to take systematic and proactive measures to (i) develop and implement appropriate, cost-effective internal control for results-oriented management; (ii) assess the adequacy of internal control in Federal programs and operations; (iii) separately assess and document internal control over financial reporting consistent with the process defined in Appendix A; (iv) identify needed improvements; (v) take corresponding corrective action; and (vi) report annually on internal control through management assurance statements. The implementation guidance for OMB Circular A-123 includes requirements that are wholly consistent with this manual.

The entity should take into consideration the statutory and regulatory requirements in its assessment of the effectiveness of application security policies and procedures, and testing of application security controls.

Management should:

- develop and document the assessment plan of application security policies and procedures;
- test and document application security controls specific to each application; and
- ensure that the frequency and scope of testing are commensurate with the criticality of the application to the entity's mission and risk.

Effectively remediate information security weaknesses

Management's commitment to application security is also demonstrated in having an effective mechanism to address weaknesses and deficiencies identified. When weaknesses or deficiencies are identified in application security, management should assess the risk associated with the weakness or deficiency, and develop a corrective action plan (for federal agencies. OMB refers to these as Plans of Actions and Milestones (POAMs)). The action plan should include testing requirements of corrective actions, milestones, monitoring of activities related to the action plan, modification to policies and procedures (if required) and implementation of the corrective action. Such action plans should be coordinated with the entitywide corrective action plan process.

Ensure that activities performed by external third parties are adequately secure

An entity may allow external third parties access to their systems for various purposes. Chapter 3 discussed policies and procedures regarding the system access granted to third party providers (e.g. service bureaus, contractors, system development, security management), including the requirement to have appropriate controls over outsourced software development. Third party provider access to applications often extends beyond the software development. It is likely that entities have vendors, business

partners and contractors not only querying the applications, but also transacting with the entity, using entity applications, or connecting to the entity's applications via their own systems. In addition, public web sites are sometimes used to transact with the entity.

The impact of an external third party provider accessing the entity's applications is directly related to the magnitude of the system or direct access the provider is granted. This is determined by the entity's agreement with the provider. The entity should, however, require the providers to be subject to the same compliance requirements as the entity, and have the ability to monitor such compliance. Appropriate policies and procedures should exist for monitoring third party performance to determine whether activities performed by these external third parties are compliant with the entity's policies, procedures, privacy requirements, agreements or contracts.[109] In addition, subsection (m) of the Privacy Act of 1974 provides that when an entity contracts for the operation of a system of records on behalf of the entity to accomplish an entity function, the entity must apply the Act's requirements to the contractor and its employees working on the contract.

[109]See GAO, Information Security: Improving Oversight of Access to Federal Systems and Data by Contractors Can Reduce Risk, (Washington, D.C.: April 2005).

Control Techniques and Suggested Audit Procedures for Critical Element AS-1

Table 39. Control Techniques and Suggested Audit Procedures for Critical Element AS-1: Implement effective application security management

Control activities	Control techniques	Audit procedures
AS-1.1 A comprehensive application security plan is in place.	AS-1.1.1 A comprehensive application security plan has been developed and documented. Topics covered include: • Application identification and description • Application risk level • Application owner • Person responsible for the security of the application • Application interconnections/information sharing • A description of all of the controls in place or planned, including how the controls are implemented or planned to be implemented and special considerations • Approach and procedures regarding security design and upgrade process • Process for developing security roles • General security administration policies, including ongoing security role maintenance and development • Identification of sensitive transactions in each functional module • Identification of high risk segregation of duty cases • Roles and responsibilities of the security organization supporting the system with consideration to segregation of duties • Security testing procedures • Coordination with entitywide security policies • Procedures for emergency access to the production system, including access to update programs in production, direct updates to the database, and modification of the system change option • System parameter settings, compliant with entitywide agency policies • Access control procedures regarding the use of system delivered critical user IDs	Inspect the application security plan to determine whether it adequately addresses all of the relevant topics.

Control activities	Control techniques	Audit procedures
	AS-1.1.2 Sensitive accounts are identified for each business process or sub-process, and appropriate security access privileges are defined and assigned.	Review the entity's identification of sensitive transactions for the business process being audited for appropriateness and completeness. Observe and inspect procedures for identifying and assigning sensitive activities. Inspect authorizations for sensitive activities.
	AS-1.1.3 Access privileges are developed to prevent users from executing incompatible transactions within the application via menus or screens.	Through inquiry and inspection, determine whether the application security plan includes plans to identify segregation of duty conflicts in each of the business processes under assessment (master data and transaction data; data entry and reconciliation), and addresses controls to mitigate risks of allowing segregation of duty conflicts in a user's role.
AS-1.2 Application security risk assessments and supporting activities are periodically performed	AS-1.2.1 Security risks are assessed for the applications and supporting systems on a periodic basis or whenever applications or supporting systems significantly change. The risk assessments and validation, and related management approvals, are documented and maintained.	Obtain the most recent security risk assessment for each application under assessment. Inspect the risk assessments to determine if the risk assessments are up-to-date, appropriately documented, approved by management, and supported by testing. Consider compliance with OMB, NIST, and other requirements/ guidance and whether technology and business processes are appropriately considered in the risk assessment.
	The risk assessments are appropriately incorporated into the application security plan.	Obtain and inspect the relevant application security plan(s) to determine whether the risk assessments are appropriately incorporated into the application security plan.
AS-1.3 Policies and procedures are established to control and periodically assess the application.	AS-1.3.1 Business process owners accept risks and approve the policies and procedures.	Determine through interview with entity management whether policies and procedures have been established to review access to the application.
	AS-1.3.2 Policies and Procedures: • are documented, • appropriately consider business process security needs, and • appropriately consider segregation of application user activity from the system administrator activity.	Review policies and procedures to determine whether they have appropriately considered (1) business security needs and (2) segregation of application user activity from system administrator activity.

Control activities	Control techniques	Audit procedures
AS 1.4 Application owners and users are aware of application security policies	AS-1.4.1 The entity has an effective process to communicate application security policies to application owners and users and reasonably assure that they have an appropriate awareness of such policies.	Obtain an understanding of how application owners and users are made aware of application security policies and assess the adequacy of the process. Interview selected application owners and users concerning their awareness of application security policies.
	AS-1.4.2 Personnel policies related to the application appropriately address security and application owners and users have adequate training and experience.	Review personnel policies for appropriateness and consistency with entitywide policies. Assess the adequacy of training and expertise for application owners and users.
AS-1.5 Management monitors and periodically assesses the appropriateness of application security policies and procedures, and compliance with them.	AS-1.5.1 An application security policy and procedure test plan is developed and documented.	Inquire of management, and inspect testing policies and procedures.
	AS-1.5.2 Security controls related to each major application are tested at least annually.	Inspect the overall testing strategy, a selection of test plans and related testing results. Determine if the scope of testing complies with OMB Circular A-123 Revised (federal entities) and other appropriate guidance. Determine if C&A testing is performed that complies with OMB and NIST requirements.
	AS-1.5.3 The frequency and scope of testing is commensurate with the risk and criticality of the application to the entity's mission.	Based upon the application test plan, assess whether the frequency and scope of testing is appropriate, given the risk and critically of the application.
	AS-1.5.4 Compliance, and a report on the state of compliance, is part of the entity's security program.	Determine through inquiry and inspection if the application security plan is incorporated into the entity's security program.
AS-1.6 Management effectively remediates information security weaknesses.	AS-1.6.1 Management has a process in place to correct deficiencies.	Inquire of management and inspect security polices and procedures, including assessment and resolution plan.
	AS-1.6.2 Management initiates prompt action to correct deficiencies. Action plans and milestones are documented and complete.	Inspect recent FMFIA/A-123 and POA&M (or equivalent) reports for reasonableness of corrective actions (nature and timing). Determine whether application security control deficiencies (identified by the audit, by management testing, and by others) are included in the plans of action and milestones (or equivalent). and determine the status of corrective actions.

Control activities	Control techniques	Audit procedures
	AS-1.6.3 Deficiencies are analyzed by application (analysis may be extended to downstream, upstream, and other related applications), and appropriate corrective actions are applied.	Evaluate the scope and appropriateness of planned corrective actions through inquiry of management and inspection of evidence.
	AS-1.6.4 Corrective actions are tested after they have been implemented and monitored on a continuing basis.	Inspect documentation to determine if implemented corrective actions have been tested and monitored periodically.
AS-1.7 External third party provider activities are secure, documented, and monitored	AS-1.7.1 Policies and procedures concerning activities of third party providers are developed and include provisions for: • Application compliance with entity's security requirements, and • Monitoring of compliance with regulatory requirements	Inspect policies and procedures pertaining to external parties for the application under assessment. Inspect documentation to determine whether the external third party provider's need to access the application is appropriately defined and documented. Review contracts with third-party providers to determine compliance with the Privacy Act, where applicable.
	AS-1.7.2 A process is in place to monitor third party provider compliance to the entity's regulatory requirements	Inquire of management regarding procedures used to monitor third party providers. Inspect external reports (SAS 70) or other documentation supporting the results of compliance monitoring.

Source: GAO.

Critical Element AS-2. Implement effective application access controls

Effective application access controls should be implemented at the application level to provide reasonable assurance that only authorized personnel have access to the application and only for authorized purposes. Without effective application access controls, persons may obtain unauthorized or inappropriate access to applications and application data.

Effective application access controls, consistent with Section 3.2, Access Controls (AC), include the following steps:

- Adequately protect information system boundaries.
- Implement effective identification and authentication mechanisms.
- Implement effective authorization controls.

- Adequately protect sensitive system resources.
- Implement an effective audit and monitoring capability.
- Establish adequate physical security controls.

Adequately protect application boundaries

Application boundaries control logical connectivity to and from applications through controlled interfaces (e.g., gateways, routers, firewalls, encryption). In defining the application, the entity creates the boundaries for the application. Once defined, the entity should design appropriate controls over the flow of information across the application boundary. In complex applications, there may boundaries within the application. The security plan for the application should identify system boundaries and IS controls implemented to protect the security of such boundaries. Application boundaries are more sensitive where the connectivity is to lower risk systems or to systems or users external to the entity.

Implement effective identification and authentication mechanisms

The entity should have application security policies and procedures in place concerning user identification and authentication. Management should have created an environment where all users have their own unique IDs and passwords, or other mechanisms, such as tokens and biometrics to access any part of the information system and applications that allow them to execute functional responsibilities. Identification and authentication policy and management are discussed in Chapter 3, Critical Element AC-2. In addition, it is important to understand the mechanisms used to assign access privileges for applications under assessment. An evaluation of identification and authentication controls includes consideration of the following factors:

- How do the users access the application?

    a. Are users required to enter user name/ID and password?

    b. Do all users have an individual and unique ID that would allow the user's activities to be recorded and reviewed?

c. Are users required to enter/use other authenticating information, such as tokens or biometrics?

d. Are users required to enter a separate ID and password for each application?

e. Does the application require the user to enter a password?

f. What are the password parameters (i.e. length, character requirements, etc)?

g. How often does the application require the user to change the password?

h. Are there any instances of users having multiple IDs and passwords?

i. Are there any instances of users sharing IDs or passwords?

- What other IDs and passwords does the user have to enter before accessing the sign-in screen for the application?

    a. Does the user enter a network ID and password?

    b. Does the user enter a terminal emulation ID and password?

The knowledge of the application security design and function enables the auditor to assess the effectiveness of the security controls over the other levels of authentication, especially when weaknesses are identified at the application security layer, as those weaknesses may be mitigated by stronger controls at other levels.

Implement effective authorization controls

The following procedures discussed in Chapter 3 are equally applicable at the application level:

- The owner identifies the nature and extent of access that should be available for each user;
- The owner approves user access to the application and data;
- Access is permitted at the file, record, or field level; and
- Owners and security managers periodically monitor user access.

Security administration procedures should provide tactical guidance on the day-to-day operations of creating, assigning, monitoring, updating, and revoking end-user access to the application. End-users should be assigned authorizations sufficient, but not excessive, to perform their duties in the application: Access should be limited to individuals with a valid business purpose (least privilege). The users should be granted the level of access by virtue of the position they hold within the organization. This will generally require user to have both:

- Functional access (for example, accounts payable) based on the role from which their position derives; and
- Organizational access (for example, account payable supervisor) based on the specific needs of their position.

Sensitive transactions and segregation of duty conflicts defined by the process and data owners (discussed in AS-1) should be used as a baseline reference by security administration. In an integrated application environment, the importance of comprehensive identification of sensitive transactions and segregation of duty needs and conflicts is heightened, compared with entities having multiple applications for business processes. Entities lose the inherent segregation in integrated applications—since more of the process is performed in the same application, the opportunities for access throughout the process are greater. For example, in an entity with separate purchasing and accounts payable applications, adequate segregation of duties might be accomplished by only allowing access to one of the applications, whereas in an integrated application, these applications may be combined. Transaction-level restricted access, which is critical in integrated applications, may be less critical in non-integrated systems.

However, in an integrated environment, the entire business process cycle may be performed in the same application and a user may have the ability to perform more than one key activity in the cycle. Therefore, restricted access (access to a sensitive business transaction) and segregation of duty conflicts (access to two or more transactions that are sensitive in combination) should be considered carefully.

An integrated application environment also generally means that more business units of the entity are using the same application. Therefore, business unit access restrictions are also necessary. Management should have an adequate understanding of the business processes and determine whether users should have access to more than their individual business unit. For example, a property manager should not have access to change asset records or maintenance schedules for entities other than his/her own.

Sensitive transactions or activities in an application are determined by the nature and use of the data processed by the application. Factors that determine the sensitivity include the mission critical elements of the application, pervasive use of the data or activity, confidentiality and privacy of data, and activities performed or supported by the application.

The key element in assigning access to sensitive transactions or activities to an application user is the alignment of user access to job responsibility. This has a dual purpose: one, the proper alignment ensures that the user has accountability for proper execution of the transactions and accuracy of the related data, and two, the expertise and skills of the user match the business process underlying the transaction or activity. For example journal voucher entry is made by a General Accounting Account Analyst of Finance Department, and not by a Procurement manager.

Adequately protect sensitive application resources

Access to sensitive application resources should be restricted to individuals or processes that have a legitimate need for this access for the purposes of accomplishing a valid business purpose. Sensitive application resources include password files, access

authorizations to read or modify applications, and sensitive application functions such as application security administration. The entity should identify and adequately protect sensitive application resources. In some cases, sensitive data may need to be encrypted.

Implement an effective audit and monitoring capability

Audit and monitoring involves the regular collection, review, and analysis of indications of inappropriate or unauthorized access to the application. Automated controls may be used to identify and report such incidents. An understanding of manual control activities surrounding access to the application is important. The following questions can help the auditor gain insight into management's controls:

- Does management maintain and review a current list of authorized users?
- Does management periodically review the user list to ensure that only authorized individuals have access, and that the access provided to each user is appropriate?
- Does management monitor access within the application (i.e. unauthorized access attempts, unusual activity etc.)? Does the application generate reports to identify unauthorized access attempts? Are security logs created and reviewed?
- Is public access (non entity employees) permitted to the application? Is access permitted via the Internet? If so, how is this access controlled?
- Is the application configured to allow for segregation of duties? If so, does the application identify the users who performed activities that were in conflict? Are the transactions/logs reviewed by the business owners?
- Has a procedure been created and placed in operation that requires a complete user recertification on a periodic basis?

- Is the security administration monitored? When suspicious activities are identified, how does management investigate them?

Establish adequate physical security controls

Appropriate physical controls, integrated with related entitywide and system level physical security, should be in place to protect resources, where applicable, at the application level. Resources to be protected at the application level include controls over removable media (e.g., tape files), workstations containing sensitive application data, and physical inputs (e.g., check stock) and outputs (e.g., physical checks or other sensitive documents). The entity should identify application resources that are sensitive to physical access and implement adequate physical security over such resources.

Control Techniques and Suggested Audit Procedures for Critical Element AS-2

Table 40. Control Techniques and Suggested Audit Procedures for Critical Element AS-2: Implement effective application access controls

Control activities	Control techniques	Audit procedures
AS-2.1 Application boundaries are adequately protected.	AS-2.1.1 Application boundaries are identified in security plans. Application boundaries are adequately secure.	Review security plans for proper identification of application boundaries. Evaluate the effectiveness of controls over application boundaries.
AS-2.2 Application users are appropriately identified and authenticated.	AS-2.2 Identification and authentication is unique to each user. All approved users should enter their user ID (unique) and password (or other authentication) to gain access to the application.	Inspect pertinent policies and procedures, and NIST guidance for authenticating user IDs. Through inquiry, observation or inspection, determine the method of user authentication used (password, token, biometrics, etc.). If a password system is used, gain an understanding of the specific information and evaluate its appropriateness, including application security authentication parameters, via inspection of system reports or observation of the system, including appropriate testing. See AC-2 for more information on criteria for evaluating password policies.

Control activities	Control techniques	Audit procedures
AS-2.3 Security policies and procedures appropriately address ID and password management.	AS-2.3.1 The entity has formal procedures and processes for granting users access to the application. The entity's IT security policies and procedures contain guidance for: • Assigning passwords; • Changing and resetting passwords; and • Handling lost or compromised passwords	Through inquiry, observation, and inspection, understand and assess procedures used by the entity for application password management: • Procedures for initial password assignment, including the password parameters; • Procedures for password changes, including initial password change; • Procedures for handling lost passwords (password resetting); and • Procedures for handling password compromise.
	AS-2.3.2 The application locks the user's account after a pre-determined number of attempts to log-on with an invalid password. The application may automatically reset the user account after a specific time period (an hour or a day), or may require an administrator to reset the account. If the user is away from his/her workspace for a preset amount of time, or the user's session is inactive, the application automatically logs off the user's account.	After obtaining an understanding of the user authentication process, inspect and/or observe the following: • Whether access to the application is permitted only after the user enters their user ID and password. • Observe a user executing invalid logins and describe the actions taken. Either 1) inspect system security settings, or 2) observe an idle user workspace to determine whether the application logs the user off after an elapsed period of idle time.
	AS-2.3.3 Each application user has only one user ID.	Through observation and inspection, determine whether each user has one, and only one, user ID to access the application.
	AS-2.3.4 Multiple log-ons are controlled and monitored.	Through inquiry, observation or inspection, determine whether the application allows multiple log-ons by the same user. If so, understand and document monitoring procedures that reasonably assure that multiple log-ons are not used to allow application access to an unauthorized user, or to violate effective segregation of duties.
AS-2.4 Access to the application is restricted to authorized users.	AS-2.4.1 Before a user obtains a user account and password for the application, the user's level of access has been authorized by a manager and the application administrator.	Review policies and procedures. From a selection of user accounts determine whether the user level of access was authorized by appropriate entity management.

Control activities	Control techniques	Audit procedures
	AS-2.4.2 Owners periodically review access to ensure continued appropriateness.	Interview security administrators and inspect evidence of the effectiveness of periodic review of access by owners.
	AS-2.4.3 Access is limited to individuals with a valid business purpose (least privilege)	Interview owners and inspect documentation, to determine whether appropriate procedures are in place to remove or modify application access, as needed. Through inquiry, observation, and inspection, determine how an unauthorized user is identified, and whether access is removed promptly and how. Based on the selection of users in AS-2.4.1 above, determine whether the user access is appropriate to the business need. If the users did not execute the transaction or activity within the expected time frame, processes should be in place to evaluate the continued need for access, and modify access accordingly.
AS-2.5 Public access is controlled. (Based on an entity's business mission, the entity may allow the public to have access to the application.)	AS-2.5.1 The entity implements a security plan and process for 1) identification and authorization of users; 2) access controls for limited user privileges; 3) use of digital signatures; 4) prohibition of direct access by the public to production data; and 5) compliance with NIST guidance.	Obtain an understanding of the following controls through inquiry of the application owner, inspection of source documents, and/or observation of the following: • Identification and authentication; • Access controls for limiting user privileges(read, write, modify, delete); • Use of digital signatures; • Prohibition of direct access by the public to live databases and restricted/sensitive records; and Legal considerations (i.e., privacy laws, OMB, NIST, etc.).
AS-2.6 User access to sensitive transactions or activities is appropriately controlled.	AS-2.6.1 Owners have identified sensitive transactions or activities for the business process.	Inquire of responsible personnel and inspect pertinent policies and procedures covering segregation of application duties

Control activities	Control techniques	Audit procedures
	AS-2.6.2 Owners authorize users to have access to sensitive transactions or activities.	Determine whether the process owners have identified a list of sensitive transactions or activities for their area. Inspect the user administration procedures to determine whether they include a requirement for the process owner to approve access to transactions or activities in their area of responsibility. Through inquiry and inspection, determine whether user access is authorized by process owners.
	AS-2.6.3 Security Administrators review application user access authorizations for access to sensitive transactions and discuss any questionable authorizations with owners.	Select user access request forms or other authorization documents [can use selection from AS-2.4.1 and AS-2.4.3] and inspect them to determine whether the process owners have approved user access to appropriate transactions or activities. Interview security administrators and inspect user access authorization procedures to determine whether access to sensitive transactions require approval by the process owner.
	AS-2.6.4 Owners periodically review access to sensitive transactions and activities to ensure continued appropriateness.	Inspect evidence of periodic review by owners of access to sensitive transactions.
	AS-2.6.5 Inactive accounts and accounts for terminated individuals are disabled or removed in a timely manner.	Review security software parameters and review system-generated list of inactive logon IDs, and determine why access for these users has not been terminated. Obtain a list of recently terminated employees and, for a selection, determine whether system access was promptly terminated.

Control activities	Control techniques	Audit procedures
	AS-2.6.6 Access to sensitive transactions is limited to individuals with a valid business purpose (least privilege)	Interview owners and inspect documentation, to determine whether appropriate procedures are in place to remove or modify application access, as needed. Through inquiry, observations, and inspection, determine how an unauthorized user is identified, and whether access is removed promptly and how. Obtain a list of users with access to identified sensitive transactions for the business process under assessment. Inspect the list to determine whether the number of users having access to sensitive transactions/ activities is appropriate to the business need. If the users did not execute the transaction or activity within the expected time frame, processes should be in place to evaluate the continued need for access, and modify access accordingly.
AS-2.7 Sensitive application resources are adequately protected	AS-2.7.1 The entity identifies sensitive application resources. Access to sensitive application resources is restricted to appropriate users. Sensitive application data is encrypted, where appropriate.	Evaluate the completeness of sensitive application resources identified. Assess the adequacy of IS controls over sensitive application resources. Review implementation of encryption of sensitive application data, where appropriate.

Control activities	Control techniques	Audit procedures
AS-2.8 An effective access audit and monitoring program is in place, documented, and approved.	AS-2.8.1 Policies and procedures are established to reasonably assure that application security audit and monitoring is effective	Inspect documented policies and procedures for application security administration for each application in scope Determine whether the monitoring program has built-in procedures to identify inappropriate user assignments. Through inquiry and inspection, determine whether monitoring procedures are performed on a regular basis. Determine whether the exceptions are handled appropriately and in a timely manner.
AS- 2.9 Application security violations are identified in a timely manner.	AS-2.9.1 Logging and other parameters are appropriately set up to notify of security violations as they occur.	Observe and inspect application logging and other parameters that identify security violations and exceptions. (For example, parameter set up indicates whether or not users can logon to an application more than once)
AS-2.10 Exceptions and violations are properly analyzed and appropriate actions taken.	AS-2.10.1 Reportable exceptions and violations are identified and logged. Exception reports are generated and reviewed by security administration. If an exception occurs, specific action is taken based upon the nature of exception.	Observe and inspect management's monitoring of security violations, such as unauthorized user access. Inspect reports that identify security violations. Through inquiry and inspection, note management's action taken. Inspect reports of authorized segregation of duty conflicts sensitive process access; Assess business level authorization and monitoring, if applicable
AS-2.11 Physical security controls over application resources are adequate	AS-2.11.1 Physical controls are integrated with entitywide and system-level controls. Application resources sensitive to physical access are identified and appropriate physical security is placed over them.	Review the appropriateness of the entity's identification of application resources sensitive to physical access. Assess the adequacy of physical security over sensitive application resources.

Source: GAO.

Critical Element AS-3. Implement effective application configuration management

Entities need to proactively manage changes to system environments, application functionality and business processes to reasonably assure financial data and process integrity. To do this, entities should restrict and monitor access to program modifications and changes to configurable objects in the production environment. Configuration Management (CM) discusses changes to baseline configuration of applications, using the concepts of identification, control, status reporting and auditing of configuration. Most application configuration changes are managed using a staging process. The staging process allows the entity to develop and unit test changes to an application within the development environment, transport the changes into a Quality Assurance environment for further system and user acceptance testing and, when the tests have been completed and the changes are approved, transport the changes into the production environment. Also, see Section CM for general controls related to configuration management.

Control over business process applications modifications and configurable objects is an extension of Configuration Management controls in Chapter 3 that addresses an organization's change management process and should be coordinated with audit procedures applied to that general control category. This chapter includes changes to application functionality that do not go through the staging process, but take place directly in the production environment of the application as changes become necessary throughout the normal course of business.

Managing change for business process applications that are accessible from the internet needs to be performed in a manner consistent with risk. Specific policies and procedures for application change controls when inbound or outbound internet access is involved should be established.

Effective application configuration management, consistent with Section 3.3 Configuration Management (CM), includes the following steps:

1. Develop and document CM policies, plans, and procedures.

2. Maintain current configuration identification information.

3. Properly authorize, test, approve, and track all configuration changes, including

- Documented system development life cycle methodology (SDLC);
- Adequate authorization of change requests that are documented and maintained;
- Appropriate authorization for the user to change the configuration;
- Adequate control of program changes through testing to final approval;
- Adequate control of software libraries; and
- Appropriate segregation of duties over the user's access to reasonably assure that critical program function integrity is not affected;

4. Routinely monitor the configuration.

5. Update systems in a timely manner to protect against known vulnerabilities.

6. Appropriately document, test, and approve emergency changes to the configuration.

In addition, NIST SP 800-100 provides guidance in assessing related configuration management programmatic areas of capital planning and investment control, and security services and product acquisition. This publication discusses practices designed to help security management identify funding needs to secure systems and provide strategies for obtaining the necessary funding. Also, it provides guidance to entities in applying risk management principles to assist in the identification and mitigation of risks associated with security services acquisitions.

Control Techniques and suggested audit procedures for AS-3

Table 41. Control Techniques and suggested audit procedures for AS-3. Implement Effective Application Configuration Management

Control activities	Control techniques	Audit procedures
AS-3.1 Policies and procedures are designed to reasonably assure that changes to application functionality in production are authorized and appropriate, and unauthorized changes are detected and reported promptly.	AS-3.1.1 Appropriate policies and procedures are established for application configuration management.	Inspect documented policies and procedures related to application change control procedures. Through inquiry and inspection, identify key transactions that provide user access to change application functionality. Inspect transaction reports of changes made to the application. From a selection of changes, inspect documentation of the changes made, including the validity, reasons, authorization, and the user authority. Note the handling of exceptions.
AS-3.2 Current configuration information is maintained.	AS-3.2.1 The entity maintains information on the current configuration of the application.	Review the entity's configuration management information.
AS-3.3 A system development life cycle methodology has been implemented.	AS-3.3.1 A SDLC methodology has been developed that • provides a structured approach consistent with generally accepted concepts and practices, including active user involvement throughout the process, • is sufficiently documented to provide guidance to staff with varying levels of skill and experience, • provides a means of controlling changes in requirements that occur over the system life, and • includes documentation requirements.	Review SDLC methodology. Review system documentation to verify that SDLC methodology was followed.
AS-3.4 Authorizations for changes are documented and maintained.	AS-3.4.1 change request forms are used to document requests and related projects.	Identify recent software modification and determine whether change request forms were used.
	AS-3.4.2 Change requests must be approved by both system users and IT staff.	Examine a selection of software change request forms for approval.
AS-3.5 Changes are controlled as programs progress through testing to final approval.	AS-3.5.1 Test plan standards have been developed for all levels of testing that define responsibilities for each party (e.g., users, system analysis, programmers, auditors, quality assurance, library control).	Perform the following procedures to determine whether control techniques AS-3.5.1 through AS-3.5.9 are achieved. Review test plan standards. Examine a selection of recent software changes and • review specifications; • trace changes from code to design specifications;

Control activities	Control techniques	Audit procedures
	AS-3.5.2 Detailed system specifications are prepared by the programmer and reviewed by a programming supervisor.	• review test plans; • compare test documentation with related test plans; • analyze test failures to determine if they indicate ineffective software testing; • review test transactions and data; • review test results; • verify user acceptance; and • review updated documentation. Determine whether operational systems experience a high number of abends and if so, whether they indicate inadequate testing prior to implementation.
	AS-3.5.3 Software changes are documented so that hey can be traced from authorization to the final approved code.	
	AS-3.5.4 Test plans are documented and approved that define responsibilities for each party involved.	
	AS-3.5.5 Unit, integration, and system testing are performed and approved • in accordance with the test plan and • applying a sufficient range of valid and invalid conditions.	
	AS-3.5.6 A comprehensive set of test transactions and data is developed that represents the various activities and conditions that will be encountered in processing.	
	AS-3.5.7 Test results are reviewed and documented.	
	AS-3.5.8 Program changes are moved into production only upon documented approval from users and system development management.	
	AS-3.5.9 Documentation is updated when a new or modified system is implemented.	
AS-3.6 Access to program libraries is restricted.	AS-3.6.1 Separate libraries are maintained for program development and maintenance, testing, and production programs.	Examine libraries to determine whether separate libraries are used for development and maintenance, testing, and production.
	AS-3.6.2 Source code is maintained in a separate library.	Verify source code exists for a selection of production code modules by (1) comparing compile dates, (2) recompiling the source modules, and (3) comparing the resulting module size to production load module size.
	AS-3.6.3 Access to all programs, including production code, source code, and extra program copies are protected by access control software and operating system features.	For critical software production programs, determine whether access control software rules are clearly defined. Test access to program libraries by examining security system parameters.

Control activities	Control techniques	Audit procedures
AS-3.7 Movement of programs and data among libraries is controlled.	AS-3.7.1 A group independent of the user and programmers control movement of programs and data among libraries. Before and after images of program code are maintained and compared to ensure that only approved changes are made.	Review pertinent policies and procedures. For a selection of program changes, examine related documentation to verify that • procedures for authorizing movement among libraries were followed, and • before and after images were compared.
AS-3.8 Access to application activities/ transactions is controlled via user roles (access privileges).	AS-3.8.1 User accounts are assigned to a role in the application. Roles are designed and approved by management to provide appropriate access and prevent an unauthorized user from executing critical transactions in production that change application functionality.	Inspect system reports and identify users who have access to configuration transactions. For a selection of users identified above, inspect user authorization forms to determine whether the user's access was authorized.
AS-3.9 Access to all application programs/codes and tables are controlled.	AS-3.9.1 Changes to application programs, codes and tables are either restricted or denied in the production environment. All changes are made using the approved change control process. User access to the application programs, codes, and tables is provided only for emergency user IDs.	Through inquiry and inspection, identify key programs and tables for the application. Inspect system reports of users with access to the key programs, codes and tables. Select users that have access to the identified programs and tables. Inspect documentation supporting how the access was provided. Note exceptions.

Control activities	Control techniques	Audit procedures
AS-3.10 Access to administration (system) transactions that provide access to table maintenance and program execution is limited to key users.	AS-3.10.1 Security design includes consideration for sensitive administration (system) transactions and restricted user access to these transactions.	Inspect policies and procedures regarding restricted access to system administration transactions. Through inquiry and inspection, identify the system administration transactions. Inspect system reports of user access to these transactions. Select users with administration access and inspect documentation to determine whether access was authorized. Select system administration transactions executed by the system users and inspect resulting changes to the system elements, such as the program code or table. Inspect critical or privileged IDs (e.g., fire call ID) to determine if activity is logged.
AS-3.11 Access and changes to programs and data are monitored.	AS-3.11.1 Procedures are established to reasonably assure that key program and table changes are monitored by a responsible individual who does not have the change authority. The procedures provide the details of reports/logs to run, specific valuation criteria and frequency of the assessment.	Inspect documented procedures related to monitoring change control. Select reports or logs that are reviewed, and inspect to note evidence of monitoring compliance.
AS-3.12 Changes are assessed periodically.	AS-3.12.1 Periodic assessment of compliance with change management process, and changes to configurable objects and programs.	Inspect evidence of documented assessments performed. Determine who performed the assessment and note the exception handling procedures.
AS-3.13 Applications are updated on a timely manner to protect against known vulnerabilities.	AS-3.13.1 The entity follows an effective process to identify vulnerabilities in applications and update them.	Determine whether vendor supplied updates have been implemented. Assess management’s process for identifying vulnerabilities and updating applications.
AS-3.14 Emergency application changes are properly documented, tested, and approved.	AS-3.14.1 The entity follows an effective process to properly document, test, and approve emergency changes.	Inspect evidence of proper documentation, testing, and approval of emergency changes.

Source: GAO.

Critical Element AS-4. Segregate user access to conflicting transactions and activities and monitor segregation

Effective segregation of duties is designed to prevent the possibility that a single person could be responsible for diverse and critical functions in such a way that errors or misappropriations could occur and not be detected in a timely manner, in the normal course of business processes. Although segregation of duties alone will not adequately assure that only authorized activities occur, inadequate segregation of duties increases the risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, and computer resources damaged or destroyed. As discussed in AS-1, the security plan should address the organization-wide policy on segregation of duties (segregation of duty) and management should organize the user departments to achieve adequate segregation of duties. As part of this process, most organizations adopt segregation of duties control matrices as a guideline of the job responsibilities that should not be combined. It is important for the auditor to assess the relationship among various job functions, responsibilities and authorities in assessing adequate segregation of duties. The auditor starts this assessment with the review of the control matrices defined by management. Several automated tools are available to dynamically manage segregation of duty conflicts within an application. Appropriate business rules are critical to the effective implementation of these tools.

Entity management should consider the organization structure and roles in determining the appropriate controls for the relevant environment. For example, an organization may not have all the positions described in the segregation of duties matrix, or one person may be responsible for more than one of the roles described. Based on the organizational resource limitation and risk management, certain levels of segregation of duty conflicts may be allowed by management for a select role or users. If so, management should have appropriate compensating controls in place to mitigate the risks of allowing the conflicts.

Appropriate segregation of duties often presents difficulties in smaller organizations. Even entities or locations that have only a few employees, however, can usually divide their responsibilities to

achieve the necessary checks and balances. More often than not, the auditor will encounter situations where a few to substantial number of users may have access to activities with segregation of duty conflicts. Management generally mitigates the risks of allowing the segregation of duty conflicts by adding compensatory controls, such as approval of transactions before they are entered in the application or review of the posted transactions or reports as direct oversight and close monitoring of the incompatible activities. Typically, a combination of access and monitoring controls is necessary for design and operational effectiveness.

Compensating controls are internal controls that are intended to reduce the risk of an existing or potential control weakness when duties cannot be appropriately segregated. Compensating controls for segregation of duties conflicts generally include additional monitoring and supervision of the activities performed by the individual possessing conflicting responsibilities, and may include an additional level of required approval. The segregation of duty conflicts are mitigated to reduce or eliminate business risks through the identification of compensating controls.

Effective segregation of duties, consistent with Section 3.4, Segregation of Duties (SD), includes the following steps:

- Segregate user access to conflicting transactions and activities
- Monitor user access to conflicting transactions and activities through formal operating procedures, supervision, and review

Control Techniques and Suggested Audit Procedures For Critical Element AS-4

Table 42. Control Techniques and Suggested Audit Procedures For Critical Element AS-4.- Segregate user access to conflicting transactions and activities and monitor segregation

Control activities	Control techniques	Audit procedures
AS-4.1 Incompatible activities and transactions are identified	AS-4.1.1 Owners have identified incompatible activities and transactions, and documented them on a segregation of duty matrix.	Through inquiry of management and inspection of policies and procedures, understand how management identifies incompatible activities and transactions.
	AS-4.1.2 Owners have appropriately considered risk acceptance when allowing segregation of duty conflicts in user roles.	Inspect list of segregation of duty conflicts to determine whether management has identified the segregation of duty conflicts appropriate for the business process and considered risk acceptance when allowing the conflicts.
AS-4.2 Application controls prevent users from performing incompatible duties.	AS-4.2.1 Users are prevented by the application from executing incompatible transactions, as authorized by the business owners.	Through inquiry, observations, and inspection, determine how the application segregates users from performing incompatible duties. Obtain and inspect a listing of users with access to the application. For a selection of users (can use same selection as in AS-2.4.1, AS-2.4.3 & AS-2.6.3), inspect documentation to determine whether access to menus/ screens corresponds with the user's defined duties. Evaluate whether their duties and access is appropriate to prevent employees from performing incompatible duties. Specifically, perform the following steps: • Obtain a system-generated user listing for the application (and other applications, if applicable); • For a selection of users, inspect their access profiles to determine whether access is appropriate (e.g., users have update access); and • For the selection of users, inspect their access profiles to determine if any of the users have access to menus with conflicting duties.

Control activities	Control techniques	Audit procedures
AS-4.3.3 There is effective segregation of duties between the security administration function of the application and the user functions.	AS-4.3.1 The profiles for security administrators do not have privileges to input and/or approve transactions.	Based on the inspection of user profiles, determine if: • individuals with security administration functions have access to input, process, or approve transactions; • security administrators have access to more than application security administration functions; and • security administrators are prevented from accessing production data.
AS-4.4 User access to transactions or activities that have segregation of duties conflicts is appropriately controlled.	AS-4.4.1 Owners authorize users to have access to transactions or activities that cause segregation of duty conflicts only when supported by a business need.	Inspect user administration policy to determine whether owner approval is required to access transactions or activities in their area of responsibility. Obtain and inspect a system report of users with conflicting responsibilities within the application. From a selection of user access request forms (electronic documents/workflow, if applicable) verify that the owners have approved user access to appropriate transactions or activities.
	AS-4.4.2 Security Administrators review application user access authorizations for segregation of duties conflicts and discuss any questionable authorizations with owners.	Interview security administrators and observe and inspect relevant procedures and documentation. If the security administrator's review is documented on the request form, inspect a selection of forms to note evidence of the security administrator's review.
	AS-4.4.3 Owners periodically review access to identify unauthorized segregation of duties conflicts and determine whether any authorized segregation of duties conflicts remain appropriate.	Interview owners and inspect documentation; determine whether appropriate procedures are in place to identify and remove or modify access, as needed.
AS-4.5 Effective monitoring controls are in place to mitigate segregation of duty risks	AS-4.5.1 Process Owner has identified the segregation of duty conflicts that can exist, and the roles and users with conflicts.	Inspect documentation of roles and users with conflicts.

Control activities	Control techniques	Audit procedures
	AS-4.5.2 Documented monitoring controls are in place that specifically address the conflict that the control mitigates.	Identify segregation of duty conflicts (including those that were intentionally established by the entity) and review documentation to determine whether: • monitoring controls adequately mitigate the risks created by the segregation of duty conflict; and • monitoring controls are effective. This can be achieved by inspecting the evidence collected by management.
	AS-4.5.3 Management has documented evidence of monitoring of control effectiveness.	Review evidence of monitoring of control effectiveness.

Source: GAO.

Critical Element AS-5. Implement effective application contingency planning

Chapter 3 addresses Contingency Planning at an entitywide and system level and is focused on the total information resources of an entity. Audit steps for the following section should be performed in conjunction with Chapter 3, which provides a more in-depth discussion of contingency planning issues. FISMA requires that each federal agency implement an information security program that includes "plans and procedures to ensure continuity of operations for information systems that support the operation and assets of the agency." Effective application contingency planning, consistent with Section 3.5, Contingency Planning (CP),

- Assess the criticality and sensitivity of computerized operations and identify supporting resources
- Take steps to prevent and minimize potential damage and interruption
- Develop and document a comprehensive contingency plan
- Periodically test the contingency plan and adjust it as appropriate

OMB Circular A-130, Appendix III, requires contingency plans for major applications, and NIST provides relevant guidance in Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*.[110]

Assess the criticality and sensitivity of the application

A key step in the contingency planning process is to conduct a Business Impact Analysis (BIA) for the application under focus.[111] The NIST contingency planning guide presents a three-step BIA process, which is discussed in Chapter 3 at the entitywide level. Following this process, staff conducting the BIA should, first, determine the critical functions performed by the application and then identify the specific IT resources required to perform the functions. Invariably, critical IT resources, in part, can include hardware and network components and telecommunication connections, as well as key application data and programs which should be backed up regularly. Second, staff should identify disruption impacts and allowable outage times for the application. And, third, staff should develop recovery priorities that will help determine recovery strategies. The NIST guide provides a range of recovery strategy considerations, including alternate sites of varying operational readiness, reciprocal agreements with other organizations, and service level agreements with equipment vendors.

Take steps to prevent and minimize potential damage and interruption.

The entity should implement policies and procedures to prevent or minimize potential damage and interruption to critical systems, including appropriate backup of application programs and data. Such policies and procedures should be incorporated into the entity's entitywide contingency planning efforts.

[110]In addition, this Circular requires and the NIST guide recommends a plan for general support systems.

[111]NIST defines **Business Impact Analysis (BIA)** as follows: An analysis of an information technology (IT) system's requirements, processes, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.

Develop and document an application contingency plan.

A key step following the BIA is to develop the application contingency plan (which NIST refers to as an IT contingency plan) and incorporate it into related plans. The NIST guide provides a discussion of various related types of plans, but recognizes that universally accepted definitions are not available, and the scope and purpose of a plan at an organization may vary from the definition provided in the NIST guide. The application contingency plan is focused on one application and may address recovery procedures at an alternative site. However, it probably will not address the recovery of a major processing facility supporting multiple applications, nor the continuity or recovery of business functions relying on multiple applications. Therefore, an entity's Disaster Recovery Plan for a major processing facility may cover multiple applications and establish recovery priorities by application. Likewise, an entity's business functions involving multiple applications may have Business Continuity and Recovery Plans that incorporate multiple contingency plans for applications. It is important that an application contingency plan be incorporated into broader-scoped, related plans so that the application receives proper priority among multiple applications. The application contingency plan should also include time-based implementation procedures so that recovery activities are performed in a logical sequence and reflect the application's allowable outage times to avoid significant impacts. Contingency plans should include consideration of alternate work sites.

No application contingency plan could be activated without the availability of key data and programs. Therefore, application data should be backed up regularly and current programs should be copied and available for use. Both should be safeguarded, stored offsite, and be retrievable when recovery actions are implemented. The NIST guide provides a discussion of backup methods and considerations.

The entity should prevent and minimize potential damage and interruption. Chapter 3 includes a discussion of steps as the entitywide and system levels. In addition, for applications, the entity should maintain appropriate backup of applications and application data. Also, it is important that restarts process data completely and accurately.

Further, when an application contingency plan has been activated, responsible contingency personnel should reasonably assure that effective controls will restrict and monitor user access to application data and programs during the contingency operation. If adequate preparations have not been made or proper procedures are not followed, the contingency plan activation could result in an operational application with vulnerabilities that might allow unauthorized access to data and programs. As examples, access control software may not be started or allow default passwords, outdated software lacking up to date patches and containing known weaknesses may be activated, and logging of auditable events may not occur.

The control environment for the contingency operation should be similar to the normal operation. In particular, access controls as specified in the previous section AS-2 should be operating. That is, contingency operations should provide for effective user identification and authentication, proper authorization to perform sensitive transactions, and a continuing audit and monitoring capability.

Periodically test the contingency plan and adjust it as appropriate.

Testing the application contingency plan is essential to ensure it will function as intended when activated for an emergency. Testing can reveal important weaknesses. Testing the contingency plan and making adjustments as needed helps ensure the application will work when the contingency plan is implemented for an actual emergency. The NIST contingency planning guide recommends the following areas to be addressed in a contingency test:

- System recovery on an alternate platform from backup media
- Coordination among recovery teams
- Internal and external connectivity
- System performance using alternate equipment
- Restoration of normal operations
- Notification procedures

NIST's Handbook on Computer Security[112] discusses various degrees of contingency plan tests that could range from 1) a simple accuracy review to determine that key personnel contacts are still employed by the entity to 2) disaster simulations. On disaster simulations, this Handbook states the following: "These tests provide valuable information about flaws in the contingency plan and provide practice for a real emergency. While they can be expensive, these tests can also provide critical information that can be used to ensure the continuity of important functions. In general, the more critical the functions and the resources addressed in the contingency plan, the more cost-beneficial it is to perform a disaster simulation."

The NIST contingency planning guide states that test results and lessons learned should be documented and reviewed. The guide further states that, to be effective, the plan should be maintained in a ready state that accurately reflects the system, requirements, procedures, organizational structure, and policies and, therefore, the plan should be reviewed and updated regularly, at least annually or whenever significant changes occur.

[112] Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*

Control Techniques And Suggested Audit Procedures For Critical Element AS-5

Table 43. Control Techniques And Suggested Audit Procedures For Critical Element AS-5. Implement effective application contingency planning

Control activities	Control techniques	Audit procedures
AS-5.1 Assess the criticality and sensitivity of the application through a Business Impact Analysis (BIA) or equivalent.	AS-5.1.1 Determine the critical functions performed by the application and identify the IT resources, including key data and programs, required to perform them.	Perform the following procedures for AS-5.1.1 to AS-5.1.3. Review the policies and methodology, and the BIA (if conducted) used to determine the application's critical functions and supporting IT resources, the outage impacts and allowable outage times, and the recovery priorities. Interview program, information technology, and security administration officials. Determine their input and assessment of the reasonableness of the results.
	AS-5.1.2 Identify the disruption impacts and allowable outage times for the application.	
	AS-5.1.3 Develop recovery priorities that will help determine recovery strategies.	
AS-5.2 Take steps to prevent and minimize potential damage and interruption.	AS-5.2.1 Backup files of key application data are created on a prescribed basis.	Review written policies and procedures for backing up and storing application data and programs.
	AS-5.2.2 Current application programs are copied and available for use	Examine the backup storage site.
	AS-5.2.3 Backup files of application data and programs are securely stored offsite and retrievable for contingency plan implementation	Interview program and information technology officials and determine their assessment of the adequacy of backup policy and procedures.
AS-5.3 Develop and document an application Contingency Plan	AS-5.3.1 Develop a time-based application Contingency Plan.	Review the application contingency plan and broader scoped related plans.
	AS-5.3.2 Incorporate the application Contingency Plan into related plans, such as the Disaster Recovery, Business Continuity, and Business Resumption Plans.	Determine whether the broader-scoped plans have incorporated the application contingency plan. Compare the plan with guidance provided in NIST SP 800-34. Interview program, information technology, and security administration officials and determine their input and assessment of the reasonableness of the plan.

Control activities	Control techniques	Audit procedures
	AS-5.3.3 Contingency operations provide for an effective control environment by restricting and monitoring user access to application data and programs, including. • Users are identified and authenticated. • Users are properly authorized before being able to perform sensitive transactions. • Audit and monitoring capabilities are operating.	Interview program, information technology, and security administration officials. Determine their assessment for providing an effective control environment during contingency operations. Review the contingency plan and any test results for control related issues.
AS-5.4 Periodically test the application contingency plan and adjust it as appropriate.	AS-5.4.1 The application contingency plan is periodically tested and test conditions include disaster simulations.	Review policies on testing. Determine when and how often contingency plans are tested.
	AS-5.4.2 The following areas are included in the contingency test: • System recovery on an alternate platform from backup media • Coordination among recovery teams • Internal and external connectivity • System performance using alternate equipment • Restoration of normal operations • Notification procedures	Determine if technology is appropriately considered in periodic tests of the contingency plan and resultant adjustments to the plan. Review test results. Observe a disaster recovery test.
	AS-5.4.3 Test results are documented and a report, such as a lessons-learned report, is developed and provided to senior management.	Review the final test report. Interview senior management to determine whether they are aware of the test results.
	AS-5.4.4 The contingency plan and related agreements and preparations are adjusted to correct any deficiencies identified during testing.	Review any documentation supporting contingency plan adjustments.

Source: GAO.

4.2. Business Process Controls (BP)

Business Process controls are the automated and/or manual controls applied to business transaction flows and relate to the completeness, accuracy, validity and confidentiality of transactions and data during application processing. They typically cover the structure, policies, and procedures that operate at a detailed business process (cycle or transaction) level and operate over individual transactions or activities across business processes. Specific types of business process controls are:

- **Transaction Data Input** relates to controls over data that enter the application (e.g., data validation and edit checks).
- **Transaction Data Processing** relates to controls over data integrity within the application (e.g., review of transaction processing logs).
- **Transaction Data Output** relates to controls over data output and distribution (e.g., output reconciliation and review).
- **Master Data Setup and Maintenance** relates to controls over master data, the key information that is relatively constant and shared between multiple functions or applications (e.g., vendor file).

The particular control techniques employed by an entity will depend on the context of the business process and its associated risks and objectives. Business process controls may be manual or automated. Automated controls are system-based, and may be used to control such things as the correctness or accuracy of data, such as edits and validations. Manual controls are procedures that require human intervention, such as the approval of a transaction, and are typically used to assure the reasonableness or propriety of transactions. Automated and manual controls can be preventive or detective. Automated controls can keep invalid data from being processed, and they can report transactions that fail to meet reasonableness criteria. Manual controls performed prior to input can identify problems before data is processed, while monitoring controls performed after processing can identify errors.

In many entities, the core business processes span across multiple applications. Some of the applications are themselves complex, integrated systems. Ideally, applications are interfaced seamlessly for the information to flow across these applications to complete a business process. Furthermore, functional areas may expand outside of the organization to include external “partners” as part of a larger vendor/contract management or personnel management, wherein partner applications are often interfaced with entity systems. This expansion of the environment to include external systems adds to the risks or challenges faced by the organization. If not properly controlled, these interfaces with external “partners” can affect the confidentiality, integrity, and availability of information and information systems. Business process controls are not limited to financial systems. For example, these controls are essential to ensuring the completeness, accuracy, validity and confidentiality of non-financial data such as patient health information.

At a high level, execution of a business process involves data input, processing and data output. However, the characteristics of data types (master or standing data and transaction data), and the complexity of the interfaced systems and the underlying data management systems, require the auditor to consider these in evaluating the completeness, accuracy, validity and confidentiality of data.

Master Data vs. Transaction Data

Every business process employs **master data**, or referential data that provides the basis for ongoing business activities, e.g., customers, vendors, and employees. The data that are generated as a result of these activities are called **transaction data**, and represent the result of the activity in the form of documents or postings, such as purchase orders and obligations.

Examples of master data are:

- Organizational structure
- G/L Account Structure

- Vendor Master
- Employee Master

Financially focused master data generally has the following characteristics:

- Relatively stable over time; even if the data records change, the overall volume of growth is limited. Example: chart of accounts, fixed assets, and vendors.

- Occur only once per object in the application. Example: assets are used by almost every organizational unit, but there is only one master record per asset.

- Everything else depends on them, e.g. inventory balances cannot be loaded without the organizational structure, G/L accounts, and material master being loaded. Therefore, master data should be loaded prior to processing business transactions.

Business Process Application Control Objectives

As discussed in the introduction to this chapter, the overall objectives of business process application level controls are to reasonably assure completeness, accuracy, validity, confidentiality, and availability[113] of transactions and data during application processing. The completeness, accuracy, and validity controls relate to the overall integrity objective. In particular, each specific business process control technique is designed to achieve one or more of these objectives. The effectiveness of business process controls depends on whether all of these overall objectives are

[113]Availability controls are principally addressed in application security controls (especially contingency planning) and therefore, are not included as specific business process application control objectives in the business process controls (BP), interface controls (IN), and data management system controls (DA) categories. The completeness, accuracy, and validity controls relate to the overall integrity objective. The availability objective is addressed as part of application level general controls in AS-5.

achieved by the application level controls. Each objective is described in more detail below.

Completeness (C) controls should provide reasonable assurance that all transactions that occurred are input into the system, accepted for processing, processed once and only once by the system, and properly included in output. Completeness controls include the following key elements:

- transactions are completely input,
- valid transactions are accepted by the system,
- duplicate postings are rejected by the system,
- rejected transactions are identified, corrected and re-processed; and
- all transactions accepted by the system are processed completely.

The most common completeness controls in applications are batch totals, sequence checking, matching, duplicate checking, reconciliations, control totals and exception reporting.

Accuracy (A) controls should provide reasonable assurance that transactions are properly recorded, with the correct amount/data, and on a timely basis (in the proper period); key data elements input for transactions are accurate; and data elements are processed accurately by applications that produce reliable results; and output is accurate.

Accuracy control techniques include programmed edit checks (e.g., validations, reasonableness checks, dependency checks, existence checks, format checks, mathematical accuracy, range checks, etc.), batch totals and check digit verification.

Validity (V) controls should provide reasonable assurance (1)that all recorded transactions actually occurred (are real), relate to the organization, and were properly approved in accordance with management's authorization; and (2) that output contains only valid

data. A transaction is valid when it has been authorized (for example, buying from a particular supplier) and when the master data relating to that transaction is reliable (for example, the name, bank account and other details on that supplier). Validity includes the concept of authenticity. Examples of validity controls are one-for-one checking and matching.

Confidentiality (CF) controls should provide reasonable assurance that application data and reports and other output are protected against unauthorized access. Examples of confidentiality controls include restricted physical and logical access to sensitive business process applications, data files, transactions, and output, and adequate segregation of duties. Confidentiality also includes restricted access to data reporting/extraction tools as well as copies or extractions of data files.

User Satisfaction Inquiry

Auditors may find it useful to query key system users on their satisfaction with business process information (transaction output). Users of business process information can help the auditor identify errors in processing or other major problem areas. The auditor should identify and interview enough principal users to develop a general idea of how they use the data and what their opinions are concerning its accuracy, timeliness, and completeness. Questions that may be used to collect information from the user include the following.

- For what purpose do you use the transaction output?
    - initiate transaction,
    - authorize changes to the system,
    - maintain information controls, or
    - other?
- Can the transaction output be used without correction?

- Is the information accurate and reliable, available when needed, current and up-to-date?
- Do you maintain manual records to supplement the transaction output?
- Do you check the information for quality (accuracy completeness, and validity) when you receive it?
- Is the transaction output ever rerun by the data center?
- Are you authorized to make changes to the information and if so, can you override validation and edit checks incorporated into the business process application?

When assessing user satisfaction, it is important to obtain evidence of incomplete or inaccurate data identified by a user. The auditor should determine

- the nature of the problem – amounts overstated or understated, incorrect totals, incomplete data fields, and negative balances which should be positive;
- how frequently errors are observed – isolated instances or recurring problems;
- whether the user can help explain why errors are made – since errors affect users the most, they may have conducted studies to show the cause and magnitude of errors; and
- whether users maintain manual records for use instead of computer reports or output – manually kept records may indicate problems with the integrity of the transaction output.

NIST Guidance

For federal systems, NIST SP 800-53 includes the following controls related to business process controls:

SI-9	Information Input Restrictions
SI-10	Information Accuracy, Completeness, Validity, and Authenticity
SI-11	Error Handling
SI-12	Information Output Handling and Retention

This section presents more detailed control objectives that should be achieved to reasonably assure that transaction data is complete, accurate, valid and confidential. Also, this section is organized to address the four principal types of business process controls: input, processing, output, and master files.

Business Process Control Critical Elements

Business Process Controls have the following four critical elements:

BP-1	Transaction Data Input is complete, accurate, valid, and confidential (Transaction data input controls).
BP-2	Transaction Data Processing is complete, accurate, valid, and confidential (Transaction data processing controls).
BP-3	Transaction Data Output is complete, accurate, valid, and confidential (Transaction data output controls).
BP-4	Master data setup and maintenance is adequately controlled.

Critical Element BP-1. Transaction Data Input is complete, accurate, valid, and confidential (Transaction Data Input Controls)

The entity should implement procedures to reasonably assure that (1) all data input is done in a controlled manner, (2) data input into the application is complete, accurate, and valid, (3) any incorrect information is identified, rejected, and corrected for subsequent processing, and (4) the confidentiality of data is adequately protected. Inadequate input controls can result in incomplete, inaccurate, and/or invalid records in the application data or unauthorized disclosure of application data.

Applications can accept input manually (application users enter data), or via automated input. In either case data input controls are relevant. The automated input may be interfaces that use batch processing or

are integrated real-time with internal and external systems. To the extent that data input is obtained from other applications, the auditor's assessment of input controls should be coordinated with data interface controls discussed in section 4.3 of this chapter.

For federal systems, NIST SP 800-53 [SI-10] establishes the following objectives for input controls:

- checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible.
- rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content.
- inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands.

Also, SI-10 states that the extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements.

Data input for processing should have all key fields completed and be validated and edited. Error handling procedures should facilitate timely resubmission of corrected data, including real-time on-line edits and validations. These controls may be configured within the system settings, or added on as a customization. Where applicable, the auditor may also process a controlled group of live data and test for expected results. However, when using live data even in a controlled environment, the auditor should use additional safeguards to ensure that the data is not compromised (e.g., breaches that may impact the accuracy, completeness, and validity of the information or loss of confidentiality (privacy issue)). Preventive controls generally allow for higher reliance and the most efficient testing.

In addition, controls should be in place to reasonably assure that access to data input is adequately controlled. Procedures should be

implemented to control access to application input routines and physical input media (blank and completed). The assessment of such controls should be coordinated with Critical Element AS-2 *Implement effective application access controls.*

For federal systems, NIST SP 800-53 includes three controls relevant to transaction data input:

SI-9	Information Input Restrictions
SI-10	Information Accuracy, Completeness, Validity, and Authenticity
SI-11	Error Handling

Data input controls are comprised of the following control activities:

- Implement an effective transaction data strategy and design
- Establish input preparation (approval and review) policies and procedures
- Build data validations and edit checks into the application
- Implement effective auditing and monitoring capability

Implement an effective transaction data strategy and design

The entity should have an appropriate data strategy and design (how the data are organized into structures to facilitate retrieval while minimizing redundancy). The design of transaction data elements is a critical factor in helping to assure the quality of data as well as its interrelationship with other data elements. Data standards[114] should be defined and maintained, but may vary depending upon the specific requirements of the entity, including regulatory requirements, and database- or application-based standards.

[114]Data standards are designed to enable systems to easily interoperate and transfer information. Standard definitions for data elements are intended to ensure that users of all entity systems define the same data in the same way and have a common understanding of their meaning.

A clearly defined data strategy minimizes data redundancies fundamental to an efficient, effective transaction processing function. Poor data quality may lead to a failure of system controls, process inefficiencies, and inaccurate management reporting. Erroneous or missing elements of critical data in the transaction file can produce discrepancies within the process cycle.

Characteristics of erroneous transaction file data elements include, but are not limited to, duplicate transactions recorded or processed, and improper coding to departments, business units or accounts. They also include unpopulated data fields and data formatting inconsistencies, as described for the master file.

Establish Input Preparation (approval and review) Policies and Procedures

The entity should have policies and procedures in place to reasonably assure that all authorized source documents and input files are complete and accurate, properly accounted for, and transmitted in a timely manner for input to the computer system. Among these, management should establish procedures to reasonably assure that all inputs into the application have been processed and accounted for; and any missing or unaccounted for source documents or input transactions have been identified and investigated. Finally, procedures should be established to reasonably assure that all source documents (paper or electronic form) have been entered and accepted to create a valid transaction. Automatic input from other applications should be integrated either through an interface (external applications) or configuration (cross-modular within the same application). Interface controls are addressed in section 4.3, below.

For federal systems, NIST SP 800-53 [SI-9] establishes a control objective that the organization restricts the capability to input information to the information system to authorized personnel. Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

Build Data Validation and Edits within the Application

Input data should be validated and edited to provide reasonable assurance that erroneous data are prevented or detected before processing. In many cases, application owners and programmers will build application input edits directly into the application to limit the number of errors that are input into the application. Edits are used to help assure that data are complete, accurate, valid, and recorded in the proper format. Edits can include programming to identify and correct invalid field lengths or characters, missing data, incorrect data, or erroneous dates.

The auditor should obtain an understanding of the application input edits to assess their adequacy and to determine the edits that will be tested. This understanding would include a determination on whether edits can be overridden or bypassed and if allowed, whether such capability is restricted to supervisory personnel only and limited in its use. In addition, entity procedures should provide for the automatic logging of all edit overrides/bypasses and include subsequent routine analysis of these logs to assess their appropriateness and correctness by entity management. The auditor should also determine whether table maintenance procedures have been established that include edit and validation controls to ensure that only valid changes are made to data tables that may be incorporated into business process applications

Implement Effective Auditing and Monitoring Capability

As part of the data input process, data entry errors may occur. These errors can occur during manual or automated entry of data. Management should have procedures to identify and correct any errors that occur during the data entry process. Error handling procedures during data entry should reasonably assure that errors and irregularities are detected, reported, and corrected. Management's audit and monitoring capability should include

- user error logs[115] to provide timely follow-up and correction of unresolved data errors and irregularities, and

- an established monitoring process to assure the effectiveness of error handling procedures. This should include procedures to periodically review user error logs to determine the extent to which data errors are being made and the status of uncorrected data errors.

For federal systems, NIST SP 800-53 [SI-11] states that the information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries. The structure and content of error messages are carefully considered by the organization. Error messages are revealed only to authorized personnel. Error messages generated by the information system provide timely and useful information without revealing potentially harmful information that could be used by adversaries. Sensitive information (e.g., account numbers, social security numbers, and credit card numbers) are not listed in error logs or associated administrative messages. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Control Techniques and Suggested Audit Procedures for Critical Element BP-1

Table 44. Control Techniques and Suggested Audit Procedures for Critical Element BP-1. Transaction Data Input is complete, accurate, valid, and confidential.

Control activities	Control Object.	Control techniques	Audit procedures
BP-1.1 A transaction data strategy is properly defined, documented, and appropriate.	C,A,V, CF	BP-1.1.1 Data management procedures exist that include transaction data strategy, data design, data definitions, data quality standards, ownership and monitoring procedures. Data strategy should be unique to each data type.	Inquire of management and inspect documented policies and procedures related to data strategy. Inspect transaction data strategy.

[115]Error logs may be automated or manual. Automated logs generally provide more reporting consistency.

Control activities	Control Object.	Control techniques	Audit procedures
BP-1.2 Source documentation and input file data collection and input preparation and entry is effectively controlled.	C,V,CF	BP-1.2.1 Procedures are established to provide reasonable assurance that all inputs into the application have been authorized, accepted for processing, and accounted for; and any missing or unaccounted for source documents or input files have been identified and investigated. Such procedures may include one or more of the following: • batch totals • sequence checking • reconciliations • control totals	Through inquiry, observations, and inspection, obtain an understanding of policies and procedures related to source document and input file collection and preparation, and determine whether the procedures are documented and properly designed. Observe and inspect input preparation policies and procedures and relevant controls, noting procedures taken when exceptions are identified. Inspect a selection of reports used by management to determine whether the necessary inputs are accepted for processing, and inquire of review procedures used. Inquire as to how source documents and input files are tracked and maintained and inspect relevant documentation.
BP-1.3 Access to data input is adequately controlled	C,A,V, CF	BP-1.3.1 Procedures are implemented to control access to application input routines and physical input media (blank and completed)	Review procedures over control of data input to determine whether they are adequate. Coordinate this step with AS-2.
BP-1.4 Input data are approved	A, V	BP-1.4.1 Documented approval procedures exist to validate input data before entering the system. Approval procedures are followed for data input.	Inspect documented procedures for approval of input data. Inspect a selection of source documents and input files and determine whether the source data were approved for input.

Control activities	Control Object.	Control techniques	Audit procedures
BP-1.5 Input data are validated and edited to provide reasonable assurance that erroneous data are detected before processing.	A,V	BP-1.5.1 Appropriate edits are used to reasonably assure that data are valid and recorded in the proper format, including: • authorization or approval codes; • field format controls; • required field controls; • limit and reasonableness controls; • valid combination of related data field values; • range checks • mathematical accuracy • master file matching • duplicate processing controls; and • balancing controls.	Through inquiry, observations, and inspection, understand edits used to reasonably assure that input data is accurate, valid, and in the proper format prior to being accepted by the application. The edits and procedures should address both manual and automated input processes. Identify the key data input screens. Consider such factors as known errors and the frequency of use. If available, use analytical reports to support reasoning for screen selection. For the key manual input layouts identified, perform the following steps as applicable: • Observe an authorized data entry clerk inputting transactions, noting edits and validations for the various transaction entries. • Observe key transaction fields to determine whether they have adequate edit/validation controls over data input. • Obtain screen prints of appropriate scenarios and document the result. For key automated inputs, observe and inspect data validation processes, completion controls, and exception reports in place. Inquire of management regarding procedures used to reject and resubmit data for processing, and procedures to provide reasonable assurance that data is not processed multiple times. Note: audit procedures apply only to the current environment at the time of test. Supplemental audit procedures would need to be applied at other points during the year to obtain evidence that the control was operating effectively.)

Control activities	Control Object.	Control techniques	Audit procedures
		BP-1.5.2 Edit and validation overrides are restricted to authorized personnel. Procedures exist to monitor, in a timely manner, overrides applied to transactions, including maintenance of override logs.	Observe and inspect existing procedures for reviewer overrides or bypassing data validation and error routines. If an override log exists, observe and inspect to determining whether adequate review and follow up of overrides is performed. Inspect a selection of overrides for evidence of proper approval. (Note: use of overrides is not by itself indicative of inadequate controls. However, the auditor needs to examine why the overrides are being used and controls in place to minimize risks from these actions).
		BP-1.5.3 Table maintenance procedures include edit and validation controls to help assure that only valid changes are made to data tables.	Through inquiry, observations, and inspection, obtain an understanding of table maintenance procedures relative to data edits and validation. Observe an authorized person attempting to make invalid changes to tables, and confirm edits and validations are performed on changes.
BP-1.6 Input values to data fields that do not fall within the tolerances or parameters determined by the management result in an automated input warning or error.	A,V	BP-1.6.1 Parameters and tolerances are configured and error conditions and messages are defined. (These restrictions can be configured based on limits on transaction amounts or based on the nature of transactions) If a workflow is used so that documents can be released only by personnel with appropriate approval authority, then these requirements should be appropriately designed in the system. Management regularly reviews the restrictions placed on data input and validates that they are accurate and appropriate.	Inspect configuration of parameters and tolerance levels defined by the entity to identify whether the application accepts the data with warning or rejects the data, if the conditions are not met. Determine whether management review and follow-up of warnings are adequate. Inspect the workflow rules and validate that the releasing authority is at an appropriate level. Inspect evidence of management's regular review of relevant tolerances and parameters, and any correctional activities taken.

Control activities	Control Object.	Control techniques	Audit procedures
BP-1.7 Error handling procedures during data origination and entry reasonably assure that errors and irregularities are detected, reported, and corrected.	C,A,V	BP-1.7.1 Procedures are established to reasonably assure that all inputs into the application have been accepted for processing and accounted for; and any missing or unaccounted for source documents or input files have been identified and investigated. The procedures specifically require the exceptions to be resolved within a specific time period.	Inspect documented procedures related to data entry error handling procedures. Inquire of management to determine which key management reports are used to monitor input errors. Select input error reports and inspect to note evidence of management review. As applicable, inspect subsequent data input reports to note where data was corrected and resubmitted for processing.
BP-1.8 Errors are investigated and resubmitted for processing promptly and accurately.	C,A,V	BP-1.8.1 Data input errors are identified in suspense or error reports and resolved or resubmitted in a timely manner (within the period specified in the procedures).	Inspect a selection of recent suspense or error reports (can use selection used in BP-1.7.1 provided information included will satisfy audit objectives for both audit procedures) and note whether suspense items are being corrected in a timely manner. Inspect the open items and note management's reasons for not correcting them in a timely manner.

Source: GAO.

Critical Element BP-2. Transaction Data Processing is complete, accurate, valid, and confidential (Transaction Data Processing Controls)

Transaction data processing controls address the completeness, accuracy, validity, and confidentiality of data as the data get processed within the application. Data processing controls are employed following input, or during batch processing or on-line user processing within the application.

Once the initial data are entered in the system and accepted for processing, the processing of the data should be controlled by a series of activities within the system. These activities are designed by management and are either programmed or configured into the application. The processing steps are different for each process (purchasing versus invoice processing) and control requirements differ to mitigate the risks inherent to the applicable process. An effective assessment of data processing controls includes an understanding of the process steps and dataflow in a process cycle,

the controls imbedded in the application, and the manual controls that are common across processes or specific to each process.

Some applications may allow user-defined processing, whereby the user may establish or modify processing. This frequently occurs in applications based on spreadsheets and report writer/data extraction tools. Entities should establish clear policies and procedures concerning user-defined processing. In addition, the entity should have adequate controls over the accuracy, completeness and validity of information processed in applications with user-defined processing.

Audit trails and security reports should be monitored on a regular basis to help assure that transactions are processing as intended. The effectiveness of such procedures depends on the level of security reporting and problem analysis tools available in the application. Controls over the processing of data should preclude or detect the erroneous or unauthorized addition, removal, or alteration of data during processing.

Interface controls relate to the integrity of data as they move from one system to another. Interface controls are addressed separately in Section 4.3 below.

For federal systems, as noted in BP-1 above, NIST SP 800-53 includes three controls relevant to data processing:

SI-9	Information Input Restrictions
SI-10	Information Accuracy, Completeness, Validity, and Authenticity
SI-11	Error Handling

Formal Transaction Processing Procedures.

Formal procedures should be established for data processing to help assure that data are processed completely and accurately, that data retains its validity, and that appropriate data confidentiality is maintained during processing. Related controls include the following:

- Transaction or table logs provide an audit trail and the ability to compare transactions to source documents. Audit trails or processing logs are often used within applications to track the pertinent information related to application transactions, both manual and automated. The processing logs should also be used to identify those transactions that did not process completely or correctly within the application. The log should document the errors identified during application processing, and should contain enough information for the systems personnel to identify the exact transactions that failed, and the application users that will need to be contacted to correct the posting (if the error can not be corrected by the systems personnel). Processing logs typically contain such information as date and time of error, responsible user (if applicable), codes describing the type of error encountered, and the corrective action that has occurred to assure correct processing of the transaction.

- An automated process exists that allows one or more of the following: capturing transaction data in correct accounts; unique documentation; tolerances in processing data; periodic review and reconciliation of subsidiary or clearing accounts (e.g., clearing Goods Received accounts against Invoice Received accounts through two- and three-way matching process); prevention of direct posting to reconciliation accounts; and workflow to initiate the approval process.

- Efficient transaction entry that eliminates unnecessary duplication of data entry. Where appropriate, data needed by the systems are entered only once and other parts of the system are automatically updated consistent with the timing requirements of each process cycle.

- Managers should provide review and authorization for transactions that are rejected and should be rerun.

Effective auditing and monitoring capability.

During data processing, transactions may not be processed completely or accurately as a result of errors or inconsistencies in data, system interruptions, communication failures, or other events. In addition, valid data may be corrupted or data may lose its confidentiality. To identify these instances, a monitoring capability should be implemented. The monitoring function should reasonably assure that data are accurately processed through the application and that processing procedures determine data to be added, or altered during processing. No data should be lost during the process. Controls may include:

- If the application is "run" on a regular schedule to process data, either manually or automatically, there are documented procedures explaining how this is performed, including controls in place to reasonably assure that all processing was completed.
- A processing log is maintained and is reviewed on a regular basis for unusual or unauthorized activity.
- The processing log, or another log or report, is used to document any errors or problems encountered during processing. Types of information that should be considered for retention are descriptions of any errors encountered, dates identified, any codes associated with errors, any corrective action taken, date and times corrected.
- controls to reasonably assure that the correct generation/cycle of files is used for processing. This may include the generation of backup files from processing to be used for disaster recovery.
- Adequate audit trails are generated during processing. These audit trails should be logs or reports that contain information about each transaction. Data that should be included are who initiated each of the transactions, the date and time of the transactions, and the location of the transaction origination (terminal or IP address as an example).

Control Techniques and Suggested Audit Procedures for Critical Element BP-2

Table 45. Control Techniques and Suggested Audit Procedures for Critical Element BP-2. Transaction Data Processing is complete, accurate, valid, and confidential.

Control activities	Control Object.	Control techniques	Audit procedures
BP-2.1 Application functionality is designed to process input data, with minimal manual intervention.	C,A,V, CF	BP-2.1.1 Application processing of input data is automated and standardized. Design documentation supporting the processing design exists for validation and change control purposes. The version of application, data and files to be processed are appropriate and current.	Inspect configuration and/or design documentation noting automatic and manual processing of transaction and information flow. Verify that proper versions of application, data and file are used.
BP-2.2 Processing errors are identified, logged and resolved.	C, A, V	BP-2.2.1 System entries use transaction logs to reasonably assure that all transactions are properly processed and identify the transactions that were not completely processed.	Inspect a selection of application, transaction and error logs, noting whether all transactions were properly processed and missing or duplicate transactions were identified, including reruns and restarts.
		BP-2.2.2 Procedures are in place to identify and review the incomplete execution of transactions, analyze and take appropriate action.	Inspect selected incomplete transactions and validate that management has adequately investigated and corrected the errors or omissions. Conduct a test with controlled group of live data and analyze the results with the expected values. Follow up with any exceptions.
		BP-2.2.3 Procedures exist to monitor, in a timely manner, overrides applied to transaction processing.	Observe and inspect existing procedures for reviewer overrides or bypassing data processing routines. If an override log exists, observe and inspect to determining whether adequate review and follow up of overrides is performed. Inspect a selection of overrides for evidence of proper approval. (Note: use of overrides is not by itself indicative of inadequate controls. However, the auditor needs to examine why the overrides are being used and controls in place to minimize risks from these actions).

Control activities	Control Object.	Control techniques	Audit procedures
BP-2.3 Transactions are executed in accordance with the pre-determined parameters and tolerances, specific to entity's risk management.	A,V	BP-2.3.1 Document processing and posting conditions (parameters and tolerances) are configured, including system errors and actions, if the are conditions are not met.	Inspect configuration of parameters and tolerances levels defined by the entity to identify whether the application processes the data with warning or rejects the data, if the conditions are not met.
		BP-2.3.2 Management regularly reviews the restrictions to validate the accuracy and appropriateness.	Inspect management review procedures, noting management action when the application processes data or rejects it. In both cases, management should clearly analyze the impact on the downstream transactions.
BP-2.4 Transactions are valid and are unique (not duplicated).	A, V	BP-2.4.1 The application performs on-line edit and validation checks against data being processed.	Perform the following procedures for BP-2.4.1 to BP-2.4.4.
		BP-2.4.2 The system produces warning or error messages.	Inspect design document to identify key data validation and edit checks.
		BP-2.4.3 Transactions with errors are rejected or suspended from processing until the error is corrected.	Inspect configuration to verify that the identified edit and validations checks are appropriately set, and transactions are rejected/suspended when data/processing errors occur. Also verify that warning and error messages are designed when the processing is incomplete.
		BP-2.4.4 The application communicates the processing error to the users either on-line (if on-line entry) or via an exception report.	Inspect the error communication methodology and assess whether all processing errors are communicated to the users.
BP-2.5 The transactions appropriately authorized.	A,V	BP-2.5.1 Transactions are matched with management's general or specific authorizations.	Review the adequacy of controls over authorization of transactions.
BP-2.6 Data from subsidiary ledgers are in balance with the general ledger (step applicable to financial-related audits only).	C,A,V	BP-2.6.1 Periodic reconciliation is performed and exceptions are appropriately handled.	Inspect periodic procedures to determine whether reconciliations are performed and documented with evidence. For a selection of reconciliations, examine supporting evidence for adequacy. Through inquiry, observations, and inspection, determine if the system is configured to auto balance, where possible.
BP-2.7 User-defined processing is adequately controlled.	C, A, V, CF	BP-2.7.1 Appropriate policies and procedures over user-defined processing are implemented.	Review policies and procedures over user-defined processing.

Control activities	Control Object.	Control techniques	Audit procedures
		BP-2.7.2 Controls over user-defined processing are adequate.	Assess the operating effectiveness of user-defined processing.
BP-2.8 As appropriate, the confidentiality of transaction data during processing is adequately controlled	CF	BP-2.8.1 Management implements adequate controls to protect the confidentiality of data during processing, as appropriate.	Assess the adequacy of management controls over confidentiality during processing. Coordinate this step with Critical Element AS-2 *Implement effective application access controls.*
BP-2.9 An adequate audit and monitoring capability is implemented.	C,A	BP-2.9.1 Management has procedures in place to reconcile the data input with the data processed by the application.	Inspect procedures regarding reconciliation of transactions.
		BP-2.9.2 Monitoring procedures should provide details of data to be added/modified during the processing, and expected result. System audit logs should be reviewed for exception.	Inspect operations activity at selected times and check for evidence that reconciliations are being performed.
		BP-2.9.3 Management maintains a process log and the log is reviewed for unusual or unauthorized activity.	Inspect the processing log and note whether the unusual or unauthorized activity was followed up properly and promptly.
		BP-2.9.4 Procedures exist to monitor, in a timely manner, overrides applied to transactions, including maintenance of override logs.	Observe and inspect existing procedures for reviewer overrides or bypassing data validation and error routines. If an override log exists, observe and inspect to determine whether adequate review and follow-up of overrides is performed.

Source: GAO.

Critical Element BP-3. Transaction data output is complete, accurate, valid, and confidential (Transaction Data Output Controls)

Like input and processing controls, transaction data output controls are used to reasonably assure that transaction data is complete, accurate, valid, and confidential. In addition, output controls are aimed at the correct and timely distribution of any output produced. Output can be in hardcopy form, in the form of files used as input to other systems, or information available for online viewing.

Formal procedures should be established for data processing to help assure that data are processed completely and accurately, that data retains its validity, and that appropriate data confidentiality is maintained during processing, output control totals are accurate and

are being verified, and the resulting information is distributed in a timely and consistent manner to the appropriate end users. Controls include:

- An overall reporting process that identifies specific output that will be generated, the form and content of the reporting, sensitivity of information and selectivity of user.
    - Output is delivered to the appropriate end user.
    - Output is restricted from unauthorized access.
    - Record retention and backup schedules for output data should be established.
- Data integrity through reconciliation of the output to the input and processing data.
    - Documented procedures explain the methods for the proper balancing/reconciliation and error correcting of output should exist. There should be adequate separation of duties for the balancing/reconciliation process.
    - Output is reviewed for general acceptability and completeness, including any control totals. There should be either error reports or a log kept of output errors. These should contain information such as a description of problems/errors and the date identified, as well as any corrective action taken.

In addition, controls should be in place to reasonably assure that access to data output is adequately controlled. Procedures should be implemented to control access to output data and physical output media (blank and completed). The assessment of such controls should be coordinated with Critical Element AS-2 *Implement effective application access controls.*

For federal systems, NIST SP 800-53 includes three controls relevant to data output controls:

SI-10	Information Accuracy, Completeness, Validity, and Authenticity
SI-11	Error Handling
SI-12	Information Output Handling and Retention

In addition, NIST SP 800-53 [SI-12] states that the organization handles and retains output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Implementing a reporting strategy

One of the key elements of output controls is having an overall reporting strategy. The strategy helps to reasonably assure that content and availability of reports is consistent with end users' needs, that end users are aware of the sensitivity and confidentiality of data, and that an "owner" has been defined for all report output. The strategy also provides a basis for policies and procedures that govern preferred report methods (hardcopy vs. soft, standard vs. custom), report generation and distribution, and any review and or approvals.

The strategy should specifically consider:

- Compliance with laws and regulations;
- Sensitivity of data;
- Levels of reporting segregation of duties;
- Consolidation/ processing of reporting from a 3rd party;
- Reporting tools utilized;
- Business needs/functionality of reports; and
- Non-standard output items.

The strategy should adequately consider the confidentiality of all types of output. For example, the entity should have adequate security over output queues, particularly for sensitive information. Inadequately secured output queues can lead to unauthorized disclosure of information. Similarly, access to output screens should be adequately controlled.

Another significant area for output controls relates to data that is routinely or episodically transferred to other systems, such as data supporting a management reporting system. If controls over such other systems are not adequate and consistent with the risk level of the data, such data may be subject to unauthorized access. For example, personnel data transferred to a management reporting system should have adequate controls to achieve the confidentiality and integrity objectives.

Establishing security and controls over report generation and distribution.

Controls over report generation and distribution should include the following:

- Reports should be reviewed for reasonableness and accuracy prior to distribution.
- Output distribution should be controlled so that output is provided to authorized recipients only and on a timely basis.
- Report retention should be adequate based on internal needs and regulatory requirements. For example, application output may be stored to back-up tapes (or kept as hard copy documentation) and rotated to an offsite storage facility.
- Output reports comply with applicable laws and regulations, including the type of clearance required to view the output reports.
- User access to reports is controlled based on the user's business need to view the report and the sensitivity of information contained in the report.

- Data output to management reporting or other copies of output files are adequately controlled.

Control Techniques and Suggested Audit Procedures for Critical Element BP-3

Table 46. Control Techniques and Suggested Audit Procedures for Critical Element BP-3. Transaction data output is complete, accurate, valid, and confidential.

Control activities	Control Object.	Control techniques	Audit procedures
BP-3.1 Outputs are appropriately defined by the management (form, sensitivity of data, user selectivity, confidentiality, etc)	C,A,V,CF	BP-3.1.1 Management has developed a reporting strategy that includes the following: • content and availability that are consistent with end users' needs, • sensitivity and confidentiality of data • appropriate user access to output data.	Inquire of management about a reporting strategy or policy. Obtain a copy of any formal reporting strategy or policy. Assess the adequacy of the strategy and related policies.
BP-3.2 Output generation and distribution are aligned with the reporting strategy.	C,A,V,CF	BP-3.2.1 Management has procedures in place to reasonably assure that content and availability of output and data are consistent with end users' needs, sensitivity, laws and regulations, and confidentiality of data and valid user access.	Inspect management procedures for defining and assigning output/reports. Select key output/reports in the area of audit scope and verify the user access to the output/reports.
		BP-3.2.2 Management has procedures in place to monitor replication of output data used in management reports or other communications within or outside the entity.	Inquire of management on the use of data output. Inspect selected management reports or other communication to verify the accurate replication of data. Verify that the user received appropriate authorization to use the data.
		BP-3.2.3 User access to output data is aligned with the user's role and confidentiality/sensitivity of information.	Review user access to selected output data and assess the appropriateness of access.
BP-3.3 System generated outputs/reports are reviewed to reasonably assure the integrity of production data and transaction processing.	C,A,V	BP-3.3.1 Management has identified key reports to track processing results.	Perform the following procedures for BP-3.3.1 to BP-3.3.3. Inquire of user management and personnel to determine the key reports used to track processing results. Obtain and inspect reports identified by management in the above test to determine whether the reports exist and are reviewed on a timely basis.
		BP-3.3.2 Management has documented procedures to (1) review processed results, where applicable and (2) monitor, in a timely manner, overrides applied to transactions, including maintenance of override logs.	

Control activities	Control Object.	Control techniques	Audit procedures
		BP-3.3.3 Procedures are in place to review critical output data or control reports on a timely basis.	Observe and inspect existing procedures for reviewer overrides or bypassing data validation and error routines. If an override log exists, observe and inspect to determine whether adequate review and follow-up of overrides is performed.
BP-3.4 Output/ reports are in compliance with applicable laws and regulations.	C,A,V,CF	BP-3.4.1 Output reports for compliance with applicable laws and regulations are accurate, complete	Inspect a selection of output/reports for compliance with applicable laws and regulations. Identify laws and regulations that are to be complied with and verify that the reports are in compliance.
BP-3.5 Access to output/reports and output files is based on business need and is limited to authorized users.	CF	BP-3.5.1 Access to reports is restricted to those users with a legitimate business need for the information.	Perform the following procedures for BP-3.5.1 to BP-3.5.2. Select output/reports and output files from the audit area and inspect application access (if the output can be accessed on-line or other electronic form) or inspect distribution to determine whether the user has appropriate level of security clearance and is authorized to access.
		BP-3.5.2 Users should have appropriate authorization for accessing reports, including the appropriate level of security clearance, where applicable.	

Source: GAO.

Critical Element BP-4. Master Data Setup and Maintenance is Adequately Controlled

Master data are the key information that is constant and shared with multiple functions, such as a customer master record, which contains the customer number, shipping address, billing address, key contact and payment terms. Most applications use the following two types of master data:

Configurable master data or business rules are defined in an application module and used by end users, but cannot be changed directly in production. Purchase order release procedures (requiring approval) and payment terms are examples of business rules.

Business master data are master data created in production based upon the criteria designed to capture essential standing data, for example, customer and vendor master data.

Master data are, usually, entered once and are shared among various application modules. Also, common data fields may be used by the application several times over a period of time until the master data is no longer valid because of termination of a contractual agreement or data owner decision.

Three key control areas specific to master data controls are the controls related to design and configuration of master data (preventive), the procedures external to the system (detective and preventive), and the monitoring of master data design compliance (detective). Master data is also subject to access controls (activities to create and maintain master data are controlled by access privileges) discussed in AS-2.

The three key steps in master file setup and maintenance are:

- Implementing an effective design of master data elements
- Establishing master data maintenance procedures, including approval, review, and adequate support for changes to master data
- Implementing an effective auditing and monitoring capability

Implementing an effective design of master data elements

Master data elements should be designed to minimize the risk of erroneous master data. The effectiveness of master data design can be affected by the following:

- Centralized versus decentralized maintenance – centralized master data maintenance provides a greater control over creation and change of master data. It could, however, delay the process. Since most applications provide field or functional level access, it is possible for key data to be centrally maintained and functional specific data maintained by a unit. For example, vendor master data can be segmented into purchasing data and finance data, separately maintained by purchasing and finance departments, respectively.

- Partial edit – Master data maintenance may be controlled by rules that can be configured to prevent changes to certain areas of data, or key fields within a record.

- Numbering – System-assigned internal numbering is generally considered to be lower risk than external numbering, however, management can choose to use external numbering (to match numbers from an external system) and can choose naming conventions appropriate to its use. Adequate procedures should be in place to reasonably assure compliance with management's policy on numbering/naming conventions.

- Ownership – Ownership should be clearly identified.

Establishing master data maintenance procedures, including approval, review, and adequate support for changes to master data

As discussed earlier, master data are much more static than transaction data, which may be created and updated on a daily basis by a wide range of users. Master data maintenance, therefore, should be the domain of fewer users than those responsible for updating transaction data.

Because Master Data serves as the basis for transaction processing, it is critical that controls exist over the integrity and quality of the data. An erroneous Master Data record will compromise the integrity of whatever transactions use the field values stored in the master data. Characteristics of erroneous master data elements include, but are not limited to, duplicate names, invalid records, duplicate addresses, improper address formats, incomplete or inaccurate address information, unpopulated data fields and other data formatting inconsistencies between the business rules and the data sets.

Because it is foundational in nature and may have a broad impact on transactional data, master data should be carefully controlled through reviews and approval by designated data owners. To reasonably assure an appropriate level of control, a combination of automated, preventive controls and manual, detective controls is recommended.

Controls over master data include controls related to:

- changes to the configuration of the master file,
- validity of all master file records,
- completeness and validity of master file data,
- consistency of master data among modules, and
- approval of changes to master file data.

Implementing an effective auditing and monitoring capability

As part of the control of master data, the organization should have an effective auditing and monitoring capability which allows changes to master data records to be recorded and reviewed where necessary. This monitoring may be done either as part of ongoing activities or through separate “master data audits”. In either case, the most important factor supporting the capability is that activity is properly captured and maintained by an automated logging mechanism.

Depending on the level of risk associated with the data, the type and frequency of monitoring may vary. Ideally, monitoring should be built into the normal, recurring responsibilities of the data owner. Because audits take place after the fact, problems often will be identified more quickly by ongoing monitoring routines.

Ongoing monitoring may include obtaining approval prior to changes, or verifying the accuracy of changes on a real-time basis.

For federal systems, NIST SP 800-53 includes the following controls related to master data setup and maintenance:

SI-9	Information Input Restrictions
SI-10	Information Accuracy, Completeness, Validity, and Authenticity
SI-11	Error Handling

Control Techniques and Suggested Audit Procedures for Critical Element BP-4

Table 47. Control Techniques and Suggested Audit Procedures for Critical Element BP-4. Master Data Setup and Maintenance is Adequately Controlled

Control activities	Control techniques	Audit procedures
BP-4.1 Master data are appropriately designed.	BP-4.1.1 An entry is required in all key fields, such as address and account number.	Inspect master data configuration for required field values.
	BP-4.1.2 Null values or invalid values are not accepted in the required fields.	Observe user input of invalid values, or blank values, and note any exceptions.
	BP-4.1.3 For financial applications, account assignments (asset, liability, income and expense) are accurately defined.	Inspect master data configuration for account groups and assignments.
BP-4.2 Changes to master data configuration are appropriately controlled.	BP-4.2.1 Policies and procedures are established for master data configuration management, which include change rules that identify data fields that are excluded from changes (for example, master data number).	Review the master data polices and procedures for change management.
	BP-4.2.2 Changes to the master data design are approved by appropriate personnel	Inspect a selection of change requests and verify that appropriate approvals are obtained. Inspect master data configuration for change rules, if the rules are configured. If the change rules are automatic, then the user should be prevented from making unauthorized configuration changes.
	BP-4.2.3 Changes to the master data records should be limited to non-key fields.	Inspect a selection of master data change reports and verify that changes are limited to management-defined non-key fields.
BP-4.3 Only valid master records exist.	BP-4.3.1 Master data is reviewed on a regular basis, duplicates are identified and removed or blocked, and unused data is identified and blocked.	Inquire of management regarding their master data review procedures. Inspect policies and procedures on master data review, including duplicate master data entry and resolution, and unused master records. Inspect evidence of the most recent management review and action. Inspect list of accounts/records blocked for posting or use. Inspect duplicate master record report and management's use of it.
	BP-4.3.2 Automatic application controls (duplicate checks, system warnings) are configured to prevent and/or identify potential duplicate master records.	Inspect application configuration for automatic controls and determine whether the controls prevent erroneous processing or simply warn of potential errors.

Control activities	Control techniques	Audit procedures
BP-4.4 Master data are complete and valid.	BP-4.4.1 Policies and procedures for master data maintenance are documented and include: • approval requirements; • data quality criteria; • data owner; • supporting documents; • backup procedures in the event of a disaster or data corruption error; • Archival policies.	Inspect master data maintenance policies and procedures for appropriateness. Inquire of responsible personnel.
	BP-4.4.2 The master data maintenance process includes a formal create/change request from the requestor and approval from the data owner.	Select master data created or changed, and inspect relevant documentation, noting appropriate approvals and compliance with policies and procedures. Obtain system report of users with master data maintenance access. For a selection of users with conflicting responsibilities, inspect user profiles noting evidence of segregation of duty consideration and review when conflicts are noted.
	BP-4.4.3 Segregation of duties conflicts are considered and resolved before providing access to master data transactions.	Inspect procedures for identifying, segregation of duty exceptions, and review compliance.
	BP-4.4.4 Edit reports are reviewed by appropriate data owners on a periodic basis to review new master data and changes made to existing master data.	Inspect evidence of proper review of edit reports by owners
BP-4.5 Master data are consistent among modules.	BP-4.5.1 Periodic review and reconciliation procedures are in place to ensure that master data are consistent between different application modules.	Inspect evidence of management reconciliation and review for effectiveness. Through inquiry and inspection, determine whether the frequency of management reconciliation of master data is appropriate.
BP-4.6 Master data additions, deletions, and changes are properly managed and monitored by data owners.	BP-4.6.1 Master data policies and procedures require data owners to be responsible for the creation, deletion, and change of master data and also changes to data characteristics.	Review policies and procedures and inquire of data owner concerning application of specific monitoring procedures.
	BP-4.6.2 Data owners monitor master data design changes, and approve and monitor creation, deletion and changes to master data on a regular basis.	Obtain and inspect evidence of monitoring by data owners, including related reports. Inquire of management regarding ongoing monitoring of master data changes. Obtain and inspect evidence of management review of master data design changes, and determine whether changes are approved and reviewed.
BP-4.7 As appropriate, the confidentiality of master data is adequately controlled	BP-4.7.1 Management implements adequate controls to protect the confidentiality of master data, as appropriate.	Assess the adequacy of management controls over confidentiality of master data. Coordinate this step with Critical Element AS-2 *Implement effective application access controls.*

Source: GAO.

4.3. Interface Controls (IN)

Interface controls consist of those controls over the a) timely, accurate, and complete processing of information between applications and other feeder and receiving systems on an on-going basis, and b) complete and accurate migration of clean data during conversion.

Interfaces[116] result in the structured exchange of data between two computer applications, referred to in this section as the source and target systems or applications. These applications may reside on the same or different computer systems that may or may not reside in the same physical environment. Interfaces are periodic and recurring in nature. Interface controls may be performed manually or automated, scheduled or event-driven, electronically or on paper. One interface transfers one business data object and is one-directional; e.g. vendor master outbound, sales order inbound, etc. Interfaces are never bi-directional, even if technically there may be handshaking, back-and-forth reconciliation, etc.

This section focuses on the scope of and controls for interfaces, governing specifically the extraction, transformation, and loading of data between two applications. The data input, validation, and output controls within an application are addressed in the preceding business process control sections. To the extent that data input is obtained from other applications, auditor's assessment of this data should be coordinated with data input controls discussed in section 4.2 of this chapter.

The interface process, including conversions, can be broken down into the following seven separate components:

1. Interface strategy – A documented strategy is developed to keep data synchronized between source and target application. The strategy should include an explanation of each interface, the interface method chosen (manual or batch, etc.), the data fields

[116]In contrast, system interconnections refer to the direct connection of two or more IT systems for the purpose of sharing data and other information resources.

being interfaced, the controls to reasonably assure that the data is interfaced completely and accurately, timing requirements, definition of responsibilities, on-going system balancing requirements, and security requirements.

2. Data Export / Extraction –The information needs of the target application (key information fields, ID fields and cross-reference fields) should be fully understood and documented. If the information needs are not fully understood, all relevant data may not be extracted. In addition, appropriate procedures/should be in place concerning the format, quality, cut-off, and audit trails related to source data.

    a. The format of the source data should be checked to reasonably assure that the information is available, accurate and at the appropriate level of detail. If the source data quality is poor, the data may not be able to be interfaced.

    b. Data processing should be cut-off as of a specific time to reasonably assure that the data is extracted for the proper period.

    c. Sufficient audit trails should exist for the source application, such that once the data is extracted, the original audit trail remains. For instance, invoices can be traced back to the applicable purchase order in the source system.

3. Data Mapping / Translation – Data mapping and translation is the process of converting source data from the source application format to the target application format. If the data is not entered in the target application in exactly the same way as it is expected, target application edit and validation checks may be rendered ineffective.

4. Data Import – Data import is the process of loading source data into the target application. Appropriate controls, such as database indicies that enforce uniqueness, should be in place to prevent duplicate processing.

5. Error Handling and Reconciliation procedures – The procedures developed to reasonably assure that all transactions are accounted for and that all errors are identified, isolated, analyzed, and corrected in a timely manner.

6. Job definition, Scheduling and Event Triggering – Due to business requirements, it may be necessary to initiate an interface daily, weekly, monthly, or after a triggering event. "Triggering events" are used to start interface processing based on specific criteria, such as date/time or completion of another event. Interfaces may run across multiple platforms. Therefore, interface jobs may need to be scheduled across platforms. Visibility of these jobs may be necessary in a single location by the system operators. Restart and recovery procedures should exist.

7. Data Handling – Original interfaced data should be preserved for re-execution of the interface, if needed. Controls should be established to support the confidentiality and proper handling of sensitive data. Access to interface data and processes should be properly restricted.

The objectives of interface controls are to:

- Implement an effective interface strategy and design
- Implement effective interface processing procedures, including
    - interfaces are processed completely, accurately and only once in the proper period.
    - interface errors are rejected, isolated and corrected in a timely manner.
    - access to interface data and processes are properly restricted. Data is reliable and obtained only from authorized sources

For federal systems, NIST SP 800-53 includes the following controls related to interface:

SI-9	Information Input Restrictions
SI-10	Information Accuracy, Completeness, Validity, and Authenticity
SI-11	Error Handling

Critical Elements

The critical elements for interface controls are:

IN-1 Implement an effective interface strategy and design
IN-2 Implement effective interface processing procedures

Because weaknesses in interface controls can affect the achievement of all of the control objectives (completeness, accuracy, validity, and confidentiality) related to applications data, the control activities in the control tables for interface controls do not contain reference to specific control objectives.

Critical Element IN-1. Implement an effective interface strategy and design.

The purpose of an interface strategy is to describe, at a high level, how the interfaces are implemented between two applications. The interface strategy is the basis for the interface design and scope. The interface strategy includes an explanation of each interface, the interface method chosen (manual or batch, etc.), the data fields being interfaced, the controls to reasonably assure that the data is interfaced completely and accurately, timing requirements, assignment of responsibilities, on-going system balancing requirements, and security requirements. Interface design uses guidelines set by the strategy and provides specific information for each of the characteristics defined in the strategy.

Control Techniques and Suggested Audit Procedures for Critical Element IN-1

Table 48. Control Techniques and Suggested Audit Procedures for Critical Element IN-1. Implement an effective interface strategy and design.

Control activities	Control techniques	Audit procedures
IN-1.1 An interface strategy is developed for each interface used in the application.	IN-1.1.1 An interface strategy exists for each interface that includes the interface method, data fields being interfaced, controls to reasonably ensure a complete and accurate interface, schedule, assignment of responsibilities, system balancing requirements and security requirements.	Obtain a list of all interfaces to and from the application audited. Inspect the interface strategy document noting the details of each interface and determine whether it contains appropriate information.
IN-1.2 An interface design is developed for each interface used in the application that includes appropriate detailed specifications.	IN-1.2.1 An interface design exists for each interface and includes appropriate specifications based on the business requirements, including: • validations and edits • ownership of the interface process • error correction and communication methods	Inspect interface design documents of each interface and determine whether it contains appropriate information.
	IN-1.2.2 Mapping tables are used to convert data from the source system to the target system. Controls are in place to reasonably assure that mapping tables are only changed when authorized and that historical data on mappings is retained with the previous mapping table.	Determine whether the interfaces use mapping tables. Verify that controls over mapping tables will be established.
	IN-1.2.3 If mapping tables are not used, appropriate edits and validations are present in the source system.	Review the edits and validations in the source system to determine whether they are appropriate and perform tests to assess their effectiveness.

Source: GAO.

Critical Element IN-2. Implement effective interface processing procedures

Because there may be several methods that are used to transfer data from one system to another, the auditor should understand the procedures that are used for each interface, including:

- Who is the owner of the interface? Who initiates the process?
- How is the data transferred from the source application?
- How often are the interface programs run?
- How does the target system get the notification of an interface?
- Where are the errors corrected - in the source or target system?

Controls surrounding interface processing should reasonably assure that data is transferred from the source system to target system completely, accurately, and timely. The processing routines should

include balancing by ensuring the opening balance control totals plus processed transactions equal the closing balance of control totals. Both the applications (source and target) are typically designed with controls so that data are controlled by the use of control totals, record counts, batching run totals, or other data logging techniques. These types of controls are commonly referred to as balancing controls. Records or data produced by one application may be used in another application and may have dependencies that are based upon the sequential processing of data. The entity should have effective procedures to reconcile control information between the source and target applications.

During interface processing, all data may not be processed completely or accurately as a result of errors or inconsistencies in data, system interruptions, communication failures, or other events. To identify these instances, a monitoring capability should be implemented. The objective of the monitoring function is to reasonably assure that data are accurately processed through the interface and that no data are added, lost, or altered during processing. Control techniques include:

- If the interface is "run" on a regular schedule to process data, either manually or automatically, documented procedures explain how this is performed, including controls in place to reasonably assure that all processing was completed.

- An interface processing log is maintained and reviewed for unusual or unauthorized activity.

- The interface processing log, or another log or report, is used to document any errors or problems encountered during processing. Types of information that should be considered for logging are descriptions of any errors encountered, dates identified, any codes associated with errors, any corrective action taken, date and times corrected.

- Procedures are in place to use the correct generation/cycle of files for processing. This may include the generation of backup files from processing to be used for disaster recovery.

- Audit trails are generated during processing. These audit trails should be logs or reports that contain information about each interface. Data that should be included are who initiated each of the interfaces, the data and time of the run, the source system, and the results.

- Procedures are implemented to identify and correct any errors that occur during the interface run. Error handling procedures during data entry should reasonably assure that errors and irregularities are detected, reported, and corrected. Errors should be corrected in the source system and reprocessed through the next run. Management should have procedures in place to reasonably assure that error logs are used to timely follow-up on and correct unresolved data errors and irregularities.

In addition, to the above, change control procedures should be implemented over the interfaced applications to prevent unauthorized and potentially inaccurate changes to fields and values. The change control procedures should include

- establishing formal change requests, authorization, and approval processes,

- testing all changes both scheduled and emergency ones, and

- logging all changes and routinely reviewing them to ensure compliance with established procedures.

Control Techniques And Suggested Audit Procedures For Critical Element IN-2

Table 49. Control Techniques And Suggested Audit Procedures For Critical Element Critical Element Critical Element IN-2. Implement effective interface processing procedures.

Control activities	Control techniques	Audit procedures
IN-2.1 Procedures are in place to reasonably assure that the interfaces are processed accurately, completely and timely	IN-2.1.1 Procedures include a complete list of interfaces to be run, the timing of the interface processing, how it is processed and how it is reconciled. If system interconnections are used, procedures should address requirements for an Interconnection Security Agreement and Memorandum of Understanding.	Inspect documentation of interface processing procedures and, if applicable, Interconnection Service Agreements and Memorandums of Understanding. Observe interface processing into the application.
	Timing for processing of the interface has been determined and is followed.	Determine whether data and files from interface activities are processed according to the stated policies and in the proper accounting period.
	A positive acknowledgement scheme is used to ensure that files sent from a source system are received by the target system (i.e., a "handshake" between the systems so that files are not skipped or lost).	Determine whether all files sent from the source system are received and acknowledged by the target system.
IN-2.2 Ownership for interface processing is appropriately assigned.	IN-2.2.1 Responsibility for processing the interface and correcting any errors has been assigned to a user from the source and to a user of the target system. Actual processing may involve a technical person, if the interface is processed via an electronic media, such as a tape.	Identify which users are assigned responsibility for the interfaces. Evaluate whether an appropriate level of resources has been assigned to maintain interfaces.
	IN-2.2.2 The files generated by an application interface (both source and target) are properly secured from unauthorized access and/or modifications.	Assess whether appropriate security is in place for all access points to the interface data are secure from unauthorized use. Identify individuals that will be responsible for providing security surrounding the interfaces.
	IN-2.2.3 Users who are processing interfaces are able to monitor the status of interfaces.	Assess whether proper access is assigned to the appropriate individuals for the monitoring of the interface status and that such individuals have access to appropriate information to monitor the status of the interface.
IN-2.3 The interfaced data is reconciled between the source and target application to ensure that the data transfer is complete and accurate.	IN-2.3.1 Reconciliations are performed between source and target applications to ensure that the interface is complete and accurate. Control totals agree between the source and target systems. Reports reconcile data interfaced between the two systems and provide adequate information to reconcile each transaction processed.	Inspect reports or other documents used to reconcile interface processing between source and target applications and review their content and frequency for appropriateness.

Control activities	Control techniques	Audit procedures
IN-2.4 Errors during interface processing are identified by balancing processes and promptly investigated, corrected and resubmitted for processing.	IN-2.4.1 Management maintains a log for interface processing. The log accounts for errors and exceptions, as well. Exception/error reports are produced, reviewed, and resolved by management on a regular basis, including correction and resubmission, as appropriate.	Through inquiry of management and review of logs, determine whether errors are properly handled. Assess the appropriateness of the frequency that exception reports are reviewed (daily, weekly, etc). Inspect evidence of such reviews having been performed.
IN-2.5 Rejected interface data is isolated, analyzed and corrected in a timely manner.	IN-2.5.1 Error and correction facilities are utilized to track and correct errors in interface data.	Assess the adequacy of procedures in place to properly correct any rejected transactions. Inquire about procedures applied with individuals responsible for identifying and correcting errors and inspect evidence that rejected data is properly processed timely basis.
	IN-2.5.2 A mechanism is used to notify users when data is rejected (for example, an e-mail message may be sent to the user). These messages should repeat daily until they are corrected.	Determine whether error messages are generated and promptly reviewed for all rejected data and are maintained until corrected.
	IN-2.5.3 Audit trails are used to identify and follow-up on interface errors. The corrections to interface errors are included in the audit trail.	Determine whether appropriate audit trails are generated, reviewed and maintained.
IN-2.6 Data files are not processed more than once.	IN-2.6.1 Interfaces files are automatically archived or deleted from the production environment after processing.	Inspect a selection of archived interface documents and verify the date and time of processing. Observe the interfaces that are in process and inspect evidence that interface files were not processed before.

Source: GAO.

4.4 Data Management System Controls (DA)

Applications that support business processes typically generate, accumulate, process, store, communicate and display data. Applications which handle significant volumes of data often employ data management systems to perform certain data processing functions within an application. Data management systems use specialized software which may operate on specialized hardware. Data management systems include database management systems, specialized data transport/communications software (often called middleware), cryptography used in conjunction with data integrity controls, data warehouse software and data reporting/data extraction software. Many of the data input and processing controls,

such as edit checks, existence checks and thresholds described in previous sections are implemented in functions of data management systems. These types of controls implemented in data management systems are often referred to as business rules.

Critical Element DA-1. Implement an Effective Data Management System Strategy and Design

When assessing the effectiveness of application controls, the auditor should evaluate functions of data management systems specific to the business processes under review, in addition to the general controls described in Chapter 3. When auditors are evaluating application security plans and independently assessing risk, consideration of the risk inherent to the data management system "layer" in the application architecture is important. Necessarily, multiple access paths must exist into the data and the business rules that reside in the data management system layer to facilitate the operation and administration of the application. In most large scale and/or high performance applications, various components of data management systems reside on different servers which often employ various operating systems and hardware technologies. The auditor should obtain an understanding of the interconnected combination of data management technologies and appropriately consider related risks.

Understanding the logical design and physical architecture of the data management components of the application is necessary for the auditor to adequately assess risk. In addition to supporting the data storage and retrieval functions, it is typical for applications to employ data management systems to support operational aspects of the application, such as the management of transient user session state data, session specific security information, transactional audit logs and other "behind the scenes" functions that are essential to the application's operation. Controls associated with these types of functions can be critical to the security of the application.

The following highlights certain key concepts the auditor considers when assessing controls over a data management systems, including database management systems, middleware, cryptography, data warehouse, and data reporting/data extraction software.

Key Concepts - Database Management Systems

Authentication/Authorization

Controls in a data management system should include consideration of the access paths to the data management system. The access paths should be clearly documented and updated as changes are made. Generally access to a data management system can be obtained in three ways, via:

- Directly, via the database management system;
- Through access paths facilitated by the application; or
- Through the operating system(s) underlying the database management system.

Data management systems have built in privileged accounts that are used to administer and maintain the data management system. The auditor's objective is to determine whether appropriate controls are in place for securing these privileged accounts. Such controls include, but are not limited to:

- Strong password usage or other authentication controls;
- Highly restrictive assignment of personnel to these accounts;
- Enforcement of unique accounts for each administrator; and
- Effective monitoring of privileged account use.

In addition to privileged accounts, the auditor should obtain an understanding of the role the data management system plays in authentication and authorization for the application. The data management system will also contain user accounts related to the application.

Generally, there are two methods of authentication using a data management system. In the first scenario, the application uses a generic ID to authenticate to the database on behalf of end-users. These generic IDs should have their access privileges carefully scoped to only provide access to what the highest level of end-user

is permitted to access. There should be a limited number of generic IDs within the database supported by well-documented and carefully monitored control procedures. In the second scenario, the application passes the user ID to the database and uses accounts assigned to each end-user to authenticate to the database. Depending upon the size of the application, there could be a large number of user accounts stored within the database management system. In either case, the auditor should review the account and password policies relevant to the database management system.

There may be situations where authentication to the data management system is done through the operating system. The auditor should, in such instances, coordinate testing of general controls related to the operating system.

There are two major types of database management systems in use, hierarchical and relational databases. Hierarchical databases, such as IBM's IMS, have a heritage near the beginning of computer systems; however they are still used in some modern applications. Each different hierarchical database product is proprietary in design and implementation. If achieving audit objectives involving hierarchical databases is a requirement, staff with knowledge of the specific database product will be necessary. Relational databases (such as Oracle, DB2, and SQL-Server) share a common design based on relational algebra and a common data access method, called the Structured Query Language (SQL). While there are differences in the implementation of the different relational database products, they are similar enough that staff should be able to perform audit work in most relational database systems with a common skill set. The discussion in this chapter will focus on relational database systems.

SQL Commands

There are two categories of commands available through SQL, data definition language statements (DDL) and data manipulation language statements (DML). DDL statements are used to define and alter the structures or objects that contain and support access to data. DDL statements are used to create, alter and delete objects such as tables and indices. DML statements are used to retrieve, add, change and delete data in existing database objects.

Application end-users would not typically need to use DDL statements.

System, Role, Object Privileges

A user *privilege* is a right to execute a particular type of Structured Query Language (SQL) server statement, or a right to access another user's object. As discussed below, there are two types of data management system privileges: system and object. *Roles* are created by users (usually administrators), and are used to group together privileges or other roles. They are a means of facilitating the granting of multiple privileges or roles to users.

System privileges relate to the ability of the user within the database to interact with the database itself using DDL statements and the ability to execute special functions. They include: CREATE, ALTER, DROP, CONNECT, and AUDIT, among many others. The auditor should examine the privileges granted to the users within the database. Typically administrator level accounts have extended system privileges while general user accounts should have limited access to system privileges.

Object privileges (through DML statements) allow the user to have access to the data within an object or allow the user to execute a stored program. These include SELECT, INSERT, DELETE, etc. Each type of object has different privileges associated with it. Examples of database objects include the following:

- **Tables** - A data structure containing a collection of rows (or records) that have associated columns (or fields). It is the logical equivalent of a database file.
- **Index** - A database object that provides access to data in the rows of a table, based on key values. Indexes provide quick access to data and can enforce uniqueness on the rows in a table.
- **Triggers** - A special form of a stored procedure that is carried out automatically when data in a specified table is modified. Triggers are often created to enforce referential integrity or consistency among logically related data in different tables.

- **Stored procedure** - A precompiled collection of SQL or other statements and optional control-of-flow statements stored under a name and processed as a unit. Stored procedures are stored within a database, can be executed with one call from an application, and enable user-declared variables, conditional execution, and other powerful programming features.

- **Views** - A virtual table generated by a query whose definition is stored in the database. For example, a view might be defined as containing three out of five available columns in a table, created to limit access to certain information. Views can be treated as tables for most database operations, including Select queries, and under some circumstances, Update, Insert, and Delete queries. Any operations performed on views actually affect the data in the table or tables on which the view is based.

The auditor should identify the objects within the data management system. The privileges that a user account has for each object should be reviewed. These privileges should be granted based on the functionality of the account.

A *role* groups several privileges and roles, so that they can be granted to and revoked from users simultaneously. A role should be enabled for a user before it can be used by the user. Predefined roles exist that can be leveraged, such as the data base administrator (e.g., DBA) role. The auditor should review the privileges granted to each role, and then analyze the role(s) granted to each user. Roles that grant high level access, or permit direct manipulation of data in the database are very sensitive. The auditor should evaluate controls over the use of such roles.

Stored Procedures

Stored procedures are programs that are compiled and stored in the data management system. These programs can be executed directly by a user or they can be called by other programs. Most data management systems are prepackaged with stored procedures that provide a structured and controlled method of administering the database. For example, when the administrator creates a user, the database management system uses a stored procedure to perform

the steps necessary to create that account. In addition custom stored procedures can be created to support additional functionality. The auditor should review stored procedures that interact with sensitive data within the database management system or provide access to the operating system.

Key Concepts – Middleware

Modern business applications frequently have user interface, data processing and data storage components hosted on different computer systems, often using different operating systems. Tying the components together is often accomplished through the use of specialized data transport/communications software commonly known as middleware. A popular example of this type of software is IBM's MQSeries. Middleware is used to connect applications together in varying architectures including interconnected systems and interfaced systems (as described in 4.3).

Middleware provides robust and potentially secure communications between application components through layers of functions across a series of host computer and network technologies. In modern application architectures, the "behind the scenes" processing and storage of information may be designed to *trust* upstream application components, such as user interfaces, due to the data security and data integrity services provided by the middleware. Middleware can be used to communicate both data and commands between systems using different operating systems. The communication links are often facilitated by *channels* created by the middleware. The channels can be configured so that they provide data security for the information flowing across the network, typically using cryptography, and data integrity through error detection and correction facilities. Middleware can also be an important aspect of an application's continuity of operations, by being configured to support multiple data paths to eliminate single points of failure across networks.

Middleware Controls

Middleware components can be found on many components in a network of computers used to support business applications. The location and function of these components should be well documented. Middleware carries not only data and system commands; it also typically facilitates the establishment of sessions between application components, often some level of application component logging onto a "back-end" host and database management system. An application's controls often rely on the encrypted transmission of information between components. This protection may be a function of the implementation of middleware, sometimes in conjunction with how the channels are configured across the network. As with other data management systems, auditors should identify the staff with administrative access privileges to middleware and verify that appropriate controls are in place.

Key Concepts – Cryptography

Modern business applications commonly employ one or more controls that rely on cryptographic services. Auditors should identify where these controls are deployed and verify that the technical implementations are appropriate and effective operational procedures are in place and being followed. The mere existence of cryptography provides no assurance that data controls are actually in place and effective. Due to the exacting nature of verifying the effectiveness of cryptographic controls, a detailed discussion is beyond the scope of this audit guidance. When it is necessary to evaluate the effectiveness of cryptographic controls to achieve audit objectives, the auditor should obtain the services of adequately qualified specialists.

Key Concepts – Data Warehouse, Data Reporting and Data Extraction Software

Increasingly, modern business applications are parts of larger business management information architectures. This is certainly

the case with ERP environments, but also is the result of interconnected and interfaced systems that supply information used for purposes beyond the application's primary business function. A common element in these combined business management information architectures is the data warehouse, which may be populated with both financial and non-financial business information. The data warehouse is often a separate data store, not operationally part of the entity's transactional systems. The reasons behind having this separate copy of business information can be multifold: separating the information eliminates potential performance issues associated with trying to use live transactional data for reporting; also the structure of the information in diverse business applications may be technically or logically incompatible with efficient information retrieval. When the auditor encounters a data warehouse, important questions related to audit objectives and system boundaries need to be addressed. Unless the data warehouse itself is the subject of the audit, the relevance to the audit objectives and potential risks created by the data warehouse need to be identified and evaluated. Since a data warehouse may represent a copy of information from other systems that are part of the audit, any data confidentiality concerns will likely need consideration. Additionally, the auditor may need to functionally understand how the entity uses the data warehouse. In a financial audit, the auditor may find that financial statements may be prepared, in part, from the data warehouse instead of directly from the general ledger.

A data warehouse typically exists to facilitate analysis and reporting from a large quantity of data. Supporting the efficient use of a data warehouse will often be specialized data reporting and data extraction software tools. The existence of these tools and data warehouses creates the potential for many different access paths to data. Depending on the control requirements of the data warehouse and the information it stores, the auditor may need to identify controls over how the data is populated, maintained, and accessed by both users and administrators. The software systems involved are often specialized and effective reviews may require the services of qualified specialists.

Segregation of Duties

Since data management systems are supported by one or more operating systems, the auditor should obtain an understanding of the role of the data management system administrators. There should be a distinct segregation between the data management system administrator and the operating system administrator. The operating system administrator may need access to the data management system, but should have limited access. Likewise, the data management system administrator may need access to the underlying operating system, but should have only the access necessary to manage the data management system functionality.

The auditor should also evaluate the segregation between the data management system administrator and personnel in charge of reviewing audit and transaction logs. The data management system administrator should not have access to the audit logs within the data management system. These logs should be reviewed by a security administrator.

There should also be a separation between the functional aspects of the data management system environments. Data management system access should be consistent with the functional separation of duties within the application environment. Users that are developers should have access to the development environment only, and consequently only the development data management system. Users that require access to production should only have access to the production data management system.

Control Techniques and Suggested Audit Procedures for Critical Element DA-1

Because weaknesses in data management controls can affect the achievement of all of the control objectives (completeness, accuracy, validity, and confidentiality) related to applications data, the control activities in the control tables for interface controls do not contain reference to specific control objectives.

Table 50. Control Techniques and Suggested Audit Procedures for Critical Element DA-1. Implement an effective data management system strategy and design

Control activities	Control techniques	Audit procedures
DA-1.1 Implement an effective data management system strategy and design, consistent with the control requirements of the application and data. The strategy addresses key concepts including: • database management, • middleware, • cryptography, • data warehouse, and • data reporting/data extraction.	DA-1.1.1 The physical and logical (in terms of connectivity) location of the data storage and retrieval functions are appropriate.	Inspect documentation of the design of the data management system(s) associated with the application.
	DA-1.1.2 The production data management system is effectively separated from non-production systems (such as testing and development) and other production systems with lesser control requirements.	Assess whether the production and non-production data management systems are effectively separated.
	DA-1.1.3 The database schema is consistent with access control requirements such that the organization of data and database-hosted functions correspond to the access limitations that need to be imposed on different groups of users.	Verify that all access paths to data and sensitive data management system administrative functions have been identified and are adequately controlled.
DA-1.2 Detective controls are implemented in a manner that effectively supports requirements to identify and react to specific system or user activity within the data management system and its related components.	DA-1.2.1 Logging and monitoring controls are in place at the data management system level which effectively satisfy requirements to accurately identify historical system activity and data access.	Identify the security events that are logged and determine whether logging is adequate. Assess the adequacy of controls to monitor the audit logs.
	DA-1.2.2 Real-time or near real-time controls are in place to detect abnormal activity and security events.	Assess the adequacy of controls to detect abnormal activity.
DA-1.3 Control of specialized data management processes used to facilitate interoperability between applications and/or functions not integrated into the applications (such as ad-hoc reporting) are consistent with control requirements for the application, data and other systems that may be affected.	DA-1.3.1 Data accuracy and completeness controls are in place and effective to correct and/or detect data anomalies.	Perform the following procedures for DA-1.3.1 to DA-1.3.2. Identify and obtain an understanding of specialized data management processes used to facilitate interoperability. Understand how system

Control activities	Control techniques	Audit procedures
	DA-1.3.2 The configuration of system connectivity that facilitates application to application and application to non-integrated functions is controlled to limit access appropriately.	interconnectivity is controlled with respect to data management systems. Assess the adequacy of controls over specialized management processes. Note: These procedures should be closely coordinated with tests of general controls related to the data management systems. Determine whether a periodic reconciliation process is implemented to ensure the data in a data warehouse matches the data from the source system.

Source: GAO.

Appendix I - Information System Controls Audit Planning Checklist

The auditor should obtain and document a preliminary understanding of the design of the entity's information system (IS) controls, including

- Understanding the entity's operations and key business processes,
- Obtaining a general understanding of the structure of the entity's networks
- Obtaining a preliminary understanding of IS controls.

In addition to this checklist, the auditor should obtain information from relevant reports and other documents concerning IS that are issued by or about the entity.

To facilitate this process, the following checklist has been developed as a guide for the auditor to collect preliminary information from the entity at the start of the audit. This checklist is intended as a starting point for collecting relevant IS control information. The information request can be tailored to the type of audit being performed. For example, an audit of application controls could be limited to the information needs listed in Sections I, II, and IV. The extent of the information requested from the entity will vary depending on whether this is a first year or follow-up review of IS controls. Also, as a result of the auditor's initial review and analysis of the information collected in this process, additional detailed information may need to be subsequently requested from the entity. The checklist is organized to request information on the entity's:

- organization and key systems/applications,
- prior audit reports/documents,
- IS general controls, and
- IS business process application level controls.

This appendix is downloadable as a Microsoft Word ® document on GAO's FISCAM web site at http://www.gao.gov/special.pubs/fiscam.html.

I. Organization and Key Systems/Applications

Understanding the entity's organization is a key to planning and performing the audit in accordance with applicable audit standards and requirements. Further, it helps to identify, respond to, and resolve problems early in the audit. Relevant information includes organizational structure, locations, use of contractors, key applications and IS platforms used to support them.

Document	Workpaper Reference
1. Entity's overall organizational chart with functional description of key components.	
2. Organizational charts that include functional description for security and IT components. Note: It is critical that the organizational relationships between management, information security, physical security, and computer operations are discernable.	
3. Name and functional description of relevant major applications, including functional owner, operating platform (including locations), operating system and version, and database management system and version. Note: FISMA requires agencies to maintain an inventory of all major systems.	
4. Name and functional description of relevant operating environments (e.g., general support systems (GSS)), including locations.	

Document	Workpaper Reference
5. List of contractors/third parties or other governmental entities that process information and/or operate systems for or on behalf of the entity. 6. Significant changes in the IT environment or significant applications implemented within the recent past (e.g., within 2 years) or planned within the near future (e.g., 2 years)	

II. Prior Audit Reports/Documents

The auditor generally gathers planning information through different methods, including previous audits, management reviews, and other documents. These reports often provide invaluable information on the effectiveness of IS controls and provides clues to areas of particular risk. Of specific interest are those reports/documents dealing with the IS control environment, including GSS and major applications. Relevant information in this area includes the following.

Document	Workpaper Reference
1. Internal or third party information system reviews, audits, or specialized testing (e.g., penetration tests, disaster recovery testing) performed during the last 2 years (e.g., IG, GAO, SAS 70 reports). 2. The entity's prior FISMA or equivalent entity reports on IS.	

Document	Workpaper Reference
3. The entity's annual performance and accountability report or equivalent reports (e.g., reports prepared under the Federal Financial Management Improvement Act of 1996 (FFMIA), Federal Managers' Financial Integrity Act of 1982 (FMFIA), Government Management and Reform Act (GMRA) and/or Accountability of Tax Dollars Act of 2002 (ATDA), as applicable). 4. Other reports by management, including privacy impact assessments and vulnerability assessments. 5. Consultant reports on IS controls.	

III. IS General Controls

General controls are the policies and procedures that apply to all or a large segment of an entity's information systems and help ensure their proper operation. General controls are applied at the entitywide, system, and business process application levels. The effectiveness of general controls at the entitywide and system levels is a significant factor in determining the effectiveness of business process application controls at the application level. General controls include security management, access controls, configuration management, segregation of duties, and contingency planning.

III.1 IS General Controls – Security Management

Security management provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls. The program should reflect the entity's consideration of the following critical elements for security

management – established security management program, periodic risk assessments, documented security policies and procedures, established security awareness training, and periodic management testing and evaluation of major systems. Other elements include implementing effective security-related personnel policies and ensuring that activities performed by external third parties are adequately secure. Relevant information for this control category includes the following.

Document	Workpaper Reference
1. Documentation of entity's security management program approved by OMB.	
2. Documented risk assessments for relevant systems (e.g., GSS and major applications).	
3. Certification and accreditation documentation or equivalent for relevant systems (e.g., GSS and major applications being reviewed).	
4. Documented security plans for relevant systems (e.g., GSS and major applications being reviewed).	
5. Entity performance measures and compliance metrics for monitoring the security processes.	
6. Management's plans of actions and milestones or their equivalent that identify corrective actions planned to address known IS weaknesses and status of prior year security findings.	

Document	Workpaper Reference
7. Entitywide policies and procedures governing • security management program, structure, and responsibilities, including system inventories • risk assessment • security awareness training for employees, contractors, third parties (including those in sensitive security and data processing position) and security-related personnel policies (including personnel hiring, reference and background checks, and job transfers and terminations), • performance of periodic tests and evaluations of IS controls and monitoring to ensure compliance with established policies and procedures (including copies of tests and evaluations performed (if not included under Section II "Prior Audit Reports/ Documents"), • security weakness remediation, and • security requirements and monitoring activities of third-party providers supporting specific application(s).	

III.2 IS General Controls – Access Controls

A basic management objective for any organization is to protect the resources that support its critical operations from unauthorized access. Organizations accomplish this objective by designing and implementing controls that are intended to prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities. Inadequate access controls diminish the

reliability of computerized information and increase the risk of unauthorized disclosure, modification, and destruction of sensitive information and disruption of service. Access controls include those related to protecting system boundaries, user identification and authentication, authorization, protecting sensitive system resources, audit and monitoring, and physical security. Relevant information for this control category includes the following.

Document	Workpaper Reference
1. High-level network schematic which identifies external network connections, inter- and intra-entity connections, contractor sites, and other external organizations. 2. Network schematic of all GSS (by site) that includes components such as: • internet presence, • firewalls, routers, and switches, • domain name servers, • intrusion detection systems, • critical systems, such as web and email servers, file transfer systems, etc. • network management systems • connectivity with other entity sites and other external organizations • remote access – virtual private networks and dial-in, and • wireless connections.	

Document	Workpaper Reference
3. Inventory of mid-level systems (Unix, Windows-based, etc.) supporting applications relevant to the audit. • operating systems/versions, • security software/versions, • list of systems/applications supported, and • data set naming conventions for the operating system, system configuration, utility software, applications, and security software. • documentation of basic security configuration settings, i.e. Windows-based, Unix, etc. 4. Inventory of mainframe systems including • operating systems/versions, • security software/versions, • IP addresses, • description and use of each LPAR configuration(production & non production),including list of user applications and software installed on each LPAR and description of any test or development activity in each LPAR. • data set naming conventions for the operating system, system configuration, utility software, applications, and security software, • identity of Exits and SVCs, including load library and module name, and • documentation of basic security configuration settings, i.e. RACF, Top Secret, or ACF2.	

Document	Workpaper Reference
5. Entitywide policies and procedures for • system boundaries • controlling remote access to entity information, including use of remote devices, • governing user and system identification and authentication, • requesting, approving, and periodically reviewing user access authorization, • restricting access to sensitive system resources (including system utilities, system software, and privileged accounts), • protecting digital and sensitive media, including portable media, • applying cryptography methods, if used, • monitoring mainframe, mid-level servers, and network systems for incidents, including management response and reporting on unusual activities, intrusion attempts, and actual intrusions, and • controlling physical security, including those concerning the granting and controlling of physical access to the data center and other IT sensitive areas. 6. Physical diagram of computer network and data center and other sensitive IT areas.	

III.3 IS General Controls – Configuration Management

Configuration management involves the identification and management of security features for all hardware and software components of an information system at a given point and systematically controls changes to that configuration during the system's life cycle. By implementing configuration management, organizations can ensure that only authorized applications and software programs are placed into production through establishing and maintaining baseline configurations and monitoring changes to these configurations. Configuration management includes

- overall policies and procedures,
- maintaining current configurations,
- authorizing, testing, and approving configuration changes,
- monitoring the configuration, updating software on a timely basis, and
- documenting and controlling emergency changes.

Relevant information for this control category includes the following.

Document	Workpaper Reference
1. Entitywide policies and procedures for: • configuration management, including the approval and testing of scheduled and emergency changes, and monitoring procedures to ensure compliance, • maintaining current configuration information, • authorizing, testing, approving, and tracking all configuration changes, • monitoring/auditing the configuration,	

Document	Workpaper Reference
• patch management, vulnerability scanning, virus protection, emerging threats, and user installed software, and • emergency changes. 2. Copy of System Development Life Cycle Methodology (SDLC). 3. Technical configuration standards for workstations, servers, related network components, mobile devices, mainframes, operating systems, and security software. 4. Description of configuration management software.	

III.4 IS General Controls- Segregation of Duties

Segregation of duties refers to the policies, procedures, and organizational structures that help ensure that no single individual can independently control all key aspects of a process or computer-related operation and thereby gain unauthorized access to assets or records. Often, organizations achieve segregation of duties by dividing responsibilities among two or more individuals or organizational groups. This diminishes the likelihood that errors and wrongful acts will go undetected, because the activities of one individual or group will serve as a check on the activities of the other. Effective segregation of duties includes segregating incompatible duties, maintaining formal operating procedures, supervision, and review. Relevant information for this control category includes the following.

Document	Workpaper Reference
1. Entitywide policies and procedures for • segregating duties. • periodically reviewing access authorizations. 2. Management reviews conducted to determine that control techniques for segregating incompatible duties are functioning as intended.	

III.5 IS General Controls – Contingency Planning

Contingency planning is critical to ensuring that when unexpected events occur, key operations continue without interruption or are promptly resumed and that critical and sensitive data are protected. Critical elements for contingency planning include: assessing the critical and sensitive computer activities and identifying supporting resources, taking steps to minimize damage and interruption, developing and documenting a comprehensive contingency plan, and periodically testing the contingency plan and adjusting it as needed. Relevant information for this control category includes the following.

Document	Workpaper Reference
1. Entitywide policies and procedures for: • assessing the availability needs of entity systems, • backing-up data, programs, and software, and	

Document	Workpaper Reference
• environmental controls, including emergency power, fire/smoke detection and response, hardware maintenance and problem management, alternate work sites, etc. 2. Documented contingency plan(s) and recent test results.	

IV. IS Business Process Application Level Controls

Business process application level controls are those controls over the completeness, accuracy, validity and confidentiality of transactions and data during application processing. The effectiveness of application level controls is dependent on the effectiveness of entitywide and system level general controls. Weaknesses in entitywide and system level general controls can result in unauthorized changes to business process applications and data that can circumvent or impair the effectiveness of application level controls. Application level controls are divided into the following four areas: application level general controls, business process controls, interface controls, and data management system controls. Relevant application specific information for this control category includes the following.

Document	Workpaper Reference
1. Certification and accreditation, or equivalent, documentation for relevant systems. 2. Documented security plans for relevant applications.	

Document	Workpaper Reference
3. Documented risk assessments for relevant applications. 4. High-level schematic of application boundaries that identifies controlled interfaces (e.g., gateways, routers, firewalls, encryption), to include: • internet presence, • firewalls, routers, and switches, • domain name servers, • intrusion detection systems, • critical systems, such as web and email servers, file transfer systems, etc. • network management systems • connectivity with other entity sites and other external organizations • remote access – virtual private networks and dial-in, and 5. Inventory of mid-level systems (Unix, Windows, etc.) supporting applications being reviewed. • operating systems/versions, • security software/versions, • list of systems/applications supported, • data set naming conventions for the operating system, system configuration, utility software, applications, and security software, and • documentation of basic security configuration settings, i.e. Windows-based, Unix.	

Document	Workpaper Reference
6. Inventory of mainframe systems supporting applications being reviewed, including • operating system/versions, • security software/versions, • IP addresses, • description of each LPAR configuration, including list of user applications and software installed on each LPAR, • data set naming conventions for the operating system, system configuration, utility software, applications, and security software, • identity of Exits and SVCs, including load library and module name. • documentation of basic security configuration settings, i.e. RACF, Top Secret, or ACF2. 7. Documented test and evaluation covering relevant applications. 8. Corrective action plan for identified IS application control weaknesses, including listing of weaknesses corrected. 9. Segregation of duties control matrices for job functions/responsibilities. 10. Application contingency plan and related disaster recovery, business continuity, and business resumption plans, including test results. 11. Documentation on data validation and edit checks, including auditing and monitoring processes.	

Document	Workpaper Reference
12. Documentation describing interface strategy between applications, including both manual and automated methods. 13. Documentation describing data management system used, including access paths to this system, privileged accounts, and authentication and authorization processes. 14. Policies and procedures for relevant application(s) being reviewed that govern • operation of application controls, • security and awareness training for employees and contractors, • granting user application access, • hiring, including reference and background checks, and job transfers and terminations, • security requirements and monitoring activities of third-party providers supporting relevant applications. • application user identification and authentication at the application level, • requesting and granting user access authorization to relevant applications, • collection, review, and analysis of access activities for unauthorized or inappropriate access to relevant applications,	

Document	Workpaper Reference
• configuration management process at the application level, including the approval and testing of scheduled and emergency application program changes and procedures to ensure compliance, • backing-up relevant application data and programs, • approval and review of data input, and • master file data configuration management and maintenance.	
15. Documentation describing system output, format of the output, and controls over the output.	

Appendix II - Tables for Summarizing Work Performed in Evaluating and Testing General and Business Process Application Controls

These tables are provided for the auditor's use in performing the audit. They are a consolidation of the tables of critical elements, control activities, control techniques, and related suggested audit procedures that are included after the discussion of each critical element. To reduce documentation and allow the tables to be tailored to individual audits, the tables are downloadable as Microsoft Word® documents from GAO's FISCAM web site at http://www.gao.gov/special.pubs/fiscam.html

These tables can be used as a guide during initial interviews and to document the preliminary assessment of controls. As the audit progresses, the auditor can continue to use the electronic version of the tables to document controls evaluated and tested, test procedures performed, conclusions, and supporting work paper references.

Note: The first page of the table is provided below for illustration purposes.

General Controls

Table 3. Security Management

Critical element and control activity	Control technique	Audit procedure	Entitywide level conclusion/ reference	System level conclusion/ reference	Application level conclusion/ reference	Overall conclusion/ reference
SM-1. A security management program has been established						
SM-1.1. A security management program is developed, documented, approved, and implemented.	SM-1.1.1. An entitywide security management program has been developed, documented, and implemented. It covers all major facilities and operations, has been approved by senior management and key affected parties, covers the key elements of a security management program: • periodic risk assessments • adequate policies and procedures • appropriate subordinate information security plans • security awareness training • management testing and evaluation • remedial action process	Review documentation supporting the entitywide security management program and discuss with key information security management and staff. Determine whether the program: • adequately covers the key elements of a security management program • is adequately documented, and • has been properly approved. Determine whether all key elements of the program are implemented. Consider audit evidence obtained during the course of the audit.				

Appendix III - Tables for Assessing the Effectiveness of General and Business Process Application Controls

The tables in this appendix are provided for the auditor's use in recording the control effectiveness for each critical element in each control category, as well as formulating an overall assessment of each control category. Judging control effectiveness should be based on the results of audit work performed and assessments of control effectiveness for specific control techniques, as summarized in Appendix II. After completing Appendix III, the auditor should prepare a narrative summarizing the control effectiveness for general and business process controls. The general control narrative should also state whether or not audit work should be conducted to determine the reliability of business process controls at the application level. These tables are downloadable as Microsoft Word® documents from GAO's FISCAM web site at http://www.gao.gov/special.pubs/fiscam.html

General Controls

Security Management

Critical elements	Are controls effective?			Comments on control effectiveness	Work paper references
	Yes	No	Partially		
SM-1. Establish a security management program					
SM-2. Periodically assess and validate risks					
SM-3. Document security control policies and procedures					
SM-4. Implement effective security awareness and other security-related personnel policies					
SM-5. Monitor the effectiveness of the security program					

Critical elements	Are controls effective?			Comments on control effectiveness	Work paper references
	Yes	No	Partially		
SM-6. Effectively remediate information security weaknesses					
SM-7. Ensure that activities performed by external third parties are adequately secure					
Overall assessment of security management					

Access Control

Critical elements	Are controls effective?			Comments on control effectiveness	Work paper references
	Yes	No	Partially		
AC-1. Adequately protect information system boundaries					
AC-2. Implement effective identification and authentication mechanisms					
AC-3. Implement effective authorization controls					
AC-4. Adequately protect sensitive system resources					
AC-5. Implement an effective audit and monitoring capability					
AC-6. Establish adequate physical security controls					
Overall assessment of access controls					

Configuration Management

Critical elements	Are controls effective?			Comments on control effectiveness	Work paper references
	Yes	No	Partially		
CM-1. Develop and document CM policies, plans, and procedures					
CM-2. Maintain current configuration identification information					
CM-3. Properly authorize, test, approve, and track all configuration changes					
CM-4. Routinely monitor the configuration					
CM-5. Update software on a timely basis to protect against known vulnerabilities					
CM-6. Appropriately document and approve emergency changes to the configuration					
Overall assessment of configuration management					

Segregation of Duties

Critical elements	Are controls effective?			Comments on control effectiveness	Work paper references
	Yes	No	Partially		
SD-1. Segregate incompatible duties and establish related policies					
SD-2. Control personnel activities through formal operating procedures, supervision, and review					
Overall assessment of segregation of duties					

Contingency Planning

Critical elements	Are controls effective?			Comments on control effectiveness	Work paper references
	Yes	No	Partially		
CP-1. Assess the criticality and sensitivity of computerized operations and identify supporting resources					
CP-2. Take steps to prevent and minimize potential damage and interruption					
CP-3. Develop and document a comprehensive contingency plan					
CP-4. Periodically test the contingency plan and adjust it as appropriate					
Overall assessment of contingency planning					

Business Process Application Level Controls

Application Security

Critical elements	Are controls effective?			Comments on control effectiveness	Work paper references
	Yes	No	Partially		
AS-1. Implement effective application security management					
AS-2. Implement effective application access controls					
AS-3. Implement effective configuration management					
AS-4. Segregate user access to conflicting transactions and activities and monitor segregation					
AS -5. Implement effective application contingency planning					
Overall assessment of application security					

Business Process Controls

Critical elements	Are controls effective?			Comments on control effectiveness	Work paper references
	Yes	No	Partially		
BP-1 Transaction data input is complete, accurate, valid, and confidential					
BP-2. Transaction data processing is complete, accurate, valid, and confidential					
BP-3. Transaction data output is complete, accurate, valid, and confidential					
BP-4. Master data setup and maintenance is adequately controlled					
Overall assessment of business process controls					

Interface Controls

Critical elements	Are controls effective?			Comments on control effectiveness	Work paper references
	Yes	No	Partially		
IN-1. Implement an effective interface strategy and design					
IN-2. Implement effective interface processing procedures					
Overall assessment of interface controls					

Data Management System Controls

Critical elements	Are controls effective?			Comments on control effectiveness	Work paper references
	Yes	No	Partially		
DA-1. Implement an effective data management system strategy and design					

Assessment(s) on control effectiveness involving cross-cutting controls issues:

NOTE: In assessing the effectiveness of general and business process application controls, the auditor may find situations where weaknesses identified solely in a specific control category (e.g., contingency planning) may not reach the level that would justify concluding controls to be ineffective for that particular category. However, when the auditor considers control weaknesses identified in separate control categories collectively, it may justify concluding controls to be ineffective (cross-cutting). For example, the auditor may have identified weaknesses indicating that the entity did not have a complete inventory of all major systems (security management), the system configuration baseline was incomplete (configuration management), and all critical systems/activities for contingency planning may not have been identified. In assessing these weaknesses solely in the context of their respective control categories, the auditor may have concluded that they did not reach the threshold to assess each of these respective control categories as ineffective. However, when the auditor assessed the weaknesses collectively, the auditor may conclude controls to be ineffective since an incomplete inventory of systems could significantly hamper the entity's ability to ensure that current and complete security settings are installed on all systems and that contingency plans address each system in the event of operational disruptions.

The space above is provided to document those assessments that are not control category specific but are made from a collectively assessment of weaknesses identified in separate control categories.

Appendix IV - Mapping of FISCAM to NIST SP 800-53 And Other Related NIST Publications

In table below, FISCAM is mapped to NIST Special Publication (SP) 800-53. To assist auditors, the individual FISCAM general and business process control activities are referenced to related NIST 800-53 controls.

FISCAM Controls	**Related NIST SP 800-53 Controls**
General Controls	
Security Management:	
SM-1. Establish a security management program	PL-2 System Security Plan PL-3 System Security Plan Update PL-6 Security-Related Activity Planning SA-2 Allocation of Resources
SM-2. Periodically assess and validate risks	CA-4 Security Certification CA-6 Security Accreditation RA-2 Security Categorization RA-3 Risk Assessment RA-4 Risk Assessment Update
SM-3. Document security control policies and procedures	See first control for each family (e.g., AC-1, AT-1)
SM-4 Implement effective security awareness and other security-related personnel policies	AT-2 Security Awareness AT-3 Security Training AT-4 Security Training Records PL-4 Rules of Behavior

FISCAM Controls	Related NIST SP 800-53 Controls
General Controls:	
Security Management:	
SM-4. Implement effective security awareness and other security-related personnel policies (continued)	PS-1 Personnel Security Policy and Procedures PS-2 Position Categorization PS-3 Personnel Screening PS-4 Personnel Termination PS-5 Personnel Transfer PS-6 Access Agreements PS-7 Third-Party Personnel Security PS-8 Personnel Sanctions
SM-5. Monitor effectiveness of the security program	CA-2 Security Assessments CA-7 Continuous Monitoring PL-5 Privacy Impact Assessment RA-5 Vulnerability Scanning
SM-6. Effectively remediate information security weaknesses	CA-5 Plan of Action and Milestones
SM-7. Ensure that activities performed by external parties third parties are adequately secure	AC-20 Use of External Information Systems MA-4 Remote Maintenance PS-7 Third-Party Personnel Security SA-9 External Information System Services
Access Controls:	
AC-1 Adequately protect information system boundaries	AC-4 Information Flow Enforcement

FISCAM Controls	Related NIST SP 800-53 Controls
General Controls: **Access Controls:**	
AC-1. Adequately protect information system boundaries (continued)	AC-8 System Use Notification AC-9 Previous Logon Notification AC-11 Session Lock AC-12 Session Termination AC-17 Remote Access AC-18 Wireless Access Restrictions AC-19 Access Control for Portable and Mobile Devices CA-3 Information System Connections SC-7 Boundary Protection SC-10 Network Disconnect
AC-2. Implement effective identification and authentication mechanisms	AC-7 Unsuccessful login attempts AC-10 Concurrent Session Control AC-14 Permitted Actions Without Identification and Authentication AU-10 Non-Repudiation IA-2 User Identification and Authentication IA-3 Device Identification and Authentication IA-4 Identifier Management IA-5 Authenticator Management IA-6 Authenticator Feedback SC-17 Public Key Infrastructure Certificates

FISCAM Controls	Related NIST SP 800-53 Controls
General Controls: **Access Controls:**	
AC-2. Implement effective identification and authentication mechanisms (continued)	SC-20 Secure Name/Address Resolution Service (Authoritative Source) SC-21 Secure Name/Address Resolution Service (Authoritative Source) SC-22 Architecture and Provisioning for Name/Address Resolution Service SC-23 Session Authenticity
AC-3. Implement effective authorization controls	AC-2 Account Management AC-3 Access Enforcement AC-6 Least Privilege CM-7 Least Functionality SC-6 Resource Priority SC-14 Public Access Protections SC-15 Collaborative Computing
AC-4. Adequately protect sensitive system resources	AC-15 Automated Markings AC-16 Automated Labeling IA-7 Cryptographic Module Authentication MP-2 Media Access MP-3 Media Labeling MP-4 Media Storage MP-5 Media Transport MP-6 Media Sanitation and Disposal PE-19 Information Leakage SC-2 Application Partitioning SC-3 Security Function Isolation

FISCAM Controls	Related NIST SP 800-53 Controls
General Controls: **Access Controls:**	
AC-4. Adequately protect sensitive system Resources (continued)	SC-4 Information Remnance SC-8 Transmission Integrity SC-9 Transmission Confidentiality SC-11 Trusted Path SC-12 Cryptographic Key Establishment and Management SC-13 Use of Cryptography SC-16 Transmission of Security Parameters SC-18 Mobile Code
AC-5. Implement an effective audit and monitoring capability	AC-13 Supervision and Review – Access Control AT-5 Contacts with Security Groups and Associations AU-2 Auditable Events AU-3 Content of Audit Records AU-4 Audit Storage Capacity AU-5 Response to Audit Processing Failures AU-6 Audit Monitoring, Analysis, and Reporting AU-7 Audit Reduction and Report Generation AU-8 Time Stamps AU-9 Protection of Audit Information AU-11 Audit Record Retention IR-1 Incident Response Policy IR-2 Incident Response Training IR-3 Incident Response Testing IR-4 Incident Handling IR-5 Incident Monitoring IR-6 Incident Reporting IR-7 Incident Response Assistance

FISCAM Controls	Related NIST SP 800-53 Controls
General Controls:	
Access Controls:	
AC-5. Implement an effective audit and monitoring capability (continued)	SC-5 Denial of Service Protection SI-4 Information System Monitoring Tools and Techniques SI-6 Security Functionality Verification
AC-6. Establish adequate physical security controls	PE-2 Physical Access Authorization PE-3 Physical Access Control PE-4 Access Control for Transmission Medium PE-5 Access Control for Display Medium PE-6 Monitoring Physical Access PE-7 Visitor Control PE-8 Access Records PE-16 Delivery and Removal
Configuration Management:	
CM-1. Develop and document CM policies, plans, and procedures	CM-1 Configuration Management Policy and Procedures
CM-2. Maintain current configuration identification information	CM-2 Baseline Configuration CM-6 Configuration Settings CM-8 Information System Component Inventory SA-5 Information System Documentation
CM-3. Properly authorize, test, approve, track and control all configuration changes	CM-3 Configuration Change Control SA-2 Allocation of Resources SA-3 Life Cycle Support SA-4 Acquisitions SA-8 Security Engineering Principles

FISCAM Controls	Related NIST SP 800-53 Controls
General Controls: **Configuration Management:**	
CM-3. Properly authorize, test, approve, and track all configuration changes (continued)	SA-10 Developer Configuration management SA-11 Developer Security Testing
CM-4. Routinely monitor the configuration	CM-4 Monitoring configuration Changes CM-5 Access Restrictions for Change SI-7 Software and Information Integrity
CM-5. Update software on a timely basis to protect against known vulnerabilities	RA-5 Vulnerability Scanning SA-6 Software Usage Restrictions SA-7 User Installed Software SC-19 Voice Over Internet Protocol SI-2 Flaw Remediation SI-3 Malicious Code Protection SI-5 Security Alerts and Advisories SI-8 Spam Protection
CM-6. Appropriately document and approve emergency changes to the configuration	CM-3 Configuration Change Control

FISCAM Controls	Related NIST SP 800-53 Controls
General Controls:	
Segregation of Duties:	
SD-1. Segregate incompatible duties and establish related policies	AC-5 Separation of Duties PS-2 Position Categorization PS-6 Access Agreements
SD-2. Control personnel activities through formal operating procedures, supervision, and review	AC-5 Separation of Duties PS-2 Position Categorization PS-6 Access Agreements
Contingency Planning:	
CP-1. Assess the criticality and sensitivity of computerized operations and identify supporting resources	RA-2 Security Categorization
CP-2. Take steps to prevent and minimize potential damage and interruption	CP-3 Contingency Training CP-6 Alternate Storage Site CP-7 Alternate Processing Site CP-9 Information System Backup CP-10 Information System Recovery and Reconstitution MA-2 Controlled Maintenance MA-3 Maintenance Tools MA-5 Maintenance Personnel MA-6 Timely Maintenance PE-9 Power Equipment and Power Cabling

FISCAM Controls	Related NIST SP 800-53 Controls
General Controls: **Continuity Planning:**	
CP-2. Take steps to prevent and minimize potential damage and interruption (continued)	PE-10 Emergency Shutoff PE-11 Emergency Power PE-12 Emergency Lighting PE-13 Fire Protection PE-14 Temperature and Humidity Controls PE-15 Water Damage Protection PE-17 Alternate Work Site PE-18 Location of Information System Components SA-5 Information System Documentation
CP-3. Develop and document a comprehensive contingency plan	CP-2 Contingency Plan CP-5 Contingency Plan Update CP-8 Telecommunications services
CP-4. Periodically test the contingency plan and adjust it as appropriate	CP-4 Contingency Plan Testing CP-5 Contingency Plan Update

FISCAM Controls	Related NIST SP 800-53 Controls
Business Process Application Level Controls:	
Application Level General Controls:	
AS-1. Implement effective application security management	The related NIST SP 800-53 application level general controls are identified under related General Controls above.
AS-2. Implement effective application access controls	
AS-3. Implement effective application configuration management	
AS-4. Segregate application user access to conflicting transactions and activities and monitor segregation	
AS-5. Implement effective application contingency planning	
Business Process Controls:	
BP-1. Transaction data input is complete, accurate, valid, and confidential	SI-9 Information Input Restrictions SI-10 Information Accuracy, Completeness, Validity, and Authenticity SI-11 Error Handling
BP-2. Transaction data processing is complete, accurate, valid, and confidential	SI-9 Information Input Restrictions SI-10 Information Accuracy, Completeness, Validity, and Authenticity SI-11 Error Handling

FISCAM Controls	Related NIST SP 800-53 Controls
Business Process Application Level Controls:	
Business Process Controls:	
BP-3. Transaction data output is complete, accurate, valid, and confidential	SI-10 Information Accuracy, Completeness, Validity, and Authenticity SI-11 Error Handling SI-12 Information Output Handling and Retention
BP-4. Master data setup and maintenance is adequately controlled	SI-9 Information Input Restrictions SI-10 Information Accuracy, Completeness, Validity, and Authenticity SI-11 Error Handling
Interface controls:	
IN-1. Implement an effective interface strategy and design	SI-9 Information input Restrictions SI-10 Information Accuracy, Completeness, Validity, and Authenticity SI-11 Error Handling
IN-2. Implement effective interface processing procedures	SI-9 Information input Restrictions SI-10 Information Accuracy, Completeness, Validity, and Authenticity SI-11 Error Handling

FISCAM Controls	Related NIST SP 800-53 Controls
Data management controls:	
DA-1. Implement an effective data management system strategy and design	

In the table below, FISCAM general and business process application level controls are mapped to related NIST publications.

FISCAM Controls	Related NIST Publications
General Controls: Security Management	
SM-1. Establish security management program	FIPS 199, 200, NIST SP 800-12, 800-14, 800-18, 800-19, 800-21, 800-25, 800-26, 800-27, 800-30, 800-31, 800-32, 800-33, 800-34, 800-35, 800-37, 800-40, 800-41, 800-44, 800-45, 800-57, 800-58, 800-64, 800-65, 800-81
SM-2. Periodically assess and validate risk	FIPS 199, NIST SP 800-12, 800-13, 800-14, 800-19, 800-23, 800-24, 800-25, 800-26, 800-28, 800-30, 800-31, 800-32, 800-34, 800-37, 800-40, 800-42, 800-44, 800-45, 800-46, 800-48, 800-53A, 800-54, 800-59, 800-60, 800-63, 800-65, 800-66, 800-76, 800-79, 800-82, 800-85A, 800-85B, 800-98
SM-3. Document and implement security policies and procedures	FIPS 199, 200, 201-1, NIST SP 800-12, 800-14, 800-18, 800-19, 800-23, 800-25, 800-28, 800-30, 800-31, 800-34, 800-35, 800-36, 800-37, 800-41, 800-42, 800-44, 800-45, 800-46 800-50, 800-53A, 800-61, 800-63, 800-64, 800-65, 800-66, 800-72, 800-73, 800-76, 800-79, 800-83, 800-84, 800-86, 800-87, 800-88, 800-92, 800-94, 800-100

FISCAM Controls	Related NIST Publications
General Controls: Security Management	
SM-4. Implement effective security awareness and other security-related personnel policies	FIPS 200, NIST SP 800-12, 800-14, 800-16, 800-31, 800-40, 800-45, 800-46, 800-48, 800-50, 800-66, 800-89, 800-100
SM-5. Monitor the effectiveness of program	FIPS 201-1, NIST SP 800-12, 800-17, 800-19, 800-20, 800-22, 800-23, 800-24, 800-26, 800-31, 800-35, 800-36, 800-37, 800-40, 800-42, 800-44, 800-45, 800-46, 800-51, 800-53A, 800-55, 800-66, 800-76, 800-79, 800-83, 800-85A, 800-85B, 800-98
SM-6. Effectively remediate information security weaknesses	NIST SP 800-18, 800-30, 800-37, 800-65
SM-7. Ensure activities performed by external third parties are adequately secure	NIST SP 800-35, 800-46, 800-66, 800-77
General Controls: Access Controls	
AC-1. Adequately protect information system boundaries	FIPS 201-1, NIST SP 800-18, 800-24, 800-28, 800-36, 800-41, 800-44, 800-45, 800-46, 800-47, 800-48, 800-54, 800-58, 800-66, 800-68, 800-70, 800-73, 800-76, 800-77, 800-78, 800-82, 800-83, 800-87, 800-96, 800-97

FISCAM Controls	Related NIST Publications
General Controls: Access Controls	
AC-2. Implement effective identification and authentication mechanism	FIPS 190, 198, 201, 201-1, NIST SP 800-12, 800-15, 800-24, 800-25, 800-32, 800-36, 800-44, 800-46, 800-48, 800-49, 800-52, 800-54, 800-56, 800-57, 800-63, 800-66, 800-68, 800-69, 800-72, 800-73, 800-76, 800-77, 800-78, 800-81, 800-87, 800-89, 800-94, 800-95, 800-97
AC-3. Implement effective authorization controls	FIPS 201-1, NIST SP 800-12, 800-19, 800-28, 800-43, 800-66, 800-68, 800-69 800-73, 800-76, 800-78, 800-81, 800-83, 800-87, 800-95, 800-96, 800-98
AC-4. Adequately protect sensitive system resources	FIPS 140-2, 180-2, 186-2, 188, 190, 197, 198, NIST SP 800-12, 800-17, 800-19, 800-20, 800-22, 800-24, 800-28, 800-29, 800-36, 800-38A, 800-38B, 800-38C, 800-38D, 800-44, 800-45, 800-49, 800-52, 800-54, 800-56, 800-57, 800-58, 800-66, 800-67, 800-72, 800-73, 800-77, 800-78, 800-81, 800-87, 800-88, 800-90, 800-92, 800-95, 900-97, 800-98
AC-5. Implement an effective audit and monitoring capability	FIPS 200, NIST SP 800-12, 800-14, 800-19, 800-31, 800-36, 800-40, 800-42, 800-44, 800-45, 800-48, 800-49, 800-50, 80052, 800-54, 800-61, 800-66, 800-68, 800-72, 800-81, 800-83, 800-84, 800-86, 800-89, 800-92, 800-94, 800-95, 800-100, 800-101

FISCAM Controls	Related NIST Publications
General Controls: Access Controls	
AC-6. Establish adequate physical security controls	NIST SP 800-12, 800-24,800-58, 800-66, 800-73, 800-76, 800-78, 800-82, 800-96, 800-98
General Controls: Configuration Management	
CM-1. Develop and document configuration management policies, plans, and procedures	FIPS 200, NIST SP 800-12, 800-14, 800-37, 800-100
CM-2. Maintain current configuration identification information	NIST SP 800-35, 800-40, 800-43, 80044, 800-45, 800-46, 800-48, 800-54, 800-68, 800-70, 800-81, 800-82, 800-83
CM-3. Properly authorize, test, approve, track, and control all activities	NIST SP 800-12, 800-14, 800-21, 800-23, 800-27, 800-30, 800-31, 800-33, 800-34, 800-35, 800-36, 800-64, 800-65, 800-76, 800-85A, 800-85B, 800-94, 800-97, 800-98
CM-4.Routinely monitor the configuration	NIST SP 800-19, 800-31, 800-44, 800-57, 800-66, 800-83, 800-94
CM-5. Update software on a timely basis to protect against known vulnerabilities	NIST SP 800-19, 800-24, 800-28, 800-31, 800-36, 800-37, 800-40, 800-42, 800-43, 800-44, 800-45, 800-46, 800-51, 800-58, 800-61, 800-69, 800-83, 800-84
CM-6. Appropriately document and approve emergency changes to the configuration	NIST SP 800-40, 800-43, 800-44, 800-45, 800-46, 800-48, 800-54, 800-68, 800-70, 800-81, 800-82, 800-83

FISCAM Controls	Related NIST Publications
General Controls: Segregation of Duties	
SD-1. Segregate incompatible duties and establish related policies	NIST SP 800-12, 800-66, 800-98
SD-2. Control personal activities through formal operating procedures, supervision, and review	NIST SP 800-12, 800-66, 800-98
General Controls: Contingency Planning	
CP-1. Assess the criticality and sensitivity of computerized operations and identify supporting resources	FIPS 199; NIST SP 800-30, 800-37, 800-40, 800-59, 800-60, 800-66
CP-2. Take steps to prevent and minimize potential damage and interruption	NIST SP 800-12, 800-21, 800-24, 800-25, 800-34, 800-41, 800-43, 800-44, 800-45, 800-50, 800-57, 800-58, 800-66, 800-69, 800-81, 800-83, 800-84, 800-98
CP-3. Develop and document a comprehensive contingency plan	NIST SP 800-12, 800-13, 800-14, 800-34, 800-66
CP-4. Periodically test the contingency plan and adjust it as appropriate	NIST SP 800-12, 800-14, 800-34, 800-56, 800-66, 800-84

FISCAM Controls	Related NIST Publications
Business Process Application Level Controls: Application Level General Controls	
AS-1. Implement effective application security management	For AS-1 – AS-5 controls, the related NIST publications are identified under related General Controls above.
AS-2. Implement effective application access controls	
AS-3. Implement effective application configuration management	
AS-4. Segregate application user access to conflicting transactions and activities and monitor segregation	
AS-5. Implement effective application contingency planning	
Business Process Application Level Controls: Business Process Controls	
BP-1. Transaction data input is complete, accurate, valid, and confidential	NIST SP 800-44, 800-57
BP-2. Transaction data processing is complete, accurate, valid, and confidential	NIST SP 800-44, 800-57
BP-3. Transaction data output is complete, accurate, valid, and confidential	NIST SP 800-44, 800-57

FISCAM Controls	Related NIST Publications
Business Process Application Level Controls: Business Process Controls	
BP-4. Master data setup and maintenance is adequately controlled	NIST SP 800-44, 800-57
Business Process Application Level Controls: Interface Controls	
IN-1. Implement an effective interface strategy and design	NIST SP 800-44, 800-57
IN-2. Implement effective interface processing procedures	NIST SP 800-44, 800-57
Business Process Application Level Controls: Data Management Controls	
DA-1. Implement an effective data management system strategy and design	

Appendix V - Knowledge, Skills, and Abilities Needed to Perform Information System Controls Audits

Information system (IS) controls audits require a broad range of technical skills. A key component of planning is determining the knowledge, skills, and abilities needed to perform the IS audit. Such needs are then compared with the audit team's current knowledge, skills, and abilities to identify any expertise that must be acquired. Any expertise gap can be filled through hiring, training, contracting, or staff sharing. The knowledge, skills, and abilities described in this appendix are not intended to be prescriptive, but to provide a framework to assist the auditor in determining the audit resources needed to effectively perform audit procedures in an IS audit. In addition, when contracting for IS audit services, this framework may be used as resource to identify the specific knowledge, skills, and abilities that will be needed to perform the contracting services requested.

Generally accepted government auditing standards (GAGAS) state that the "staff assigned to conduct an audit or attestation engagement under GAGAS must collectively possess the technical knowledge, skills, and experience necessary to be competent for the type of work being performed before beginning work on that assignment." The standards further require that if the work involves a review of information systems, the staff assigned to the GAGAS audit engagement should collectively possess knowledge of information technology.[117]These skills are often described in terms of knowledge, skills, and abilities (KSAs). KSAs are typically used in job position descriptions and job announcements to describe the attributes required for those in particular jobs. These terms are defined as follows:

[117]*Government Auditing Standards: July 2007 Revision* (GAO-07-731G), paragraph 3.43.

Knowledge—the foundation upon which skills and abilities are built. Knowledge is an organized body of information, facts, principles, or procedures that, if applied, make adequate performance of a job possible. An example is knowledge of tools and techniques used to establish logical access control over an information system.

Skill—the proficient manual, verbal, or mental manipulation of people, ideas, or things. A skill is demonstrable and implies a degree of proficiency. For example, a person may be skilled in operating a personal computer to prepare electronic spreadsheets or in using a software product to conduct an automated review of the integrity of an operating system.

Ability—the power to perform a job function while applying or using the essential knowledge. Abilities are evidenced through activities or behaviors required to do a job. An example is the ability to apply knowledge about logical access controls to evaluate the adequacy of an organization's implementation of such controls.

A staff member's knowledge, skills, and abilities can be categorized in accordance with FISCAM audit areas. Table 1 includes an overview of the knowledge, skills, and abilities that a team typically needs to effectively perform an IS audit. It assumes a level of proficiency in performing basic auditing tasks, such as interviewing, gathering and documenting evidence, communicating both orally and in writing, and managing projects. It focuses on attributes associated specifically with IS auditing. Although each staff member assigned to such an audit need not have all these attributes, the audit team must collectively possess the KSAs necessary to perform the audit, including adequately planning the audit, assessing the effectiveness of IS controls, testing IS controls, determining the effect of the results of testing on the audit objectives, developing findings and recommendations, and reporting the results. Audit resources may be supplemented from outside the organization through partnering or engaging consultants.

Table 1. Knowledge, Skills, and Abilities for IS Security Audit Areas by FISCAM Objective

FISCAM objective	Associated knowledge, skills, and abilities

Security Management	• Knowledge of the legislative requirements for an entity's information security management program
	• Knowledge of the sensitivity of data and the risk management process through risk assessment and risk mitigation
	• Knowledge of the risks associated with a deficient information security management program
	• Knowledge of the key elements of a good information security management program
	• Ability to analyze and evaluate an entity's security policies and procedures and identify their strengths and weaknesses
	• **Ability to analyze and evaluate the entity's security management program and identify the strengthens and weaknesses, including:**
	  • security management program, structure, and responsibilities, including system inventories
	  • risk assessment
	  • security awareness training for employees, contractors, third parties (including those in sensitive security and data processing position) and security-related personnel policies (including personnel hiring, including reference and background checks, and job transfers and terminations),
	  • performance of periodic tests and evaluations of IS controls and monitoring to ensure compliance with established policies and procedures (including copies of tests and evaluations performed), and
	  • security requirements and monitoring activities of third-party providers supporting specific application(s).

FISCAM objective	Associated knowledge, skills, and abilities

Access Control	• Knowledge across platforms of the access paths into computer systems and of the functions of associated hardware and software that provides an access path
	• Knowledge of access level privileges granted to users and the technology used to provide and control them
	• Knowledge of the procedures, tools, and techniques that provide for good physical, technical, and administrative controls over access
	• Knowledge of the risks associated with inadequate access controls
	• Skills to perform vulnerability assessments of the entity's applications and supporting computer systems
	• **Ability to analyze and evaluate the entity's access controls and identify the strengthens and weaknesses, including:**
	  • system boundaries
	  • controlling remote access to entity information, including use of remote devices,
	  • user and system identification and authentication,
	  • requesting, approving, and periodically reviewing user access authorization,
	  • restricting access to sensitive system resources (including system utilities, system software, and privileged accounts),
	  • protecting digital and sensitive media, including portable media,
	  • applying cryptography methods, if used,
	  • monitoring mainframe, mid-level servers, and network systems for incidents, including management response and reporting on unusual activities, intrusion attempts, and actual intrusions, and
	  • controlling physical security, including granting and controlling of physical access to the data center and other IT sensitive areas.

FISCAM objective	Associated knowledge, skills, and abilities

Configuration Management	• Knowledge of the concept of configuration management and the System Development Life Cycle (SDLC) process
	• Knowledge of baseline configuration management procedures, tools, and techniques that provide control over application and system software, and computer security settings
	• Knowledge of the risks associated with the modification, including emergency changes, of application and system software, and computer security settings
	• Knowledge of the risks associated with inadequate procedures for updating software to protect against known vulnerabilities
	• Ability to analyze and evaluate the entity's configuration management and identify the strengths and weaknesses, including:
	  • configuration management policies, including the approval and testing of scheduled and emergency changes, and monitoring procedures to ensure compliance,
	  • maintaining current configuration information,
	  • authorizing, testing, approving, and tracking all configuration changes,
	  • monitoring/auditing the configuration,
	  • patch management, vulnerability scanning, virus protection, emerging threats, and user installed software, and
	  • emergency changes.

Segregation of Duties	• Knowledge of the different functions involved with information systems and data processing and incompatible duties associated with these functions • Knowledge of the risks associated with inadequate segregation of duties • Ability to analyze and evaluate the entity's organizational structure and segregation of duties (including periodic review of access authorizations) and identify the strengths and weaknesses

Contingency Planning	• Knowledge of the procedures, tools, and techniques that provide for contingency planning and business continuity
	• Knowledge of the risks that exist when measures are not taken to provide for contingency planning and business continuity
	• Ability to analyze and evaluate an entity's contingency planning program and contingency plans for business continuity and identify the strengths and weaknesses, including:
	  • assessing the availability needs of entity systems
	  • backing-up data, programs, and software, and
	  • environmental controls, including emergency power, fire/smoke detection and response, hardware maintenance and problem management, alternate work sites, etc.

FISCAM objective	Associated knowledge, skills, and abilities
Business Process Controls	• Knowledge about the practices, procedures, and techniques that provide for the completeness, accuracy, validity, and confidentiality of application data • Knowledge of typical applications in each business process transaction cycle • Skills to use a generalized audit software package to conduct data analyses and tests of application data, and to plan, extract, and evaluate data samples • Ability to analyze and evaluate the entity's application controls and identify the strengths and weaknesses

Source: GAO.

Auditors performing tasks in two of the above FISCAM areas—**Access Controls and Configuration Management**—require additional specialized technical skills. Such technical specialists should have skills in one or more of the categories listed in table 2.

Table 2. KSAs for Information Security Technical Specialists

Specialist	Skills
Network analyst	• Advanced knowledge of network hardware and software • Understanding of data communication protocols • Ability to evaluate the configuration of routers , firewalls, and intrusion detection systems • Ability to perform external and internal vulnerability tests with manual and automated tools • Knowledge of the operating systems used by servers
Windows/Novell analyst	• Detailed understanding of microcomputer and network architectures • Ability to evaluate the configuration of servers and the major applications hosted on servers • Ability to perform internal vulnerability tests with manual and automated tools
Unix analyst	• Detailed understanding of the primary variants of the Unix architectures • Ability to evaluate the configuration of servers and the major applications hosted on servers • Ability to perform internal vulnerability tests with manual and automated tools
Database analyst	• Understanding of the control functions of the major database management systems • Understanding of the control considerations of the typical application designs that use database systems • Ability to evaluate the configuration of major database software products

Specialist	Skills
Mainframe system software analyst	• Detailed understanding of the design and function of the major components of the operating system • Ability to develop or modify tools necessary to extract and analyze control information from mainframe computers • Ability to use audit software tools • Ability to analyze modifications to system software components
Mainframe access control analyst	• Detailed understanding of auditing access control security software such as ACF2, Top Secret, and RACF • Ability to analyze mainframe audit log data • Ability to develop or modify tools to extract and analyze access control information

Source: GAO.

As table 2 shows, some activities require a high degree of IT knowledge, skills, and abilities, while others involve more basic auditing tasks (interviewing, gathering background information, and documenting the IT security environment). Audit management may therefore want to organize staff that have highly specialized technical skills into a separate group that has access to special-purpose computer hardware and software. A group of this kind can focus on more technical issues, while other groups within the organization can perform the less technical work.

Appendix VI - Scope of an Information System Controls Audit in Support of a Financial Audit

This appendix provides a framework for assessing the effectiveness of information system controls audits in support of financial statement audits. Given the prevalence of the use of information systems to process financial information, performing a financial audit generally includes an assessment of the effectiveness of information system controls. The information system controls audit should be performed as an integral part of the financial audit.

This appendix is intended to assist (1) financial auditors in communicating audit requirements to IS control specialists, and (2) financial auditors and IS control specialists in understanding how an assessment of the effectiveness of IS controls integrates with financial audit requirements.

The Government Accountability Office (GAO) and the President's Council on Integrity and Efficiency (PCIE) *Financial Audit Manual* (FAM) presents a methodology for performing financial statement audits of federal entities in accordance with professional standards. Chapter 2 (and related steps in Chapter 4) of the FISCAM describe a methodology for performing the IS controls audit in the context of an audit performed in accordance with generally accepted government auditing standards (GAGAS). This appendix discusses how the audit steps described in Chapter 2 of the FISCAM (and related steps in Chapter 4) provide more specific guidance concerning the evaluation of the effectiveness of information systems controls in support of the audit steps in the FAM. For financial audits performed in accordance with the FAM, the steps in the FISCAM should be performed in coordination with the related steps in the FAM. The flowchart of steps in assessing IS controls in a financial statement audit, appearing in FAM 295 J, is presented at the end of this appendix.

The following table presents a summary of the relationship between selected FAM steps and related FISCAM steps.

FAM Step(s)	Related FISCAM Step(s)
AUDIT PLANNING	
220 Understand the Entity's Operations 235 Identify Significant Line Items, Accounts, Assertions, and RSSI 240 Identify Significant Cycles, Accounting Applications, And Financial Management Systems	2.1.1 Planning the Information System Controls Audit—Overview 2.1.2 Understand the Overall Audit Objectives and Related Scope of the Information System Controls Audit 2.1.3 Understand the Entity's Operations and Key Business Processes 2.1.4 Obtain a General Understanding of the Structure of the Entity's Networks 2.1.5 Identify Key Areas of Audit Interest (files, applications, systems, locations)
260 Identify Risk Factors	2.1.6 Assess Information system Risk on a Preliminary Basis
270 Determine Likelihood of Effective IT System Controls	2.1.7 Identify Critical Control Points (for example, external access points to networks) 2.1.8 Obtain a Preliminary Understanding of Information System Controls
Miscellaneous FAM planning sections	2.1.9 Perform Other Audit Planning Procedures

INTERNAL CONTROL TESTING	
310 Overview of the Internal Control Phase 320 Understand Information Systems 330 Identify Control Objectives 340 Identify and Understand Relevant Control Activities 350 Determine the Nature, Timing, and Extent of Control Tests And Of Tests For Systems' Compliance With FFMIA Requirements 360 Perform Nonsampling Control Tests And Tests For Systems' Compliance With FFMIA Requirements, including 360.03-.09—Test IT System Controls	2.2 Perform Information System Controls Audit Tests • Understand Information Systems Relevant to the Audit Objectives • Identify IS Control Techniques Relevant to the Audit Objectives • Test IT System Controls
REPORTING THE RESULTS OF THE IS CONTROLS AUDIT	
370 Assess Controls On A Preliminary Basis 580 Draft Reports – Internal Control	2.3 Report Audit Results

AUDIT PLANNING

IS Audit Resources

As discussed in FAM Section 110.27, the audit team should possess sufficient knowledge of IS controls to determine the effect of IT on the audit, to understand IS controls, and to consult with an IS

controls specialist[118] to design and test IS controls. Specialized IS audit skills generally are needed in situations where

- the entity's systems, automated controls, or the manner in which they are used in conducting the entity's business are complex;
- significant changes have been made to existing systems or new systems have been implemented;
- data are extensively shared among systems;
- the entity participates in electronic commerce;
- the entity uses emerging technologies; or
- significant audit evidence is available only in electronic form.

In some cases, the financial auditor may consult with IS controls specialists within the audit organization or use outside contractors to provide these skills. However, per AU 311.22, the financial auditor should have sufficient knowledge to communicate the objectives of the specialists' work, to evaluate whether the specified procedures will meet the audit objectives, and to evaluate the results of the procedures as they relate to the nature, extent, and timing of further planned audit procedures.

Appendix V of the FISCAM provides a framework to assist the auditor in determining the audit resources needed to effectively perform an IS controls audit. In addition, when contracting for IS systems audit services, this framework may be used as a resource to identify the specific knowledge, skills, and abilities that will be needed to perform the contracting services requested. Section 2.1.9.D "Audit Resources" in Chapter 2 provides additional information on the use of IS controls specialists in a GAGAS audit.

[118] The IS control specialist is a person with technical expertise in information technology systems, general controls, business process applications and controls, and information security.

The following sections discuss IT-related FAM steps and the related FISCAM steps.

Understand the Entity's Operations, Identify Significant Line Items, Accounts, Assertions, and RSSI, and Identify Significant Cycles, Accounting Applications, and Financial Management Systems

FAM 220.01 states that the auditor must obtain an understanding of the entity and its environment, including internal control to assess the risk of material misstatement of the financial statements, whether due to error or fraud, and to design the nature, extent, and timing of further audit procedures. The following IT-related FAM sections discuss obtaining an understanding of the entity's operations and information systems:

- 220.04—the auditor should identify significant external and internal factors that affect the entity's operations as part of understanding the entity and its environment for purposes of planning the audit, including the IT structure and the extent to which IT processing is performed externally such as through cross-servicing agreements.

- 220.07—the auditor should develop and document a high-level understanding of the entity's use of IS controls and how IT affects the generation of financial statement information and supplementary information. An IS controls specialist may assist the auditor in understanding the entity's use of IS controls. Appendix I of the FISCAM may be used to document this understanding.

- 235.01—the auditor should identify significant line items and accounts in the financial statements and significant related financial statement assertions.

- 240.08—once the auditor identifies significant accounting applications, the auditor should determine which information systems are involved in those applications.

- 240.09—the auditor should obtain sufficient knowledge of the information systems relevant to financial reporting to

understand the accounting processing from initiation of a transaction to its inclusion in the financial statements, including electronic means used to transmit, process, maintain, and access information (see AU 319.49, SAS No. 94).

The following FISCAM sections (Chapter 2) provide more specific guidance on how the auditor obtains an understanding of the entity's IT operations and information systems:

- Planning the information system controls audit—overview – 2.1.1
- Understand the entity's operations and key business processes - 2.1.3
- Obtain a general understanding of the structure of the entity's networks – 2.1.4
- Identify key areas of audit interest (files, applications, systems, locations) – 2.1.5

More specifically, based on the audit objectives and the auditor's understanding of the business processes and networks, the auditor's identification of key areas of audit interest includes:

- key business process applications and where each key business process application is processed,
- key data files used by each key business application, and
- relevant general controls at the entitywide and system levels, upon which application level controls depend.

These FISCAM sections include information related to the IS controls audit that should be included in audit documentation. Such information should be summarized, as appropriate, in the entity profile or an equivalent document, as discussed in FAM Section 290.04. However, the auditor generally should document internal control separately as discussed below and in FAM 390.

Identify Risk Factors

FAM Section 260.09 states that the auditor should (1) identify conditions that significantly increase inherent, fraud, and control risk (based on identified control environment, risk assessment, communication, or monitoring weaknesses) and (2) conclude

whether any identified control risks preclude the effectiveness of specific control activities in significant applications. The auditor should identify specific inherent risks, fraud risks, and control environment, risk assessment, communication, and monitoring weaknesses based on information obtained in the planning phase, primarily from understanding the entity's operations, including significant IT processing performed outside the entity and preliminary analytical procedures. SAS No. 70 reports, which are discussed further in FAM 310 and in Appendix VII, may be prepared by service auditors for organizations performing significant IT processing for the entity. The auditor may find these reports useful for performing risk assessments and planning other audit procedures. The auditor should update the risk assessment throughout the audit.

FAM Section 260.22 states that IS controls do not affect the audit objectives for an account or a cycle. However, IS controls can introduce inherent risk factors not present in a manual accounting system. The FAM section states that the auditor should assess the overall impact of IS processing on inherent risk. The impact of these factors typically will be pervasive in nature. An IS controls specialist may assist the auditor in considering these factors and making this assessment.

FAM Section 260.56 states that IS controls affect the effectiveness of control activities, the control environment, risk assessment, communication, and monitoring. For example, controls that normally would be performed by separate individuals in manual systems may be concentrated in one computer application and pose a potential segregation-of-duties issue. See SAS No. 109.57-63 for further discussion of the effect of IT on internal control.

FAM Section 260.57 provides several IS factors, discussed in Chapter 2 of the FISCAM, that the auditor should evaluate in making an overall assessment of the control environment, risk assessment, communication, and monitoring.

The FISCAM section 2.1.6 entitled "Assess Information System Risk on a Preliminary Basis" provides more specific guidance on how the auditor identifies IS risk (inherent and the control environment, risk assessment, communication, and monitoring components of internal

control). Also, the FISCAM section 2.1.9.B entitled "Consideration of the Risk of Fraud" provides more specific guidance concerning identification of the risk of fraud arising from IT, including coordination between the financial auditor and the IS controls specialist. In addition, the FISCAM section 2.5.1 "Additional IS Risk Factors" provides more risk factors for the auditor to consider. Further, FISCAM Appendix VII provides more information on the use of SAS 70 reports.

These FISCAM sections include information that should be included in audit documentation. In addition, such information should be summarized, as appropriate, in the GRA or equivalent document as discussed in FAM Section 290, including:

- the assessments of overall inherent risk and the risk factors considered in the assessment, and
- the assessments of the overall effectiveness of the control environment, risk assessment, communication, and monitoring, including whether an ineffective control environment precludes the effectiveness of specific control activities.

Determine Likelihood of Effective IS Controls

As discussed in FAM 270, information system (IS) controls consist of those internal controls that are dependent on information systems processing and include general, business process application, and user controls. IS controls consist of those internal controls that are dependent on information systems processing and include general controls (entitywide, system, and business process application levels), business process application controls (input, processing, output, master file, interface, and data management system controls), and user controls (controls performed by people interacting with information systems). General and business process application controls are always IS controls. A user control is an IS control if its effectiveness depends on information systems processing or the reliability (accuracy, completeness, and validity) of information processed by information systems. Conversely, a user control is not an IS control if its effectiveness does not depend on information systems processing or the reliability of information processed by information systems.

In the financial audit planning phase, the auditor, with the assistance of an IS control specialist should determine whether IS controls are likely to be effective and should therefore be considered in the internal control phase. The auditor may coordinate work done to meet the provisions of FISMA with work done as part of the financial statement audit.

The procedures performed to determine the likelihood of effective IS controls build on those procedures performed while understanding the entity's operations and assessing the effects of IS controls on inherent risk and the control environment, risk assessment, communication, and monitoring. Under SAS No. 109, the auditor should sufficiently understand each of the five components of internal control—control environment, risk assessment, information and communication, monitoring, and control activities—to assess the risk of material misstatement. This understanding should include relevant IS aspects.

As discussed in FAM 260.06, the auditor evaluates and tests the following types of controls in a financial statement audit:

- financial reporting controls,
- compliance controls, and
- certain operations controls (to the extent described in FAM 275).

For each of the specific controls to be evaluated and tested, as documented in the SCE Form or equivalent, the auditor should distinguish which are IS controls. In addition, based on such IS controls and the audit planning procedures (particularly the identification of critical control points), the auditor should identify those other IS controls (general and business process application controls) upon which the effectiveness of the controls in the SCE depend. These other IS controls also need to be effective for the specific controls in the SCE to be effective. FISCAM Appendices II and III can be used to document such controls.

IS controls can be classified into three types:

- general controls – GAGAS defines information systems general controls as the policies and procedures that apply to all or a large segment of an entity's information systems. General controls help ensure the proper operation of information

systems by creating the environment for proper operation of application controls. General controls include security management, logical and physical access, configuration management, segregation of duties, and contingency planning.

- business process application controls –GAGAS defines application controls, sometimes referred to as business process controls, as those controls that are incorporated directly into computer applications to help ensure the validity, completeness, accuracy, and confidentiality of transactions and data during application processing. Application controls include controls over input, processing, output, master data, application interfaces, and data management system interfaces.
- user controls – portions of controls that are performed by people interacting with IS controls. The effectiveness of user controls typically depend on information systems processing or the reliability of information processed by IS controls.

An IS controls specialist generally should review and concur with the auditor's identification of IS controls.

Testing of technical IS controls should be performed by an IS controls specialist as described in FAM 360. The audit team may work with the IS controls specialist by testing user controls and application controls involving manual follow-up.

FAM Section 270.05 states that early in the audit's planning phase, the auditor and the IS controls specialist should understand the design of each of the three types of IS controls (general, business process application level, and user controls) to the extent necessary to tentatively conclude whether these controls are likely to be effective.

If they are likely to be effective, the auditor should consider specific IS controls in determining whether control objectives are achieved in the internal control phase. As discussed in SAS No. 109.54, evaluating the design of a control involves considering whether the control, individually or in combination with other controls, is capable of effectively preventing, detecting, and correcting material misstatements.

If IS controls are not likely to be effective, the auditor, with the assistance of the IS controls specialist, should obtain a sufficient understanding of control risks arising from IS controls to

- identify types of potential misstatements,
- consider factors that affect the risks of material misstatement,
- design tests of controls and substantive procedures, and
- develop appropriate findings.

Also, in the internal control phase, the auditor generally should focus on the effectiveness of manual controls in achieving control objectives, including manual controls that may mitigate weaknesses in IS controls. If IS controls are not likely to be effective due to poor general controls and if manual controls do not achieve the control objectives, the auditor should identify and evaluate any specific IS controls that are designed to achieve the control objectives to develop recommendations for improving internal controls.

As discussed in SAS No. 109.117-.120, in some circumstances, such as where a significant amount of information is electronically initiated, recorded, processed, and reported, it may not be practical or possible to restrict detection risk to an acceptable level by performing only substantive tests for one or more financial statement assertions. In such circumstances, the auditor should test IS controls to obtain evidential matter about the effectiveness of both the design and operation of controls to reduce the assessed level of the risk of material misstatement.

The following FISCAM sections provide more specific guidance on how the auditor determines the likelihood of effective IS controls:

- Identify critical control points (for example, external access points to networks) – 2.1.7
- Obtain a preliminary understanding of information system controls – 2.1.8

These FISCAM sections include information that should be included in audit documentation. In addition to this audit documentation, as discussed in FAM Section 290, the auditor should document tentative conclusions on the likelihood that IT controls and any compensating controls such as manual controls, reviews, or reconciliations are operating effectively.

Other Audit Planning Procedures

The FISCAM section 2.1.9 provides additional information concerning the following planning steps in the IS controls audit that should be coordinated with the financial audit.

- Relevant laws and regulations—this section provides more specific guidance on how the auditor identifies significant IT related provisions of laws and regulations and should be performed in coordination with FAM Section 245
- Consideration of the risk of fraud—as discussed above, this section provides more specific guidance on how the auditor identifies the risk of fraud arising from IT, including coordination between the financial auditor and the IS controls specialist, and should be performed in coordination with FAM Section 260.
- Audit Resources—as discussed above, this section provides more specific guidance on how the auditor identifies the knowledge, skills, and abilities needed to perform an IS controls audit and the auditor's responsibilities and procedures for using the work of an IS controls specialist, and should be performed in coordination with FAM Section 110.
- Multiyear testing plans—this section provides more specific guidance on how the auditor establishes a multiyear testing plan for IS controls, and should be performed in coordination with FAM Section 395G.
- Communication with entity management and those charged with governance—this section provides more specific guidance on communicating relevant IT-related information with entity management and those charged with governance, and should be performed in coordination with FAM Section 215.
- Service organizations—this section provides more specific guidance on the auditor's consideration of IS controls, significant to the IS audit, that are performed by a service organization. This issue is discussed further in Appendix VII "Entity's Use of Service Organizations". This section should be performed in coordination with FAM 310.
- Using the work of others—this section provides more specific guidance on how the auditor prepares uses the work of others in performing the IS controls audit, and should be performed in coordination with FAM section 650.

- Audit plan—this section provides more specific guidance on how the auditor prepares an audit plan and strategy for performing the IS controls audit, and should be performed in coordination with FAM section 290.

Also the FISCAM provides more specific guidance on how the auditor documents the planning of the IS controls audit, and should be performed in coordination with FAM Section 290.

INTERNAL CONTROL TESTING

Overview

In general, FAM Section 300 describes the methodology for assessing the effectiveness of internal control in a financial audit. FAM Section 310 summarizes the methodology. Specifically, Section 310 states that, in the internal control phase, the auditor should gain an understanding of internal control and obtain evidence about the effectiveness of internal control to (1) assess control risk, (2) determine the nature, timing, and extent of control, compliance, and substantive testing, and (3) form an opinion or report on internal control over financial reporting and compliance. Control risk should be assessed separately for each significant financial statement assertion in each significant cycle/accounting application (including RSSI).

The auditor of federal financial statements must evaluate and test certain controls. AU 319 permits the auditor to assess control risk at a high (maximum) level and forgo evaluation and testing of financial reporting controls if the auditor believes evaluating their effectiveness would be inefficient. However, because OMB audit guidance requires the auditor to perform sufficient tests of internal controls that have been properly designed and placed in operation to support a low assessed level of control risk, the auditor in a federal financial audit may not elect to forgo control tests solely because it is more efficient to extend compliance and substantive audit procedures.

The following are the types of controls tested in a financial audit:

- financial reporting controls (including certain safeguarding and budget controls) for each significant assertion in each significant cycle/accounting application (identified in section 240),
- compliance controls for each significant provision of laws and regulations (identified in section 245), including budget controls for each relevant budget restriction (identified in section 250), and
- operations controls for each operations control (1) relied on in performing financial audit procedures or (2) selected for testing by the audit team. (see section 275).

The auditor is not required to test controls that have not been properly designed and implemented (placed in operation). Thus, internal controls that are not effective in design do not need to be tested. If the auditor determined in a prior year that controls in a particular accounting application were ineffective and if management indicates that controls have not improved, the auditor need not test them.

On the other hand, if controls have been determined to be effective in design and implemented (placed in operation), the auditor of federal financial statements must perform sufficient tests of their effectiveness to support a low assessed level of control risk. In such cases, the auditor may consider using a rotation approach to testing controls over the various accounting applications, as described in FAM Section 395 G (and in the FISCAM section 2.1.9.E “Multiyear Testing Plans”). If the auditor expects to disclaim an opinion because of scope limitations or inadequate controls, the auditor may limit internal control work to updating the understanding of controls and whether they have been placed in operation. The auditor may do this by inquiring as to whether previously identified control weaknesses have been corrected. In the year the auditor expects to issue an opinion on the financial statements, the auditor needs a basis of sufficient work on internal control.

In the internal control phase of a financial audit, the auditor should perform and document the following procedures:

- Understand the entity's information systems for financial reporting, compliance with laws and regulations, and relevant operations (see FAM Section 320).
- Identify control objectives (see FAM Section 330).
- Identify and understand relevant control activities that effectively achieve the control objectives (see FAM Section 340).
- Determine the nature, timing, and extent of control testing (see FAM Section 350).
- Perform control tests that do not involve sampling (nonsampling control tests - see section 360).1 (Sampling control tests, if necessary, are performed in the testing phase, as discussed in FAM Section 450.)
- On a preliminary basis, based on the evidence obtained, assess (1) the effectiveness of financial reporting, compliance, and relevant operations controls and (2) control and combined risk (see FAM Section 370). (Combined risk, which includes inherent and control risk, is discussed in FAM paragraph 370.09).

As discussed in FAM Section 310.10, in gaining an understanding of an entity's internal control, including internal control related to IT and other business processing performed outside the entity, the auditor should obtain evidence about the design of relevant controls and whether they have been placed in operation. In obtaining evidence about whether controls have been placed in operation, the auditor should determine whether the entity is using them, rather than merely having them written in a manual, for example. This differs from determining a control's operating effectiveness, which is concerned with how the control was applied, the consistency with which it was applied, and by whom. Gaining an understanding of the design of internal control does not require that the auditor obtain evidence about operating effectiveness.

As discussed in FAM Section 310.11, the auditor should obtain an understanding of internal control for IT and other business processing performed outside the entity under a service agreement or other contract arrangements for assessing risk and planning other audit procedures. The auditor may obtain this understanding by performing work directly at the service organization or by using SAS

No. 70 reports that include these internal controls as discussed in AU 324.06-.21.

For each potential weakness, consider the impact of compensating controls or other factors that mitigate or reduce the risks related to potential weaknesses.

The following sections summarize FAM audit steps related to the testing of information system controls. The auditor should coordinate these steps with the related FISCAM steps.

Understand Information Systems

FAM Section 320 states that the auditor may use an IS controls specialist to assist in understanding and documenting the IT aspects of these systems. The auditor should document the understanding of these systems in cycle memorandums, or other equivalent narratives, and generally should prepare or obtain related flow charts. FAM 340 and 350 discuss identifying and documenting controls that are designed to mitigate the risk of material misstatement.

Walk-throughs are important for understanding the transaction process and for determining appropriate audit procedures. The auditor should perform walk-throughs for all significant accounting applications. Walk-throughs of budget, accounting, compliance, and operations systems provide evidence about the functioning of such systems. The auditor should document these walk-throughs. The auditor should incorporate the IT aspects of each system into the audit documentation and may include additional flow charts, narratives, and checklists.

FAM Section 320 continues that the auditor should obtain an understanding of and should document the following for each significant cycle and accounting application (including those dealing with RSSI):

- The manner in which transactions are initiated;
- The nature and type of records, journals, ledgers, and source documents, and the accounts involved;

- The processing involved from the initiation of transactions to their inclusion in the financial statements, including the nature of computer files and the manner in which they are accessed, updated, and deleted; and
- The process used to prepare the entity's financial statements and budget information, including significant accounting estimates, disclosures, and computerized processing.

FAM Section 320.03 states that for each significant cycle and accounting application identified for significant line items and assertions in FAM 240 (including those dealing with RSSI) the auditor should obtain an understanding of and should document, among other things, processes used to prepare the entity's financial statements and budget information, including significant accounting estimates, disclosures, and IT processing. These processes include

- Procedures used to enter transaction totals into the general ledger;
- procedures used to initiate, authorize, record, and process journal entries in the general ledger;
- procedures used to record recurring and nonrecurring adjustments to the financial statements;
- procedures used to combine and consolidate general ledger data; and
- closing process, including manual and automated procedures, for preparing the financial statements and related disclosures.

The FISCAM section entitled "Understand Information Systems Relevant to the Audit Objectives" included in section 2.2 provides more specific guidance on how the auditor obtains an understanding of information systems. This FISCAM section includes information that should be included in audit documentation. As discussed in FAM Section 320, the auditor must document the understanding gained of each component of internal control, including the information system. The auditor should prepare sufficient documentation to clearly describe the accounting system. For each significant cycle, the auditor should prepare a cycle memorandum or equivalent. Also, the auditor generally should prepare an illustrative flowchart of the cycle and component accounting application(s). Flowcharts provide a good mechanism to document the process and the flow of transactions through the system.

However, the auditor should avoid extreme detail, which makes the charts confusing and hard to follow. Complex systems, particularly those involving IT, may be difficult to understand without a flowchart. To the extent required as described above, the auditor should use the following documents or equivalents to document.

Identify Relevant Control Objectives

FAM Section 330 discusses the identification of control objectives. In a financial audit, the auditor should identify control objectives for each type of control that if achieved, would provide the entity with reasonable assurance that individual and aggregate misstatements (whether caused by error or fraud), losses, or noncompliance material to the financial statements would be prevented or detected. For Required Supplementary Stewardship Information (RSSI), the Statement of Social Insurance, and nonmonetary information in the financial statements, such as physical units of heritage assets, the objectives would relate to controls that would provide reasonable assurance that misstatements, losses, or noncompliance that would be considered material by users of the information would be prevented or detected. As noted above, control objectives in a financial audit involve:

- financial reporting controls, including safeguarding controls and segregation-of-duties controls,
- compliance controls,
- budget controls, and
- relevant operations controls.

As discussed in FAM Section 495A.21, if the reliability of internally-generated data used in the substantive analytical procedures is dependent on the effectiveness of IS controls, the auditor should perform additional procedures before relying on the data. The auditor should test, as appropriate, (1) the relevant general controls and the specific business process application level controls over the data and/or (2) the data in the report.

The FISCAM section "Identify IS Control Techniques That are Relevant to the Audit Objectives" included in section 2.2 provides more specific guidance on how the auditor identifies relevant IS control activities. This FISCAM section includes information that

should be included in audit documentation. In addition to such documentation, as discussed in FAM Sections 390 and 395H, the auditor documents relevant control objectives in the SCE form or equivalent documentation. Based on such controls and the audit planning procedures (particularly the identification of critical control points), the auditor should identify those other IS controls (general, business process application, interface, and data management system controls) upon which the controls in the SCE depend. FISCAM Appendices II and III can be used to document such controls.

Identify Relevant Control Activities

As discussed in FAM Section 340, the auditor identifies and understands relevant control activities. For each control objective, based on discussions with entity personnel and the results of other procedures performed, the auditor should identify the control activities designed to achieve the specific control objective. The auditor may indicate these controls in the auditor's informal notes and/or interview write-ups for use in the following procedures, but the auditor need not formally document them on the SCE worksheet at this time. The auditor should first screen the activities to identify those that are effective and efficient to test. An IS controls specialist may assist the auditor in identifying and understanding IT controls. As discussed in FAM 350, the auditor should use walk-throughs to confirm that the entity has implemented these controls identified for further audit procedures. These walk-throughs are in addition to those performed earlier to understand the transaction processing. As discussed in FAM 270, in determining whether control objectives are achieved, the auditor should consider both manual and IS controls, if likely to be effective.

FAM Section 340.05 states that the auditor also should evaluate the appropriateness of the specified criteria used to identify items in a management or exception report. For example, IT input controls (such as the matching of vendor invoices with receiving reports and purchase orders) that require exact matches of data from different sources before a transaction is accepted for processing may be more effective than controls that accept transactions that fall within a broader range of values. On the other hand, controls based on exception reports that are limited to selected information or use

more selective criteria may be more effective than lengthy reports that contain excessive information.

The FISCAM section "Identify IS Control Techniques That are Relevant to the Audit Objectives" provides more specific guidance on how the auditor identifies relevant IS controls.

The FISCAM is organized in a hierarchical structure to assist the auditor in performing the IS controls audit. Chapter 3 (general controls) and Chapter 4 (business process application level controls) contain several control categories, which are groupings of related controls pertaining to similar types of risk. For each control category, the manual identifies critical elements—tasks that are essential for establishing adequate controls within the category. For each critical element, there is a discussion of the associated objectives, risks, and control activities, as well as related potential control techniques and suggested audit procedures. This hierarchical structure facilitates the auditor's audit planning and the auditor's analysis of identified control weaknesses.

Because control activities are generally necessary to achieve the critical elements, they are generally relevant to a GAGAS audit unless the related control category is not relevant, the audit scope is limited, or the auditor determines that, due to significant IS control weaknesses, it is not necessary to assess the effectiveness of all relevant IS controls. Within each relevant control activity, the auditor should identify control techniques implemented by the entity and determine whether the control techniques, as designed, are sufficient to achieve the control activity, considering IS risk and the audit objectives. The auditor may be able to determine whether control techniques are sufficient to achieve a particular control activity without evaluating and testing all of the control techniques. Also, depending on IS risk and the audit objectives, the nature and extent of control techniques necessary to achieve a particular control objective will vary.

If sufficient, the auditor should determine whether the control techniques are implemented (placed in operation) and are operating effectively. Also, the auditor should evaluate the nature and extent of testing performed by the entity. Such information can assist in

identifying key controls and in assessing risk, but the auditor should not rely on testing performed by the entity in lieu of appropriate auditor testing. If the control techniques implemented by the entity, as designed, are not sufficient to address the control activity, or the control techniques are not effectively implemented as designed, the auditor should determine the effect on IS controls and the audit objectives.

This FISCAM section includes information that should be included in audit documentation. In addition to this documentation, as discussed in FAM Sections 390 and 395H, the auditor documents relevant controls in the SCE form or equivalent documentation. Based on such controls and the audit planning procedures (particularly the identification of critical control points), the auditor should identify those other IS controls (general, business process application, interface, and data management system controls) upon which the controls in the SCE depend. FISCAM Appendices II and III can be used to document such controls.

Determine the Nature, Timing, and Extent of Control Tests

FAM Section 350 discusses determining the nature, extent, and timing of control tests and compliance with FFMIA. FAM Section 350.01 states that for each control objective, the auditor should

- identify specific relevant control activities to test (FAM 350.06-.08),
- perform walk-throughs to determine whether those controls have been placed in operation (FAM 350.09),
- document these control activities in the SCE worksheet or equivalent (FAM 350.10),
- determine the nature of control tests (FAM 350.11-.18),
- determine the extent of control tests (FAM 350.19-.20), and
- determine the timing of control tests (FAM 350.21).

As discussed in FAM Section 350, for each control objective identified in FAM 330, the auditor should identify the control activity, or combination of control activities, that is likely to (1) achieve the control objective and (2) improve the efficiency of control tests. In doing this, the auditor should consider (1) the extent of any inherent risk and control environment, risk

assessment, communication, or monitoring weaknesses, including those related to IS controls (as documented in the ARA and/or audit strategy document, or equivalent (see FAM 260)), and (2) the tentative determination of the likelihood that IS controls will be effective, as determined in the planning phase (see FAM 270). The auditor generally should test only the control activities necessary to achieve the objective.

If, in any phase of the audit, the auditor determines that control activities selected for testing are, in fact, ineffective in design or operation, the auditor should discontinue the specific control evaluation of the related control objectives and should report the identified weaknesses in internal control as discussed in FAM 580. This would include situations where the control activities are not effective in design or operation due to ineffective IS controls. If the entity's management does not agree with the auditor's conclusion that effective control activities do not exist or are unlikely to exist, the auditor may need to perform procedures sufficient to support that conclusion.

As discussed in FAM Section 350.10, the auditor should document the control activities to be tested on the SCE worksheet or equivalent (see an illustration in FAM 395 H). The auditor generally should test other components of internal control by observation and inquiry in the planning phase (see FAM 260.09). The auditor may list (and evaluate) controls that satisfy more than one control objective only once and refer to these controls, when applicable, on subsequent occasions. For each control to be tested, the auditor should determine whether the control is an IS control. An IS controls specialist generally should review and concur with the auditor's identification of IS controls.

For every IS control identified above and included in the SCE form or equivalent document, based upon IS controls audit planning, the IS controls specialist should identify the general controls (entitywide, and system levels) and business process application level controls upon which the IS controls depend. Such systems and business process application level controls would principally relate to the critical control points. For example, if the IS control is the review of an exception report, the auditor should identify and test the business process application controls directly related to the

production of the exception report, as well as the general and other business process application controls upon which the reliability of the information in the exception report depends, including the proper functioning of the business process application that generated the exception report and the reliability of the data used to generate the exception report. In addition, the auditor should test the effectiveness of the user control (i.e., management review and followup on the items in the exception report).

Test Information System Controls

FAM Section 360 discusses tests of application controls and user controls. As discussed in FAM Section 360.10, the auditor, with IS controls specialist assistance, generally should perform tests of those application controls and user controls necessary to achieve the control objectives where the entitywide, system, and application-level general controls were determined to be effective.

FAM 360.01 states that the auditor should design and conduct tests of control activities that are effective in design to determine their effectiveness in operation. (See FAM 380.02 if control activities are not effective in design during the entire audit period.) The auditor generally should

- request IS controls specialist assistance and test IS controls (FAM 360.03-.10),
- perform nonsampling control tests (the auditor generally should perform sampling control tests in the testing phase, as discussed in FAM 450), (FAM 360.11-.13), and
- evaluate the results of nonsampling control tests (FAM 360.14-15).

If the auditor identifies IS controls for testing, the auditor, with IS controls specialist assistance, should evaluate the effectiveness of relevant

- general controls at the entitywide and system level;
- general controls at the business process application level; and
- specific business process controls, interface controls, data management system controls and/or user controls, unless the IS controls that achieve the control objectives are general controls.

If controls are not effective, see FAM 360.07 and FAM 360.09.
It is generally more efficient for the auditor to test IS controls on a tiered basis, starting with the general controls at the entitywide and system levels, followed by the general controls at the business process application level, and concluding with tests of business process application, interface, and data management system controls at the business process application level. Such a testing strategy may be used because ineffective IS controls at each tier generally preclude effective controls at the subsequent tier.

The auditor, with IS controls specialist assistance, should determine whether relevant entitywide and system level general controls are effectively designed, implemented, and operating effectively by

- identifying applicable general controls;
- determining how those controls function, and whether they have been placed in operation; and
- evaluating and testing the effectiveness of the identified controls.

The auditor and the IS controls specialist generally should use knowledge obtained in the planning phase. The auditor, with assistance from the IS controls specialist, should document the understanding of general controls and should conclude whether such controls are effectively designed, placed in operation, and, for those controls tested, operating as intended.

Tests of General Controls at the Entitywide and System Levels

The auditor may test general controls through a combination of procedures, including observation, inquiry, inspection (which includes a review of documentation on systems and procedures), and reperformance using appropriate test software. Although sampling is generally not used to test general controls, the auditor may use sampling to test certain controls, such as those involving approvals.

If general controls are not effectively designed and operating as intended, the auditor will generally be unable to obtain satisfaction that application controls are effective. In such instances, the auditor should (1) determine and document the nature and extent of risks

resulting from ineffective general controls and (2) identify and test any manual controls that achieve the control objectives that the IS controls in the SCE or equivalent document were to achieve.

However, if manual controls do not achieve the control objectives, the auditor, with IS controls specialist assistance, should determine whether any specific IS controls are designed to achieve the objectives. If not, the auditor should develop appropriate findings principally to provide recommendations to improve internal control. If specific IS controls are designed to achieve the objectives, but are in fact ineffective because of poor general controls, testing would typically not be necessary, except to support findings.

Tests of General Controls at the Business Process Application Level

If the auditor reaches a favorable conclusion on general controls at the entitywide and system levels, the IS controls specialist should evaluate and test the effectiveness of general controls for those business process applications within which business process application controls or user controls are to be tested.

If general controls are not operating effectively within the application, application controls and user controls generally will be ineffective. In such instances, the IS controls specialist should discuss the nature and extent of risks resulting from ineffective general controls with the audit team. The auditor should determine whether to proceed with the evaluation of application controls and user controls.

Tests of Business Process Application Controls and User Controls

The auditor, with IS controls specialist assistance, generally should perform tests of those business process application controls (business process controls, interface controls, and data management system controls), and user controls necessary to achieve the control objectives where the entitywide, system, and application-level general controls were determined to be effective.

As discussed in FAM Section 360.13, the auditor should test segregation of duties in the situations described in FAM 330.08. The auditor may use the following procedures to test segregation-of-duties controls:

a. Identify the assets to be controlled through the segregation of duties.
b. Identify the individuals who have authorized access (direct or indirect) to the assets. Direct access exists when the individual is authorized to handle the assets directly (such as during the processing of cash receipts). Indirect access exists when the individual is authorized to prepare documents that cause the release or transfer of assets (such as preparing the necessary forms to request a cash disbursement or transfer of inventory).
c. For each individual with authorized access to assets, determine whether there are sufficient asset access controls. Asset access controls are those controls that are designed to provide assurance that actions taken by individuals with authorized access to assets are reviewed and approved by other individuals. For example, an approval of an invoice for payment generally provides asset access controls (relating to cash) over those individuals authorized to prepare supporting documentation for the transaction. If IS controls provide access to assets, the auditor should design tests of IS controls to identify (1) individuals (including IT personnel) who may use the computer to obtain access and (2) asset access controls over such individuals.
d. For individuals with authorized access to assets over which asset access controls are insufficient, determine whether such individuals can affect any recording of transactions in the accounting records. If so, segregation of duties is insufficient, unless such access to accounting records is controlled. For example, the person who processes cash receipts may also be able to record entries in the accounting records.

Such a person may be in a position to manipulate the accounting records to conceal a shortage in the cash account, unless another individual reviews all accounting entries made (and those that should have been made) by that person. In an IT accounting system, access to assets frequently provides access to records. For example,

generation of a check may automatically record a related accounting entry. In such circumstances, a lack of asset access controls would result in inadequate segregation of duties, and the auditor should determine whether other controls would mitigate the effects of this lack of asset access control.

The FISCAM section "Test Information System Controls" included in section 2.2 provides more specific guidance on how the auditor tests relevant IS control techniques. This FISCAM section includes information that should be included in audit documentation. In addition, FISCAM Chapters 3 and 4 provide general controls and business process application level controls consistent with GAGAS categories. In addition, Appendices II and III may be used to document the results of the IS controls audit tests.

As discussed in FAM Section 390, the auditor should document the evaluation of specific control activities in the SCE worksheet or equivalent. The auditor should document control tests in the control test audit plan (formerly referred to as the audit program) and in accompanying documents. The auditor should also document any IT system control tests as discussed in FAM 370.05. FAM 395 H presents an example of a completed SCE worksheet documents. FISCAM Appendices II and III can be used to document such controls.

REPORTING THE RESULTS OF THE IS CONTROLS AUDIT

FAM Sections 370 and 580 discuss the auditor's assessment of the effectiveness of IS controls based on internal control tests performed.

As discussed in FAM Section 370.03, based on the procedures performed, the auditor and IS controls specialist should discuss conclusions on the effectiveness of IS controls and reach agreement. The auditor should (1) incorporate the conclusions into the audit documentation for each IS control tested and (2) perform tests of application controls (principally manual follow-up of exceptions) or user controls identified by the IS controls specialist for the audit team to test.

If the auditor and the IS controls specialist determine that IS controls are effective, the auditor may also ask the IS controls specialist to identify any IS controls within the applications tested that were not previously identified by the auditor using the above procedures. For example, such IS controls might achieve control objectives not otherwise achieved through manual controls or might be more efficient or effective to test than manual controls. The IS controls specialist may assist the auditor in determining the efficiency and effectiveness of searching for and testing additional IS controls. The auditor should document these decisions, including a description of the expected scope of the IS controls specialist's work.

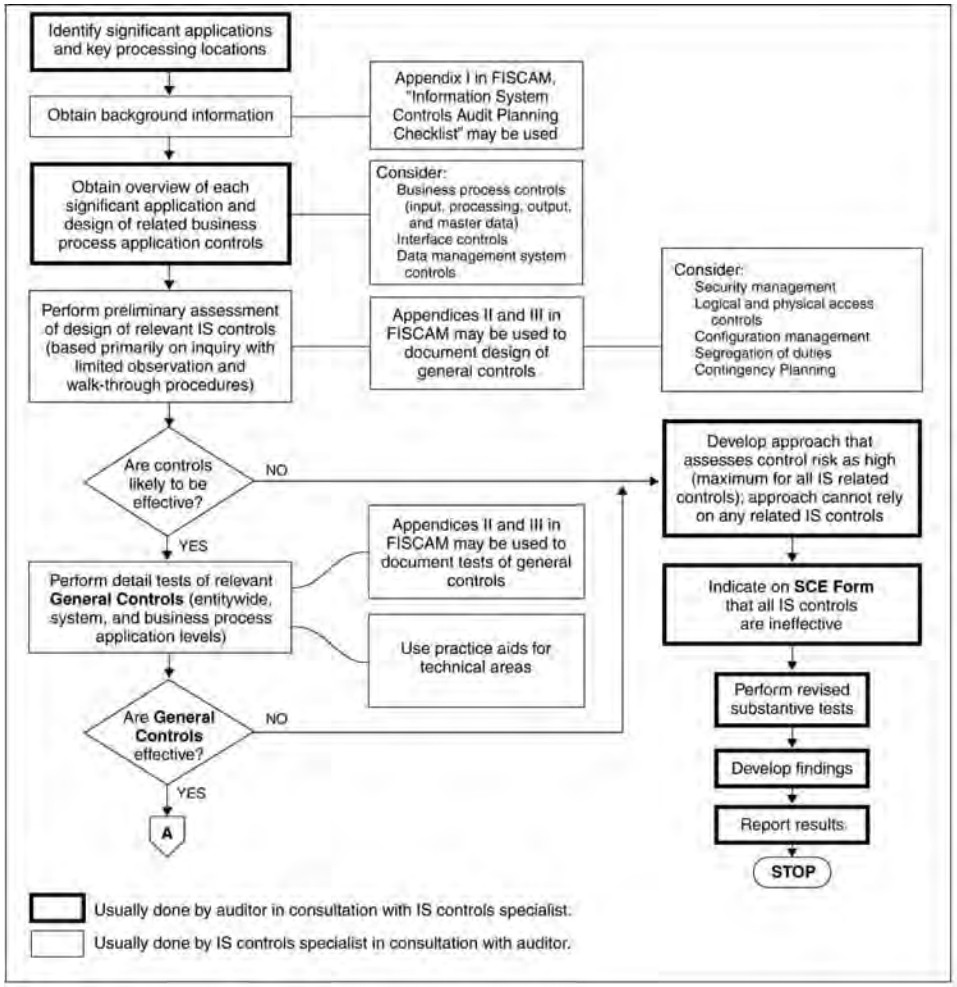
The auditor and the IS controls specialist should work together to document the procedures for evaluating and testing the effectiveness of IS controls and the results of this work.

The FISCAM section 2.3 "Report Audit Results" provides more specific guidance on how the auditor evaluates the results of tests of IS controls within the context of a financial audit. More specifically, the section discusses the auditor's considerations for determining whether IS control weaknesses are material weaknesses, significant deficiencies, and significant deficiencies for purposes of FFMIA reporting.

Steps in Assessing Information System Controls

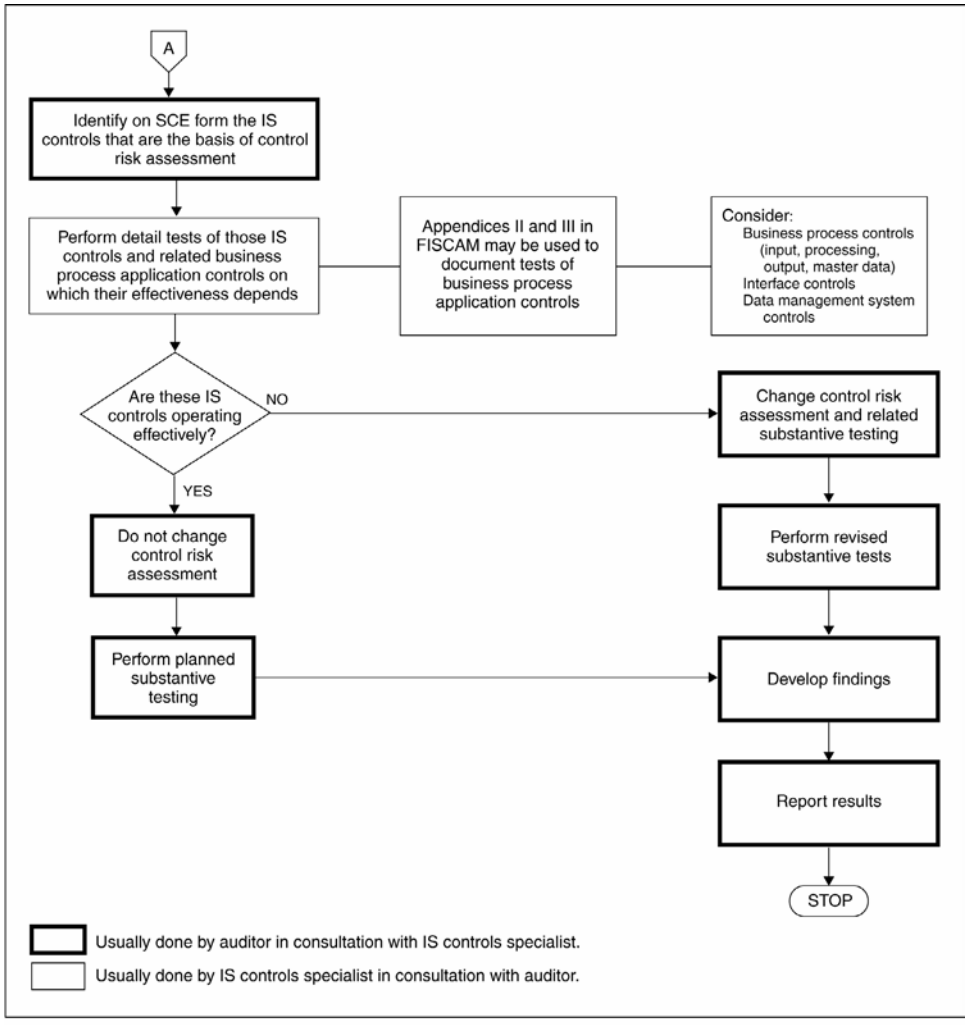
As discussed in FAM 270, the following flowcharts illustrate steps the auditor and the IS controls specialist generally follow in assessing IS controls in a financial statement audit. However, the audit team may decide to test the effectiveness of the general controls even if they are not likely to be effective (see fig. 6) or review business process application controls even though general controls are not effective (see fig. 7), in order to make recommendations on how to fix weak controls.

Figure 6: Steps in Assessing IT Systems Controls in a Financial Statement Audit



Source: GAO.

Figure 7: Steps for Each Significant Application in Assessing Information System Controls in a Financial Statement Audit



Source: GAO.

Appendix VII - Entity's Use of Service Organizations

Many entities use outside service organizations to support business processes. Service organizations provide services ranging from performing a specific task (e.g., payroll processing) to replacing entire business units or functions of an entity. To determine the significance of the functions performed by service organizations to the audit objectives, auditors should obtain information about (1) services performed by the service organizations, (2) the related service organization controls, and (3) their effects on the audit objectives.

If an organization uses a service organization, information and information processing are subjected to controls that may be physically and operationally removed from the user organization. Consequently, an entity's internal control may include controls that are not directly administered by the user organization, but rather by the service organization. For this reason, to obtain an understanding of IS controls, the auditor of the user organization (the user auditor) should gain an understanding of controls at the service organization that may affect the user organization's business processes. This understanding may be gained in several ways, including discussions with management and/or obtaining a service auditor's report. In addition, FISMA requirements specifically apply to information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of the entity.

During the planning stage of the audit, the user auditor should determine the significance of the service organization's controls to the user organization's internal control and to the audit objectives. Factors that may affect the significance to the audit of a service organization's controls include the following:

- The nature and materiality/significance of the transactions or information affected by the service organization

- The degree of interaction between internal control at the user organization and the service organization's controls. The degree of interaction refers to the extent to which a user organization is able to and elects to implement effective controls over the processing performed by the service organization.

With respect to financial audits, a service organization's services are part of an entity's information system, and therefore significant to the user organization's internal control, if they affect any of the following:

- The classes of transactions in the entity's operations that are significant to the financial statements
- The procedures, both automated and manual, by which the entity's transactions are initiated, recorded, processed, and reported, from their occurrence to their inclusion in the financial statements
- The related accounting records (whether electronic or manual), supporting information, and specific accounts in the financial statements involved in initiating, recording, processing, and reporting the entity's transactions
- How the entity's information system captures other events and conditions that are significant to the financial statements
- The financial reporting process used to prepare the entity's financial statements, including significant accounting estimates and disclosures

If the user auditor determines that the service organization's controls are significant to the user organization's internal control, and within the context of the audit objectives, the user auditor should gain a sufficient understanding of those controls to assess risk and plan the audit. Such controls include (1) user controls and (2) other controls implemented by the user entity to monitor the effectiveness of the design and operation of controls related to the information processed by the service organization. Such monitoring controls could include:

- contractual security requirements,
- service level agreements,

- receipt and analysis of service organization reports,
- additional testing requested of the service auditor or performed by the user entity, and
- other user entity controls

If the service organization's controls are significant to the user organization's internal control and within the context of the audit objectives, inadequate monitoring controls prevent entity management from having reasonable assurance that controls over the information processed and/or maintained by the service organization are designed and operating effectively.

Sources of information include analysis of user controls implemented by the user entity and interviews of appropriate entity personnel. Also, the auditor may review any service auditor reports. The service organization may hire an independent auditor (referred to as the service auditor) to provide a report (referred to as the SAS 70 report[119]) on the internal controls at the service provider. Each user organization and its auditor may use this report to assess the internal control policies and procedures at the service organization as part of the overall evaluation of the internal control at the user organization. If additional information about service bureau controls is still needed, the auditor may contact the service organization, through the user entity, for additional information.

The user auditor should obtain a sufficient understanding of internal control to evaluate the effectiveness of the design of controls relevant to the audit objectives and determine whether they have been implemented. In some instances, the user entity may have effective controls over the service organization. In such cases, evidence about the operating effectiveness of internal control can be obtained from the user entity. However, in other cases, the controls are applied only at the service organization.

[119]The Auditing Standards Board of the American Institute of Certified Public Accountants is currently deliberating on possible changes to SAS 70 requirements. Users of the FISCAM should determine whether such changes have been made before applying this Appendix.

For internal control that is significant within the context of the audit objectives, auditors should assess whether internal control has been properly designed and implemented. Based on the user auditor's understanding of the design effectiveness and implementation of internal control, the auditor should assess risks relevant to the audit objectives. In a financial statement audit, the auditor should identify and assess the risk of material misstatement at the financial statement level and at the relevant assertion level related to classes of transactions, account balances, and disclosures.

In a performance audit, for those internal controls that are deemed significant within the context of the audit objectives, auditors should plan to obtain sufficient, appropriate evidence to support their assessment about the operating effectiveness of those controls, including tests of such controls. In a financial audit, the auditor should perform tests of the operating effectiveness of controls when the auditor's risk assessment includes an expectation of the operating effectiveness of controls or when substantive procedures alone do not provide sufficient appropriate audit evidence at the relevant assertion level. For federal financial audits, OMB requires auditors of federal financial statements to test those controls that are effectively designed.

To obtain sufficient, appropriate evidence about the operating effectiveness of service organization controls, the auditor may determine that it is appropriate to use a service auditor's report. In such instances, the auditor should determine whether the service auditor's report is sufficient to meet the audit objectives. For financial audits, the auditor's considerations are discussed at AU 543 (Part of Audit Performed by Other Independent Auditors). In some instances, the user auditor may determine that it is necessary and appropriate to supplement the service auditor report by discussing it with the service auditor, by requesting the service auditor to perform agreed-upon procedures, or by performing procedures at the service organization. In addition, in some instances, the user auditor may request the service auditor to perform tests of data maintained by the service organizations. Any such requests of the service auditor should be coordinated through the user and service organizations.

A service auditor may provide a service organization with one of two types of SAS 70 reports:

- Type 1 is a report on the design and implementation of controls (placed in operation) at a service organization, but does not include testing of the operating effectiveness of controls. This information, in conjunction with other information about a user organization's internal control, may assist the user auditor in obtaining an understanding of the user organization's internal control. A type 1 report is not intended to provide a basis for the auditor to reduce the assessment of risk, because it does not include control testing to determine whether the controls are operating effectively.

- Type 2 is a report on the design and implementation of controls (placed in operation) *and* on their operating effectiveness. In a type 2 engagement, the service auditor performs the procedures required for a type 1 engagement and also performs tests of specific controls to evaluate their operating effectiveness in achieving the specified control objectives. The service auditor issues a report that includes the type 1 report opinions and refers the reader to a description of tests of operative effectiveness performed by a service auditor. The report states whether, in the opinion of the service auditor, the controls tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the related control objectives were achieved during the period specified. If a service organization's controls that affect a user organization's financial statements are operating with sufficient effectiveness to achieve the related control objectives, a user auditor may be able to use the type 2 report as evidence of control effectiveness, reduce their assessment of risk for certain financial statement assertions affected by the service organization's service, and reduce the extent of substantive procedures performed for those assertions.

The nature, timing, and extent of the tests of operating effectiveness are also affected by the period covered by the report. Tests of operating effectiveness may provide evidence that will enable the service auditor to report on the entire period covered by the report. To be useful to user auditors, the report ordinarily should cover the

reporting period of the user organization. However, for the SAS 70 report to be received in time for the completion of the user entity audit, SAS 70 reports may need to be requested for periods prior to the end of the federal fiscal year. If it does not cover the entire reporting period, the user auditor should evaluate the related effect on the user auditor's risk assessment and, for the period not covered by the service auditor report(s), should evaluate the adequacy of evidence about the operating effectiveness of controls.

The service organization is responsible for identifying the internal controls that may be relevant to a user organization's internal control (description of controls). The service auditor is responsible for determining whether the description provides sufficient information for user auditors to obtain an understanding of those aspects of the service organization's controls that would have an effect on the user organization's internal control. Also, the service auditor may identify certain controls that the service organization assumes would be implemented by the user organization.

In OMB Circular A-123, Appendix A, OMB stated that an agency can leverage SAS 70 reports during the assessment. Management should determine if a Type II SAS 70 report exists and consider whether it is sufficient in scope. Entity management should look at the scope of the SAS 70 report in the context of the overall internal control assessment when considering the nature and type of other assessment activities needed outside of the SAS 70 process. OMB Bulletin 07-04, as revised, *Audit Requirements for Federal Financial Statements*, para. 6-16-18 states that service organizations *must* either provide its user organizations with an audit report on whether (1) internal controls were designed properly to achieve specified objectives and placed into operation as of a specified date and (2) the controls that were tested were operating effectively to provide reasonable assurance that the related control objectives were met during the period specified or allow user auditors to perform appropriate tests of controls at the service organization. If the service organization uses another service organization (subservicer), the service organization is responsible for requesting or obtaining appropriate audit coverage. Such audit reports should be submitted to user organizations within a reasonable time *but no later than September 30* to allow the auditor of the user

organization to use the audit report during the audit of the user organization's financial statements.[120]

In addition, the "Implementation Guide for OMB Circular A-123, Management's Responsibility for Internal Control Appendix A, Internal Control over Financial Reporting," issued by the Chief Financial Officer's Council (July 2005) provides guidance for considering service organization controls as part of the annual A-123 assessment.

FISMA applies to both (1) information collected or maintained by or on behalf of an agency and (2) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. As discussed in OMB Memoranda, as part of FISMA, agency management is responsible for ensuring that contractors (and others covered by FISMA) meet FISMA requirements, including annual testing. SAS 70 reports may provide sufficient evidence of contractor compliance. However, it may not address all of the FISMA control objectives and it may not ensure the specific systems that support the government or contract activity are actually reviewed.

Therefore, in determining whether SAS 70 reports provide sufficient evidence of contractor system FISMA compliance, it is the entity's responsibility to ensure:

- The scope of the SAS 70 audit was sufficient, and fully addressed the specific contractor system requiring FISMA review.
- The audit encompassed all controls and requirements of law, OMB policy and NIST guidance.

In addition, NIST SP 800-47 discusses additional steps entity management should implement with respect to contractors, such as an Interconnection Security Agreement (ISA) and a Memorandum of Understanding (MOU). The ISA specifies the technical and security

[120]Supersedes requirements in OMB Memorandum M-04-11, *Service Organization Audits*.

requirements of the interconnection, and the MOU defines the responsibilities of the participating organizations.

SAS 70 reports do not include contingency planning controls, as auditing standards (AU 324) do not apply to internal control deficiencies that affect processing in future periods. However, service auditors can be requested to perform procedures to test the effectiveness of contingency planning controls and report the results of such testing to service organization management, who may in turn disclose the information and plans to correct deficiencies in the section of the SAS 70 report titled "Other Information Provided by the Service Organization."

The FISCAM can be used as a basis for performing a SAS 70 audit, using the control objectives discussed in Chapter 1.

Appendix VIII - Application of FISCAM to Single Audits[121]

The FISCAM can be used to assess information system controls over compliance requirements and financial reporting in connection with a Single Audit. The following provides a brief introduction to Single Audit requirements and how the FISCAM relates to such requirements. See the Single Audit Act, as amended, OMB Circular A-133, the Compliance Supplement, and the AICPA Audit Guide: Government Auditing Standards and Circular A-133 Audits for additional information.

Single Audits include opinions on the entity's financial statements, the schedule of expenditures of federal awards, and the entity's compliance with laws, regulations, and the provisions of contracts or grant agreements pertaining to federal awards that may have a direct and material effect on each of its major programs (referred to as compliance requirements). Government Auditing Standards ("yellow book") require certain audit procedures relating to internal controls over financial reporting in relation to the audit of the financial statements and the schedule of expenditures. In addition, auditors performing a Single Audit should obtain evidence about the effectiveness of internal control over the compliance requirements of major Federal programs.

In assessing internal control over compliance requirements and financial reporting, the auditor should evaluate whether the each of the specific control techniques that are significant to compliance

[121]The Single Audit is intended to provide a cost-effective audit for nonfederal entities in that one audit is conducted in lieu of multiple audits of individual programs. Such audits are performed in accordance with the Single Audit Act Amendments of 1996 and OMB Circular A-133 (*Audits of States, Local Governments, and Non-Profit Organizations*) to determine whether federal funds to nonfederal entities are expended properly.

and financial reporting is an information systems (IS) control. An IS controls specialist generally should review and concur with the audit team's identification of IS controls, particularly with respect to whether all IS controls were properly identified as such.

As discussed in Chapter 1, IS controls consist of those internal controls that are dependent on information systems processing and include general controls (entitywide, system, and business process application levels), business process application controls (input, processing, output, master file, interface, and data management system controls), and user controls[122] (controls performed by people interacting with information systems). General and business process application controls are always IS controls. A user control is an IS control if its effectiveness depends on information systems processing or the reliability (accuracy, completeness, and validity) of information processed by information systems. Conversely, a user control is not an IS control if its effectiveness does not depend on information systems processing or the reliability of information processed by information systems.

The FISCAM can be used to determine whether IS controls are (1) appropriately designed and implemented (placed in operation), and (2) operating effectively.

As discussed in Chapter 2, the auditor should identify and document the other entitywide, system, and business process level IS controls upon which the effectiveness of each significant IS control technique depends. These other IS controls will principally relate to the entitywide level controls and to each of the critical control points (including control dependencies) at the system and business process application levels. For example, if the IS control is the review of an exception report, the auditor should identify and test the business process application controls directly related to the production of the exception report, as well as the general and other business process application controls upon which the reliability of the information in the exception report depends, including the

[122]User controls are portions of controls that are performed by people interacting with IS controls. The effectiveness of user controls typically depend on information systems processing or the reliability of information processed.

proper functioning of the business process application that generated the exception report and the reliability of the data used to generate the exception report. In addition, the auditor should test the effectiveness of the user control (i.e., management review and followup on the items in the exception report).

The following sections address the audit procedures that should be applied in a Single Audit with respect to controls over (1) compliance requirements and (2) financial reporting.

Internal Control over Compliance Requirements

To evaluate internal control over compliance requirements for major programs, the auditor should:

- plan the audit and testing of internal control to support a low assessed level of control risk for the assertions relevant to the compliance requirements for each major program, and
- unless internal controls are ineffective in design, perform testing of the operating effectiveness of internal controls as planned to support a low assessed level of control risk for the assertions relevant to the compliance requirements for each major program.

When internal control over compliance requirements for a major program is ineffective in preventing or detecting noncompliance (either in design or operation), the auditor should report a significant deficiency (including whether any such condition is a material weakness), assess the related control risk at the maximum, and determine whether to apply further audit procedures to test compliance based on ineffective internal control.

In planning and performing a Single Audit, the auditor should:

- Identify the major programs subject to the Single Audit.
- Identify systems that process data for major programs.
- Determine the types of compliance requirements that are relevant to the audit (see A-133 and the *Compliance Supplement*).

- For each relevant type of compliance requirement, determine/identify the relevant control objectives (see the Compliance Supplement).
- For each relevant control objective, identify the internal control technique(s) designed/implemented by the entity to achieve the objective.
- Determine whether such control techniques are effectively designed to achieve the related control objective(s) and if so, whether they are placed in operation (implemented), including related IS controls upon which the effectiveness of the control technique depends. The auditor can use the FISCAM to assess the effectiveness of the design of IS control techniques and whether they have been implemented (placed in operation).
- For each control that is effectively designed and implemented (placed in operation), the auditor should determine whether it is effectively operating. The auditor can use the FISCAM to determine whether IS controls are effectively operating. As discussed in Chapter 2, for each IS control technique, the auditor should test the effectiveness of:
  - the specific IS control technique, and
  - the business process application and general controls upon which the effectiveness of specific IS control depends.

When the auditor assesses control risk below the maximum level, the auditor should obtain sufficient evidential matter to support that assessed level of control risk. The type of evidential matter, its source, its timeliness, and the existence of other evidential matter related to the conclusions to which it leads all bear on the degree of assurance the evidential matter provides.

Based on the tests of controls, the auditor should draw conclusions on the assessed level of control risk. The auditor should also consider the impact on the assessment of internal controls of any exceptions noted as part of the audit procedures applied to test conformance with compliance requirements. The assessment of the effectiveness of internal control over compliance in preventing or detecting noncompliance is determined in relation to each individual type of compliance requirement for each major program

or to an audit objective identified in the Compliance Supplement (e.g., controls over requirements for eligibility).

The auditor should determine whether any deficiencies in IS controls represent material weaknesses or significant deficiencies. The following definitions are provided in the draft reports on A-133 provided by the AICPA[123]:

- A *control deficiency* in an entity's internal control over compliance exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect noncompliance with a type of compliance requirement of a federal program on a timely basis.
- A *significant deficiency* is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to administer a federal program such that there is more than a remote likelihood that noncompliance with a type of compliance requirement of a federal program that is more than inconsequential will not be prevented or detected by the entity's internal control.
- A *material weakness* is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that material noncompliance with a type of compliance requirement of a federal program will not be prevented or detected by the entity's internal control.

[123]The definitions currently in Circular A-133, based on superseded GAGAS, are as follows: Reportable conditions involve matters coming to the auditor's attention relating to significant deficiencies in the design or operation of the internal control over compliance that, in the auditor's judgment, could adversely affect the entity's ability to administer a major federal program in accordance with the applicable requirements of laws, regulations, contracts, and grants. A material weakness is a reportable condition in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that noncompliance with the applicable requirements of laws, regulations, contracts, and grants caused by error or fraud that would be material in relation to a major federal program being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions.

The objectives of internal control pertaining to the compliance requirements for Federal programs are as follows:

(1) Transactions are properly recorded and accounted for to:

(i) Permit the preparation of reliable financial statements and Federal reports;
(ii) Maintain accountability over assets; and
(iii) Demonstrate compliance with laws, regulations, and other compliance requirements;

(2) Transactions are executed in compliance with:

(i) Laws, regulations, and the provisions of contracts or grant agreements that could have a direct and material effect on a Federal program; and
(ii) Any other laws and regulations that are identified in the compliance supplements; and

(3) Funds, property, and other assets are safeguarded against loss from unauthorized use or disposition.

Part 6 of the *Compliance Supplement* is designed to assist non-Federal entities and their auditors in complying with these requirements by describing, for each type of compliance requirement, the objectives of internal control, and certain characteristics of internal control that, when present and operating effectively, may ensure compliance with program requirements. Part 6 cautions that the categorizations used in the Supplement may not necessarily reflect how an entity considers and implements internal control. Also, Part 6 was not designed as a checklist of required internal control characteristics. Non-Federal entities could have adequate internal control even though some or all of the characteristics included in Part 6 are not present. Further, non-Federal entities could have other appropriate internal controls operating effectively that have not been included in Part 6. Non-Federal entities and their auditors should exercise judgment in determining the most appropriate and cost effective internal control in a given environment or circumstance to provide reasonable assurance for compliance with Federal program requirements.

The characteristics of internal control in Part 6 of the *Compliance Supplement* are presented in the context of the components of

internal control discussed in *Internal Control-Integrated Framework* (COSO Report), published by the Committee of Sponsoring Organizations of the Treadway Commission. These components are consistent with the *Standards for Internal Control in the Federal Government* (Green Book).[124] Part 6 describes characteristics of internal control relating to each of the five components of internal control that should reasonably assure compliance with the requirements of Federal laws, regulations, and program compliance requirements.

Internal Control over Financial Reporting

In addition, the auditor should gather evidence about internal controls over financial reporting, including information system controls, as part of the financial audits of the financial statements and schedule of expenditures of federal awards. The auditor may use evidence gathered in connection with the testing of controls over compliance discussed above.

GAGAS financial audit standards require the auditor to obtain an understanding of internal control over financial reporting sufficient to assess the risk of material misstatement of the financial statements whether due to error or fraud, and to design the nature, timing, and extent of further audit procedures. This includes performing risk assessment procedures to evaluate the design of controls relevant to an audit of financial statements and to determine whether they have been implemented. In obtaining this understanding, the auditor considers how an entity's use of information technology (IT) and manual procedures affect controls relevant to the audit. The FISCAM can be used to assist the auditor in obtaining an understanding of internal controls relevant to the financial statements and schedule of expenditures of federal awards.

In addition, when the auditor has determined that it is not possible or practicable to reduce the detection risk at the relevant assertion

[124]Standards for Internal Control in the Federal Government (GAO/AIMD-00-21.3.1, November 1999)

level to an acceptably low level with audit evidence obtained only from substantive procedures, the auditor should perform tests of controls to obtain audit evidence about their operating effectiveness. For example, the auditor may find it impossible to design effective substantive procedures that by themselves provide sufficient appropriate audit evidence at the relevant assertion level when an entity conducts its business using information technology (IT) and no documentation of transactions is produced or maintained, other than through the IT system.

Specifically, as discussed in Chapter 2, for those internal controls over financial reporting that the auditor (1) has determined are suitably designed and implemented (2) plans to test whether they are operating effectively, and (3) has determined to be IS controls (as defined above), the auditor should test the effectiveness of

- the specific IS control, and
- the business process application and general controls upon which the effectiveness of specific IS control depends.

The FISCAM can be used to assess the effectiveness of the design and operation of information system controls as part of the financial audits of the financial statements and schedule of expenditures of federal awards.

Appendix IX - Application of FISCAM to FISMA

The FISCAM may be used as a basis for the independent evaluation of a federal agency's information security program required by the Federal Information Security Management Act (FISMA). FISMA requires that each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices. Independent evaluations of non-national-security systems are to be performed by the agency's Inspector General, or by an independent external auditor chosen by the IG, if any, or by the head of the agency, if there is no agency IG. Evaluations related to national security systems are to be performed only by an entity designated by the agency head.

Each evaluation shall include:

- testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems;
- an assessment (made on the basis of the results of the testing) of compliance with the requirements of FISMA and related information security policies, procedures, standards, and guidelines; and
- separate presentations, as appropriate, regarding information security relating to national security systems.

Although FISMA does not require that these evaluations be performed in accordance with GAGAS, or use the FISCAM, agency Inspectors General and independent external auditors may use FISCAM as the basis for FISMA evaluations performed under GAGAS. Also, this guidance may be used to perform FISMA evaluations that are not performed as GAGAS audits.

The FISCAM was designed as a risk-based methodology to assess the effectiveness of an entity's information system controls. It can also be used to provide a reasonable basis for determining whether information security is effective, and identifying information

security strengths and weaknesses as a basis for that determination. The FISCAM control activities are consistent with NIST guidance in NIST SP 800-53 (see Appendix IV). All controls in NIST SP 800-53 have been mapped to FISCAM.

The following selected topics, which supplement the methodology (including the planning, testing, and reporting phases) and controls discussed in Chapters 1-4, may provide useful supplemental guidance to assist the auditor in applying the FISCAM to meet the evaluation (testing and assessment) requirements of FISMA:

- selecting a representative subset of systems;
- independence requirements; and
- reporting.

Selecting a representative subset of systems

The concept of a representative subset of systems was intended to provide the evaluator (the party performing the independent evaluation) with a reasonable basis for their evaluation. The evaluator uses professional judgment to identify a sufficient scope of systems testing to constitute a representative subset of the entity's systems with the expectation that it would be representative of all of the entity's systems covered by FISMA, in all significant respects. The evaluator may supplement systems tested for other purposes (e.g., financial audits) with additional systems necessary to obtain a representative subset. Alternatively, the evaluator also may select a representative subset of systems for purposes of the FISMA evaluation and supplement it with additional systems necessary to perform the financial audit or other audits.

Factors that the evaluator may consider in determining a representative subset of agency systems include:

- systems at different risk levels (high, moderate, and low)
- both general support systems and major application systems
- different types of applications (e.g., financial management, operations) operated by the agency
- major processing locations

- general and business process controls
- coverage of the FISCAM control areas
- contractor and other non-entity systems that are covered by FISMA requirements.

In determining the specific systems to be tested in the current evaluation period, the evaluator may consider implementing a multi-year testing strategy (as discussed FISCAM Section 2.1.9.E) or may consider recent testing performed as part of a multi-year testing strategy. Also, evidence of continuing material weaknesses or significant deficiencies may reduce the extent of testing necessary to reasonably conclude that information security is ineffective; however, the evaluator may consider the benefits of testing to identify additional weaknesses that the agency can begin to address.

Independence requirements

FISMA requires that an independent evaluation be performed. This means that the auditor should be independent of the entity in fact and in appearance. In addition, if the auditor would like to use the work of other parties as a basis for the auditor's evaluation, the auditor should consider the independence and objectivity of the persons performing the testing on behalf of the agency. If such other parties are considered independent, the auditor may determine that the work of the other parties can be used as support for the evaluation without retesting. The less independent or objective the other parties' work is, the less the auditor can use the work of the other party without retesting the other parties' work. If the other parties are not independent, the auditor should not use such work as a substitute for their own testing. Although GAGAS is not required to be applied in the FISMA evaluation, such standards provide guidance on considering independence that is consistent with other discussions of independence in professional literature. Also, the auditor may elect to perform the FISMA evaluation using GAGAS. GAGAS independence requirements are discussed in GAGAS 3.20-3.30.

Reporting

The Reporting phase discussed in Chapter 2 describes how to evaluate the results of the tests of controls and conclude as to their effectiveness. As part of evaluating the results of the testing for audits used to as a basis for the FISMA evaluations, the evaluator should determine whether any weaknesses identified, individually or collectively, represent FISMA significant deficiencies as that term is used in FISMA (see "Related Reporting Responsibilities" in Chapter 2 for further information.) FISMA requires agencies to report any significant deficiencies (FISMA significant deficiencies) (1) as material weaknesses under FMFIA, and 2) as instances of a lack of substantial compliance under FFMIA, if related to financial management systems.

OMB defines a FISMA significant deficiency as "a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems which significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken."

As part of evaluating the effectiveness of information security controls, the evaluator may perform audit procedures to determine whether information used in management reports or used to support FISMA reporting to OMB is consistent with the results of the testing they performed. More specifically, for each system tested, the evaluator may compare the results of testing with related information included in management and FISMA reports. For example, the evaluator may compare evidence obtained about the effectiveness of a system's certification and accreditation with information included in management and FISMA reports to determine whether such reporting was accurate (e.g., whether a certification and accreditation was effectively completed). If, in this circumstance, a certification and accreditation was completed and was reported as such in management and FISMA reports, but the evaluator's testing revealed that it was not properly performed, the

evaluator should consider this deficiency in management's controls over monitoring in their evaluation of the results of testing and determine whether there are systemic reasons for the deficiency.

For additional guidance on performing FISMA evaluations, refer to the PCIE FISMA Framework.

Appendix X - Information System Controls Audit Documentation

This appendix summarizes the audit documentation that should be prepared by the auditor in connection with the IS controls audit, as discussed in Chapter 2.

Planning Phase

The auditor should document the following information developed in the planning phase:

- Objectives of the IS controls audit and, if it is part of a broader audit, a description of how such objectives support the overall audit objectives.
- The scope of the IS controls audit.
- The auditor's understanding of the entity's operations and key business processes, including, to the extent relevant to the audit objectives, the following:
  - The significance and nature of the programs and functions supported by information systems;
  - Key business processes relevant to the audit objectives, including business rules, transaction flows, and application and software module interaction;
  - Significant general support systems and major applications that support each key process;
  - Background information request, if used;
  - Significant internal and external factors that could affect the IS controls audit objectives;
  - Detailed organization chart, particularly the IT and the IS components;
  - Significant changes in the IT environment/architecture or significant applications implemented within the past 2 years or planned within the next 2 years; and

- The entity's reliance on third parties to provide IT services (e.g., in-house, remote connectivity, remote processing).

- A general understanding of the structure of the entity's or component's networks as a basis for planning the IS controls audit, including high-level and detailed network schematics relevant to the audit objectives.
- Key areas of audit interest, including relevant general support systems and major applications and files. This includes (1) the operational locations of each key system or file, (2) significant components of the associated hardware and software (e.g., firewalls, routers, hosts, operating systems), (3) other significant systems or system-level resources that support the key areas of audit interest, and (4) prior audit problems reported. Also, the auditor should document all access paths in and out of the key areas of audit interest.
- Factors that significantly increase or decrease IS risk and their potential impact on the effectiveness of information system controls. For each risk identified, the auditor should document the nature and extent of the risk; the conditions that gave rise to that risk; and the specific information or operations affected (if not pervasive).
- Preliminary assessment of IS risks related to the key areas of audit interest and the basis for the assessed risk. For each risk identified, the auditor should document the nature and extent of the risk; the conditions that gave rise to that risk; and the specific information or operations affected (if not pervasive). The auditor should also document other considerations that may mitigate the effects of identified risks.
- Critical control points.
- A preliminary understanding of the entity's IS controls, including the organization, staffing, responsibilities, authorities, and resources of the entity's security management function. The auditor should include the following information in the documentation of their preliminary understanding of the design of IS controls, to the extent relevant to the audit objectives:
  - Identification of entitywide level controls (and appropriate system level controls) designed to achieve the control activities for each critical element within each general control area and a determination of whether they are designed effectively and

implemented (placed in operation), including identification of control activities for which there are no or ineffective controls at the entitywide level and the related risks;

- Identification of business process level controls for key applications identified as key areas of audit interest, determination of where those controls are implemented (placed in operation) within the entity's systems, and the auditor's conclusion about whether the controls are designed effectively, including identification of control activities for which there are no or ineffective controls and the related risks and the potential impact of any identified design weaknesses on the completeness, accuracy, validity, and confidentiality of application data;
- Any internal or third-party information systems reviews, audits, or specialized systems testing (e.g., penetration tests, disaster recovery tests, and application-specific tests) performed during the last year;
- Management's plans of action and milestones, or their equivalent, that identify corrective actions planned to address known IS control weaknesses;
- Status of the prior years' audit findings;
- Documentation for any significant computer security related incidents identified and reported for the last year;
- Documented security plans;
- Documented risk assessments for relevant systems (e.g., general support systems and major applications);
- System certification and accreditation documentation or equivalent for relevant systems;
- Documented business continuity of operations plans and disaster recovery plans; and
- A description of the entity's use of third-party IT services

- Relevant laws and regulations and their relation to the audit objectives, including documentation of any consultation with legal counsel.
- Description of the auditor's procedures to consider the risk of fraud, any fraud risk factors that the auditor believes could affect the audit objectives, and planned audit procedures to detect any fraud significant to the audit objectives.
- Audit resources planned.

- Current multiyear testing plans.
- Documentation of communications with entity management.
- If IS controls are performed by service organizations, conclusions whether such controls are significant to the audit objectives and any audit procedures performed with respect to such controls (e.g., review of service auditor reports)
- If the auditor plans to use the work of others, conclusions concerning the planned use of the work of others and any audit procedures performed with respect to using the work of others.
- Audit plan that adequately describes the objectives, scope, and methodology of the audit.
- Any decision to reduce testing of IS controls due to the identification of significant IS control weaknesses.

Testing Phase

The auditor should document the following information developed in the testing phase:

- An understanding of the information systems that are relevant to the audit objectives
- IS control objectives and activities relevant to the audit objectives.
- By level (e.g., entitywide, system, business process application) and system sublevel (e.g., network, operating system, infrastructure applications), a description of control techniques used by the entity to achieve the relevant control activities.
- By level and sublevel, specific tests performed, including:
  - related documentation that describes the nature, timing, and extent of the tests;
  - evidence of the effective operation of the control techniques or lack thereof (e.g., memos describing procedures and results, output of tools and related analysis);
  - if a control activity is not achieved, any compensating controls or other factors and the basis for determining whether they are effective;

- the auditor's conclusions about the effectiveness of the entity's IS controls in achieving the control activity; and
- for each weakness, whether the weakness is a material weakness, significant deficiency, or just a deficiency, as well as the criteria, condition, cause, and effect if necessary to achieve the audit objectives.

Reporting Phase

The auditor should document the following information developed in the reporting phase:

- The auditor's conclusion about the effectiveness of IS controls (in relation to the IS controls audit objectives) in achieving the control categories, critical elements, and the relevant control activities and the basis for the conclusion, including the factors that the auditor considered in making the determination.
- If part of a broader audit, the impact of any identified IS control weaknesses on the overall audit objectives.
- Copies of any reports or written communications issued in connection with the audit, including entity management comments related to such reports and communications.
- For financial audits and attestation engagements, the auditor's determination of whether identified weaknesses represent material weaknesses or significant deficiencies, and the basis for the auditor's conclusions.
- Other documentation required by the audit organization's policies and procedures, including quality assurance processes.
- Results of procedures to detect any fraud significant to the audit objectives and the impact on the audit.
- Results of audit follow-up procedures to determine whether agency corrective actions have been implemented, based on risk and a cost benefit analysis, to sufficiently remediate previously reported IS control weaknesses.
- As appropriate, the auditor's considerations and determinations concerning FMFIA, FFMIA, and other reporting responsibilities.

Appendix XI - Glossary

The definitions in this glossary are drawn from various sources, including this manual and the materials in the bibliography. In addition, certain definitions were developed by project staff and contractors.

Acceptance testing	Final testing by users to decide whether to accept a new system.
Access control	The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).
Access control list (ACL)	A register of: 1) users (including groups, machines, and processes) who have been given permission to use a particular system resource, and 2) the types of access they have been permitted.
Access control software	(CA-ACF2, RACF, CA-TOP SECRET) This type of software, which is external to the operating system, provides a means of specifying who has access to a system, which has access to specific resources, and what capabilities authorized users are granted. Access control software can generally be implemented in different modes that provide varying degrees of protection such as denying access for which the user is not expressly authorized, allowing access which is not expressly authorized but providing a warning, or allowing access to all resources without warning regardless of authority.
Access method	The technique used for selecting records in a file for processing, retrieval, or storage.
Access path	Sequence of hardware and software components significant to access control. Any component capable of enforcing access restrictions or any component that could be used to bypass an access restriction should be considered part of the access path. The access path can also be defined as the path through which a user request travels, including the telecommunications software, transaction processing software, application program, etc.
Access path diagram	Network schematic that identifies the users of the system, the type of device from which they can access the system, the software used to access the system, the resource they may access, the system on which these resources reside, and the modes of operation and telecommunication paths.

Access privileges	Precise statements that define the extent to which an individual can access computer systems and use or modify the programs and data on a system, and under what circumstances this access will be allowed.
Access rights	Also called permissions or privileges, these are the rights granted to users by the administrator or supervisor. Access rights determine the actions users can perform (e.g., read, write, execute, create and delete) on files in shared volumes or file shares on the server.
Accountability	The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
Account Management	Involves (1) the process of requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions.
Accreditation	The official management decision given by a senior agency/entity official to authorize operation of an information system and to explicitly accept the risk to agency/entity operations (including mission, functions, image, or reputation), agency/entity assets, or individuals, based on the implementation of an agreed-upon set of security controls.
Accreditation boundary	All components of an information system to be accredited by an authorizing official and excludes separately accredited systems, to which the information system is connected.
Accuracy	See Accuracy Control.
Accuracy control	Controls that are designed to provide reasonable assurance that transactions are properly recorded, with correct amount/data, and on a timely basis (in the proper period); key data elements input for transactions are accurate; data elements are processed accurately by applications that produce reliable results; and output is accurate.
Adequate security	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.
Advanced Encryption Standard (AES)	The Advanced Encryption Standard specifies a U.S. Government-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.
Alternate work site	Entity authorized work at home or at geographically convenient satellite offices (e.g., telecommuting).

Application controls	Application controls, sometimes referred to as business controls, are incorporated directly into computer applications to help ensure the validity, completeness, accuracy, and confidentiality of data during application processing and reporting.
Application level general controls	Controls consist of general controls operating at the business process application level, including those related to security management, access controls, configuration management, segregation of duties, and contingency planning.
Application System	The use of information resources to satisfy a specific set of user requirements. Performs a certain type of work, including specific functions such as payroll, inventory control, accounting, and mission support. Depending on the work for which it was designed, an application system can manipulate text, numbers, graphics, or a combination of these elements.
Application programmer	A person who develops and maintains application programs, as opposed to system programmers who develop and maintain the operating system and system utilities.
Application programs	See application system.
Assertion	Financial statement assertions are management representations that are embodied in financial statement components. The assertions can be either explicit or implicit and can be classified into the following broad categories: existence or occurrence (an entity's assets or liabilities exist at a given date and recorded transactions have occurred during a given period; completeness (all transactions and accounts that should be presented in the financial statements are included; rights and obligations (assets are the rights of the entity and liabilities are the obligations of the entity at a given date; valuation or allocation (asset, liability, revenue, and expense components have been included in the financial statements at appropriate amounts; and presentation and disclosure (the particular components of the financial statements are properly classified, described, and disclosed).
Attack	Attempt to gain unauthorized access to an information system's services, resources, or information, or the attempt to compromise an information system's integrity, availability, or confidentiality.
Audit logging	Recording of user activity in a system or application initiated by the user (e.g., access to a file, record, or field, use of modem). Further, it may record any attempts to log on (successful or unsuccessful) to a system and record log on ID, date and time of each log on.

Audit plan	A high level description of the audit work to be performed in a certain period of time (ordinarily a year). It includes the areas to be audited, the type of work planned, the high level objectives and scope of the work, and topics such as budget, resource allocation, schedule dates, type of report and its intended audience and other general aspects of the work.
Auditable event	A system activity identified by the entity's audit monitoring system that may be indicative of a violation of security policy. The activity may range from simple browsing to attempts to plant a Trojan horse or gain unauthorized access privilege.
Audit risk	For financial statement audits, the risk that the auditor may unknowingly fail to appropriately modify the audit opinion on financial statements that are materially misstated. In a performance audit, the risk that the auditor's findings, conclusions, recommendations, or assurance may be improper or incomplete.
Audit strategy	Plan for assessing organizational activities based on an understanding of the entity's business processes and related risk assessments.
Audit trail	A record showing who has accessed an Information Technology (IT) system and what operations the user has performed during a given period.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authenticity	The property of being genuine and being able to be verifies and trusted; confidence in the validity of a transmission, a message, or message originator. See authentication.
Authorization	The official management decision given by a senior agency/entity official to authorize operation of an information system and to explicitly accept the risk to agency/entity operations (including mission, functions, image, or reputation), agency/entity assets, or individuals, based on the implementation of an agreed-upon set of security controls.
Authorizing official	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency/entity operations (including mission, functions, image, or reputation), agency/entity assets, or individuals.
Availability	Ensuring timely and reliable access to and use of information.
Backdoor	An undocumented way to gain access to a program, data, or an entire computer system, often known only to the programmer who created it. Backdoors can be handy when the standard way of getting information is unavailable, but they usually constitute a security risk.

Backup	Any duplicate of a primary resource function, such as a copy of a computer program or data file. This standby is used in case of loss or failure of the primary resource.
Backup procedures	A regular maintenance procedure that copies all new or altered files to a backup storage medium, such as a tape drive.
Baseline configuration	Current inventory of all entity hardware, software, and firmware plus approved changes from the baseline.
Biometric	A physical or behavioral characteristic of a human being.
Boundary	Software, hardware, or physical barrier that limits access to a system or part of a system.
Boundary Protection	Monitoring and control of communications at the external boundary between information systems completely under the management and control of the organization, and at key internal boundaries between information systems completely under the management and control of the organization, to prevent and detect malicious and other unauthorized communication, employing controlled interfaces (e.g., proxies, gateways, routers, firewalls, encrypted tunnels).
Browsing	The act of electronically perusing files and records without authorization.
Business Impact Analysis (BIA)	An analysis of an information technology (IT) system's requirements, processes, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.
Business process	Processes that are the primary functions that the entity performs in accomplishing its mission. Examples include, financial management processes, such as collections, disbursements, or payroll; and mission-related processes, typically at the program or subprogram level, such as education, public health, law enforcement, or income security.
Business process application	A computer program designed to help perform a business function such as payroll, inventory control, accounting, and mission support. Depending on the work for which it was designed, an application can manipulate text, numbers, graphics, or a combination of these elements.
Business process application controls	Controls directly related to individual computerized applications. They help ensure that transactions are complete, accurate, valid, confidential, and available. These controls include programmed control techniques, such as automated edits, and manual follow-up of computer generated reports, such as reviews of reports identifying rejected or unusual items.
Business process application level	Controls at the business process application level consist of policies, procedures for controlling specific processes. For example, the entity's configuration management should reasonably ensure that all changes to application systems are fully tested and authorized.

Business process controls (FISCAM)	These controls are the automated and /or manual controls applied to business transaction flows. They relate to the completeness, accuracy, validity and confidentiality of transactions and data during application processing.
Bypass label processing (BLP)	The technique of reading a computer file while bypassing the internal file/data set label. This process could result in bypassing security access controls.
CAAT	See computer-assisted audit technique.
CD-ROM	See compact disk-read only memory.
Central processing unit (CPU)	The computational and control unit of a computer; the device that interprets and executes instructions.
Certificate	A digital representation of information which at least 1) identifies the certification authority issuing it, 2) names or identifies its subscriber, 3) contains the subscriber's public key, 4) identifies its operational period, and 5) is digitally signed by the certification authority issuing it.
Certificate Authority (CA)	A trusted third party that serves authentication infrastructures or organizations and registers entities and issues them certificates.
Certificate Management	Process whereby certificates (as defined above) are generated, stored, protected, transferred, loaded, used, and destroyed.
Certification	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Certification and Accreditation	A comprehensive assessment of the management, operational and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision given by a senior agency/entity official to authorize operation of an information system and to explicitly accept the risk to agency/entity operations (including mission, functions, image, or reputation), agency/entity assets, or individuals, based on the implementation of an agreed-upon set of security controls.
Certification Authority	A trusted entity that issues and revokes public key certificates.

Checkpoint	The process of saving the current state of a program and its data, including intermediate results, to disk or other nonvolatile storage, so that, if interrupted, the program could be restarted at the point at which the last checkpoint occurred.
Chief Information Officer	Under the Paperwork Reduction Act, the agency official responsible for ensuring agency compliance with, and prompt, efficient, and effective implementation of, information policies and information resources management responsibilities, including information security and the management of information technology.
Cipher key lock	A lock with a key pad-like device that requires the manual entry of a predetermined code for entry.
Cipher text	Data output from the Cipher or input to the Inverse Cipher. Data in its encrypted form.
Code	Instructions written in a computer programming language. (See object code and source code.)
Cold site	An IS backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternative site.
Collaborative computing	Applications and technology (e.g., white boarding, group conferencing) that allow two or more individuals to share information real time in an inter- or intra-enterprise environment.
Command	A job control statement or a message, sent to the computer system, that initiates a processing task.
Compact disc-read only memory (CD-ROM)	Compact Disc (CD)-Read Only Memory (ROM) is a form of optical, rather than magnetic, storage. CD-ROM devices are generally read only.
Compensating control	An internal control that reduces the risk of an existing or potential control weakness that could result in errors or omissions.
Compiler	A program that reads the statements in a human-readable programming language and translates them into a machine-readable executable program.
Completeness control	Controls that ensure entity management that all transactions that occurred are entered into the system, accepted for processing, and processed once and only once by the system and are properly included in output.
Component	A single resource with defined characteristics, such as a terminal or printer. These components are also defined by their relationship to other components.
Computer-assisted audit technique (CAAT)	Any automated audit technique, such as generalized audit software, test data generators, computerized audit programs, and special audit utilities.
Computer facility	A site or location with computer hardware where information processing is performed or where data from such sites are stored.

Computer operations	The function responsible for operating the computer and peripheral equipment, including providing the tape, disk, or paper resources as requested by the application systems.
Computer processing location	See computer facility.
Computer resource	See resource.
Computer room	Room within a facility that houses computers and/or telecommunication devices.
Computer security	Computer security, as defined by Appendix III to OMB Circular A-130, involves the use of management, personnel, operational, and technical controls to ensure that systems and applications operate effectively and provide confidentiality, integrity, and availability.
Computer system	A complete computer installation, including peripherals, in which all the components are designed to work with each other.
Computer-related controls	Computer-related controls help ensure the reliability, confidentiality, and availability of automated information. They include both general controls, which apply to all or a large segment of an entity's information systems, and application controls, which apply to individual applications.
Computing environment	Workstation or server (host) and its operating system, peripherals, and applications. .
Confidentiality	Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.
Confidentiality control	Controls that are designed to provide reasonable assurance that application data and reports and other output are protected against unauthorized access.
Configuration auditing	Procedures for determining alignment between the actual system and the documentation describing it, thereby ensuring that the documentation used to support decision making is complete and correct.
Configuration control	Process for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation.
Configuration control board	Evaluates and approves or disapproves proposed changes to configuration items and ensures implementation of approved changes
Configuration identification	Procedures for identifying, documenting, and assigning unique identifiers (for example, serial numbers and name) to a system's hardware and software component parts and subparts generally referred to as configuration items.
Configuration settings	Information system parameters that provide only essential capabilities and specifically prohibit or restrict the use of unnecessary functions, ports, protocols, and services.

Configuration status accounting	A procedure for documenting and reporting on the status of configuration items as a system evolves. Documentation, such as historical change lists and original designs or drawings, are generated and kept in a library, thereby allowing entities to continuously know the state of a system's configuration and be in a position to make informed decisions about changing the configuration.
Configuration management	The control and documentation of changes made to a system's hardware, software, and documentation throughout the development and operational life of the system.
Console	Traditionally, a control unit such as a terminal through which a user communicates with a computer. In the mainframe environment, a console is the operator's station.
Contingency plan	Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failure, or disaster.
Contingency planning	See contingency plan.
Continuity of Operations Plan (COOP)	A predetermined set of instructions or procedures that describe how an organization's essential functions will be sustained for up to 30 days as a result of a disaster event before returning to normal operations.
Control activities	Descriptions of individual control requirements for each critical control element (e.g., implement effective authorization controls, adequately protect sensitive system resources).
Control categories	Groupings of related controls pertaining to similar types of risk. Control categories include security management, access controls, configuration management, segregation of duties, and contingency planning.
Control deficiency - financial audit	In financial audits, a control deficiency in an entity's internal control over financial reporting exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.
Control deficiency - Single Audit	In Single Audits, a control deficiency in an entity's internal control over compliance exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect noncompliance with a type of compliance requirement of a federal program on a timely manner.
Control dependency	Exists when the effectiveness of an internal control is dependent on the effectiveness of other internal controls.

Control environment	The control environment is an important component of an entity's internal control structure. It sets the "tone at the top" and can influence the effectiveness of specific control techniques. Factors that influence the control environment include management's philosophy and operating style, the entity's organizational structure, methods of assigning authority and responsibility, management's control methods for monitoring and following up on performance, the effectiveness of the Inspector General's and internal audits, personnel policies and practices, and influences external to the entity.
Control objectives	The intent of the specific control to effectively secure specific general support or business activities.
Control risk	In a financial statement audit, the risk that a material misstatement that could occur in an assertion will not be prevented, or detected and corrected on a timely basis by the entity's internal control structure.
Control techniques	The specific control implemented by the entity to secure a specific general support system or business process activity.
Controlled Interface	Mechanism that facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system).
Countermeasures	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.
CPU	See central processing unit.
Critical control point	System control points that, if compromised, could allow an individual to gain unauthorized access to or perform unauthorized or inappropriate activities on entity systems or data, which could lead directly or indirectly to unauthorized access or modifications to the key areas of audit interest.
Cryptography	The science of coding messages so they cannot be read by any person other than the intended recipient. Ordinary text—or plain text—and other data are transformed into coded form by encryption and translated back to plain text or data by decryption.
Data	Facts and information that can be communicated and manipulated.
Data access method	See access method.
Data administration	The function that plans for and administers the data used throughout the entity. This function is concerned with identifying, cataloging, controlling, and coordinating the information needs of the entity.

Database	A collection of related information about a subject organized in a useful manner that provides a base or foundation for procedures, such as retrieving information, drawing conclusions, or making decisions. Any collection of information that serves these purposes qualifies as a database, even if the information is not stored on a computer.
Database administrator (DBA)	The individual responsible for both the design of the database, including the structure and contents, and the access capabilities of application programs and users to the database. Additional responsibilities include operation, performance, integrity, and security of the database.
Database management	Tasks related to creating, maintaining, organizing, and retrieving information from a database.
Database management system (DBMS)	(DB2, IMS, IDMS) A software product that aids in controlling and using the data needed by application programs. DBMSs organize data in a database, manage all requests for database actions—such as queries or updates from users—and permit centralized control of security and data integrity.
Data center	See computer facility.
Data communications	The transfer of information from one computer to another through a communications medium, such as telephone lines, microwave relay, satellite link, or physical cable.
Data communications systems	See data communications.
Data design	Organization of data into structures to facilitate retrieval while minimizing redundancy. The design of transaction data elements is a critical factor in helping assure the quality of data as well as its interrelationship with other data elements.
Data definition	Identification of all fields in the database, how they are formatted, how they are combined into different types of records, and how the record types are interrelated.
Data file	See file.
Data management systems	Applications which handle significant volumes of data often employ data management system to perform certain data processing functions within an application. Data management systems include database management systems, specialized data transport/communications software (often called middleware, cryptography used in conjunction with data integrity controls, data warehouse software and data reporting/data extraction software.
Data owner	See owner.
Data processing	The computerized preparation of documents and the flow of data contained in these documents through the major steps of recording, classifying, and summarizing.
Data processing center	See computer facility.

Data quality standard	Requirements to ensure the state of completeness, validity, consistency, timeliness and accuracy that make data appropriate for a specific use.
Data security	See security management function.
Data strategy	Plan used to identify data needed to support business processes. A clearly defined data strategy minimizes data redundancies fundamental to an efficient, effective transaction processing function.
Data validation	Checking transaction data for any errors or omissions that can be detected by examining the data.
Data warehouse	A generic term for a system used to store, retrieve, and manage large amounts of data. A database, often remote, that contains recent snapshots of corporate data that can be used for analysis without slowing down day-to-day operations of the production database.
DBA	See database administrator.
DBMS	See database management system.
Debug	With software, to detect, locate, and correct logical or syntactical errors in a computer program.
Decryption	The process of changing ciphertext using a cryptographic algorithm and key.
Defense-in-depth	A commonly accepted “best practice” for implementing computer security controls in today’s networked environments. Integrates people, operations, and technology capabilities to protect information systems across multiple layers.
Delete access	This level of access provides the ability to erase or remove data or programs.
Denial of Service (DOS)	The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)
Denial of Service (DOS) Attack	An assault on a service from a single source that floods it with so many requests that it becomes overwhelmed and is either stopped completely or operates at a significantly reduced rate
Detection risk	The risk that the auditor will not detect a material misstatement that exists in an assertion.
Dial-up access	A means of connecting to another computer, or a network similar to the Internet, over a telecommunications line using a modem-equipped computer.
Dial-back	Used as a control over dial-up telecommunications lines. The telecommunications link established through dial-up into the computer from a remote location is interrupted so the computer can dial back to the caller. The link is permitted only if the caller is from a valid phone number or telecommunications channel.

Digital Certificate	A certificate identifying a public key to its subscriber, corresponding to a private key held by that subscriber. It is a unique code that typically is used to allow the authenticity and integrity of communicated data to be verified.
Digital signature	Cryptographic process used to assure message originator authenticity, integrity, and nonrepudiation.
Direct access	An access method for finding an individual item on a storage device and accessing it directly, without having to access all preceding records.
Disaster recovery plan	A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.
Diskette	A removable and widely-used data storage medium that uses a magnetically coated flexible disk of Mylar enclosed in a plastic case.
DNS (domain name system)	A hierarchical database that is distributed across the Internet that allows names to be resolved into IP addresses (and vice versa) to locate services such as web and e-mail servers
Download	Process of transferring data from a central computer to a personal computer or workstation.
Edit controls	Detects errors in the input portion of information that is sent to the computer for processing. The controls may be manual or automated and allow the user to edit data errors before processing.
Electronic signature	A symbol generated through electronic means that can be used to (1) identify the sender of information and (2) ensure the integrity of the critical information received from the sender. An electronic signature may represent either an individual or an entity. Adequate electronic signatures are (1) unique to the signer, (2) under the signer's sole control, (3) capable of being verified, and (4) linked to the data in such a manner that, if data are changed, the signature is invalidated upon verification. Traditional user identification code/password techniques do not meet these criteria.
Embedded Audit Module	Integral part of an application system that is designed to identify and report specific transactions or other information based on pre-determined criteria. Identification of reportable items occurs as part of real-time processing. Reporting may be real-time online, or may use store and forward methods. Also known as integrated test facility or continuous auditing module.
Encryption	Encryption is the conversion of data into a form, called a cipher text, which cannot be easily understood by unauthorized people.

Enterprise Resource Planning (ERP)	Commercial software that integrates all the information flowing through the entity. ERP systems contain functional modules (e.g., financial, accounting, human resources, supply chain, and customer information) that are integrated within the core system or interfaced to external systems.
Entity or component level	Controls at the entity or component level consist of the entitywide or componentwide processes designed to achieve the control activities. They are focused on how the entity or component manages IS related to each general control activity.
Entitywide information security program	An entity program that establishes a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. An entitywide information security program is the foundation of a security control structure and a reflection of senior management's commitment to addressing security risks. FISMA requires federal agencies to establish an agency-wide information security program.
Entry points	Access points to the entity's information systems. This may include remote access through dial-up, wireless devices, or the Internet
Environmental controls	This subset of physical access controls prevents or mitigates damage to facilities and interruptions in service. Smoke detectors, fire alarms and extinguishers, and uninterruptible power supplies are some examples of environmental controls.
Execute access	This level of access provides the ability to execute a program.
Exit	A predefined or in-house written routine that receives controls at a predefined point in processing. These routines provide an entity with the flexibility to customize processing, but also create the opportunity to bypass security controls.
Field	A location in a record in which a particular type of data are stored. In a database, the smallest unit of data that can be named. A string of fields is a concatenated field or record.
File	A collection of records stored in computerized form.
Financial management system	Under FFMIA, a financial management system includes financial information systems and the financial portions of mixed systems (systems that support both financial and nonfinancial functions) that are necessary to support financial management.
Firewall	Hardware and software components that protect one set of system resources (e.g., computers, networks) from attack by outside network users (e.g., Internet users) by blocking and checking all incoming network traffic. Firewalls permit authorized users to access and transmit privileged information and deny access to unauthorized users.

Firmware	Program recorded in permanent or semi permanent computer memory.
FFMIA	Enacted into law in Public Law 104-208, Title VIII (31 U.S.C. 3512 note), was intended to advance Federal financial management by ensuring that Federal financial management systems can and do provide reliable, consistent disclosure of financial data, and that they do so on a basis that is uniform across the Federal government from year to year consistently using professionally accepted accounting standards.
FISMA	Enacted into law as Title III of the E-Government Act of 2002 (PL 107-347; December 17, 2002), FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets.
FMFIA	The objective of the Federal Managers' Financial Integrity Act of 1982 (31 U.S.C. 3512 (c)and (d)) is to provide reasonable assurance that (1) obligations and costs are in compliance with applicable law, (2) funds, property, and other assets are safeguarded against waste, loss, unauthorized use, or misappropriation, and (3) revenues and expenditures applicable to agency operations are properly recorded and accounted for to permit the preparation of accounts and reliable financial and statistical reports and to maintain accountability over the assets.
Flowchart	A diagram of the movement of transactions, computer functions, media, and/or operations within a system. The processing flow is represented by arrows between symbolic shapes for operation, device, data file, etc. to depict the system or program.
Fraud	Fraud is a type of illegal act involving the obtaining of something of value through willful misrepresentation.
FTP (file transfer protocol)	A protocol used to transfer files over a TCP/IP network (Internet, UNIX, etc.)
GAGAS	Also referred to as the Yellow Book. IT provides standards and guidance for use by government auditors to ensure that they maintain competence, integrity, objectivity, and independence in planning, conducting, and reporting their work, and are to be followed by auditors and audit organizations when required by law regulation, contract, agreement, or policy.
Gateway	In networks, a computer that connects two dissimilar local area networks, or connects a local area network to a wide area network, minicomputer, or mainframe. A gateway may perform network protocol conversion and bandwidth conversion.

General controls	General controls are the structure, policies, and procedures that apply to an entity's overall computer operations. They include an entitywide security program, access controls, application development and change controls, segregation of duties, system software controls, and service continuity controls.
General support system	An interconnected set of information resources under the same direct management control that shares common functionality. Normally, the purpose of a general support system is to provide processing or communications support.
Hacker	A person who attempts to enter a system without authorization from a remote location.
Hardware	The physical components of IT, including the computers, peripheral devices such as printers, disks, and scanners, and cables, switches, and other elements of the telecommunications infrastructure.
Hashing	Value computed on data to detect error or manipulation.
Hot site	A fully operational off-site data processing facility equipped with both hardware and system software to be used in the event of a disaster.
HTTP (hyper text transfer protocol)	A communication protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a web server and transmit HTML pages to the client browser.
HTTPS (hyper text transfer protocol secure)	A protocol for accessing a secure web server, whereby all data transferred is encrypted
Hub	A common connection point for devices in a network, hubs commonly is used to connect segments of a LAN. A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.
Identification	The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system.
IDS	See intrusion detection system.
IEEE	Institute of Electrical and Electronics Engineers)—Pronounced I-triple-E, IEEE is an organization composed of engineers, scientists and students. The IEEE is best known for developing standards for the computer and electronics industry.
Implementation	The process of making a system operational in the organization.
Incident	Assessed occurrence having actual or potentially adverse effects on an IS.
Incident response program	A process that involves detecting a problem, determining its cause, minimizing the damage it causes, resolving the problem, and documenting each step of the response for future reference.

Incompatible duties	When work responsibilities are not segregated so that one individual controls critical stages of a process incompatible duties exist. For example, while users may authorize program changes, programmers should not be allowed to do so because they are not the owners of the system and do not have the responsibility to see that the system meets user needs. Similarly, one computer programmer should not be allowed to independently write, test, and approve program changes.
Information	The meaning of data. Data are facts; they become information when they are seen in context and convey meaning.
Information resource owner	See owner.
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information system boundaries	Logical or physical boundaries around information resources and implementing measures to prevent unauthorized information exchange across the boundary in either direction. Firewall devices represent the most common boundary protection technology at the network level.
Information System (IS) Control	As defined in GAGAS, information system (IS) controls consist of those internal controls that are dependent on information systems processing and include general controls and application controls.
Information System Owner (or Program Manager)	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
Information systems management	The function that directs or manages the activities and staff of the IS department and its various organizational components.
Information Type	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, executive order, directive, policy, or regulation.
Infrastructure application	Include software that is used to assist in performing systems operations, including management of network devices. These applications include database, e-mail, browsers, plug-ins, utilities, and applications not directly related to business processes.
Input	Any information entered into a computer, or the process of entering data into the computer.
Integration testing	Testing to determine if related information system components perform to specifications.

Integrity	Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity. This involves ensuring that transmitted or stored data are not altered by unauthorized persons in a way that is not detectable by authorized users.
Interface	A connection between two devices, applications, or networks or a boundary across which two systems communicate. Interface may also refer to the portion of a program that interacts with the user.
Interface controls	Controls used to provide reasonable assurance that data used by applications that is input from legacy systems is reliable, valid, complete, and properly converted from the legacy application into the applications they support.
Interface design	Uses guidelines set by the strategy and provides specific information for each of the characteristics defined in the strategy. See Interface Strategy
Interface strategy	Describes at the highest level how the interfaces are implemented between two applications, The interface strategy includes an explanation of each interface, the interface method chosen (manual or batch, etc.), the data fields being interfaced, the controls to reasonably assure that the data is interfaced completely and accurately, timing requirements, assignment of responsibilities, on-going system balancing requirements, and security requirements.
Internal control	(also referred to as internal control structure) A process, affected by entity management and other personnel, designed to provide reasonable assurance that (1) operations, including the use of entity resources, are effective and efficient; (2) financial reporting, including reports on budget execution, financial statements, and other reports for internal and external use, are reliable; and (3) applicable laws and regulations are followed. Internal control also includes the safeguarding of entity assets against unauthorized acquisition, use, or disposition. Internal control consists of 5 interrelated components that form an integrated process that can react to changing circumstances and conditions within the entity. These components include the control environment, risk assessment, control activities, information and communication, and monitoring.
Internet	When capitalized, the term “Internet” refers to the collection of networks and gateways that use the transmission control protocol/Internet protocol suite of protocols.
Internet protocol	Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks.
Intrusion	Any intentional violation of the security policy of a system.

Intrusion Detection System (IDS)	An intrusion detection system (IDS) inspects network activity to identify suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system
Intranet	A private network that uses the infrastructure and standards of the Internet and World Wide Web, but is isolated from the public Internet by firewall barriers.
Inventory	FISMA requires that each agency develop, maintain, and annually update an inventory of major information systems operated by the agency or under its control. The inventory must include identification of the interfaces between agency systems and all other systems or networks, including interfaces not controlled by the agency.
Job	A set of data that completely defines a unit of work for a computer. A job usually includes programs, linkages, files, and instructions to the operating system.
Key	A long stream of seemingly random bits used with cryptographic algorithms. The keys must be known or guessed to forge a digital signature or decrypt an encrypted message.
Key area of audit interest	Those areas which are critical to achieving the audit objectives (e.g., general support and business process application systems and files or components thereof).
LAN	See local area network.
Label	See security label.
Least Privilege	Principle requiring that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. Application of this principle limits the damage that can result from accident, error, or unauthorized use of an IS.
Legacy system	A computer system consisting of older applications and hardware that was developed to solve a specific business problem. Many legacy systems do not conform to current standards, but are still in use because they solve the problem and replacing them would be too expensive.
Library	In computer terms, a library is a collection of similar files, such as data sets contained on tape and/or disks, stored together in a common area. Typical uses are to store a group of source programs or a group of load modules. In a library, each program is called a member. Libraries are also called partitioned data sets (PDS). Library can also be used to refer to the physical site where magnetic media, such as a magnetic tape, is stored. These sites are usually referred to as tape libraries.
Library control/management	The function responsible for controlling program and data files that are either kept on-line or on tapes and disks that are loaded onto the computer as needed.
Library copier	Software that can copy source code from a library into a program.

Library management software	Software that provides an automated means of inventorying software, ensuring that differing versions are not accidentally misidentified, and maintaining a record of software changes.
Local area network (LAN)	A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables a device to interact with any other on the network. Local area networks (LAN) commonly include microcomputers and shared (often expensive) resources such as laser printers and large hard disks. Most modern LANs can support a wide variety of computers and other devices. Separate LANs can be connected to form larger networks.
Log	With respect to computer systems, to record an event or transaction.
Log on	The process of establishing a connection with, or gaining access to, a computer system or peripheral device.
Logging file	See log.
Logical access control	The use of computer hardware and software to prevent or detect unauthorized access. For example, users may be required to input user identification numbers (ID), passwords, or other identifiers that are linked to predetermined access privileges.
Logical security	See logical access control.
Mainframe computer	A multi-user computer designed to meet the computing needs of a large organization. The term came to be used to refer generally to the large central computers developed in the late 1950s and 1960s to meet the accounting and information management needs of large organizations.
Maintenance	Altering programs after they have been in use for a while. Maintenance programming may be performed to add features, correct errors that were not discovered during testing, or update key variables (such as the inflation rate) that change over time.
Major application	OMB Circular A-130 defines a major application as an application that requires special attention due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification o, information in the application.
Malicious code	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host.

Management controls	The organization, policies, and procedures used to provide reasonable assurance that (1) programs achieve their intended result, (2) resources are used that are consistent with the organization's mission, (3) programs and resources are protected from waste, fraud, and mismanagement, (4) laws and regulations are followed, and (5) reliable and timely information is obtained, maintained, reported, and used for decision making.
Master console	In MVS environments, the master console provides the principal means of communicating with the system. Other multiple console support (MCS) consoles often serve specialized functions, but can have master authority to enter all MVS commands.
Master data	Referential data that provides the basis for ongoing business activities, e.g., customers, vendors, and employees.
Master data controls	Controls over master data, the key information that is relatively constant and shared between multiple functions or applications (e.g., vendors, customers, employee's data, and vendor files).
Master data design	Layout of key data requirements to ensure integrity and utility of data information. Data integrity requirements include, for example, requiring an entry in all key fields, such as address and account number and not accepting invalid values in the required fields.
Master file	In a computer, the most currently accurate and authoritative permanent or semi-permanent computerized record of information maintained over an extended period.
Material weakness – A-123 – Financial Reporting Controls	A material weakness is a reportable condition in which the design or operation of the internal controls does not reduce to a relatively low level the risk that losses, noncompliance, or misstatements in amounts that would be material in relation to the principal statements or to a performance measure or aggregation of related performance measures may occur and not be detected within a timely period by employees in the normal course of their assigned duties.
Material weakness – A-123 – Other Controls	Control deficiency or combination of control deficiencies that in management's judgment should be communicated because they represent significant weaknesses in the design or operation of internal control that could adversely affect the organization's ability to meet its internal control objectives.
Material weakness – GAGAS – financial reporting	A significant deficiency or combination of significant deficiencies that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected.
Material weakness – Single Audit compliance	A significant deficiency or combination of significant deficiencies, that result in more than a remote likelihood that material noncompliance with a type of compliance requirement of a federal program will not be prevented or detected by the entity's internal control.

Materiality	An auditing concept regarding the relative importance of an amount or item. An item is considered not to be material when it is not significant enough to influence decisions or have an effect on the financial statements.
Media controls	Controls implemented to prevent unauthorized physical access to digital (e.g., diskettes, flash/thumb drives, compact disks) and printed media (e.g., paper, microfilm) removed from information system and during pick-up, transport, and delivery to authorized users.
Merge access	This level of access provides the ability to combine data from two separate sources.
Microcomputer	Any computer with its arithmetic logic unit and control unit contained in one integrated circuit, called a microprocessor.
Microprocessor	An integrated circuit device that contains the miniaturized circuitry to perform arithmetic, logic, and control operations (i.e. contains the entire CPU on a single chip).
Middleware	Another term for an application programmer interface (API). It refers to the interfaces that allow programmers to access lower- or higher-level services by providing an intermediary layer that includes function calls to the services.
Migration	A change from an older hardware platform, operating system, or software version to a newer one.
Mobile code	Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.
Mobile computing	Ability to use technology that is not physically connected, or in remote or mobile (non static) environments. Requires that the mobile computing activity be connected wirelessly to and through the internet or to and through a private network. This connection ties the mobile device to centrally located information and/or application software through the use of battery powered, portable, and wireless computing and communication devices. This includes devices like laptops with wireless LAN or wireless WAN technology, smart mobile phones, wearable computers and Personal Digital Assistants (PDAs).
Modem	Short for modulator-demodulator. A device that allows digital signals to be transmitted and received over analog telephone lines. This type of device makes it possible to link a digital computer to the analog telephone system. It also determines the speed at which information can be transmitted and received.

Multiyear testing plan	Where IS audits are performed on a regular basis the auditor may develop a multiyear audit plan. Such a plan will cover relevant key entity applications, systems, and processing centers. These strategic plans should cover no more than 3-year period and include the schedule and scope of assessments to be performed during the period and the rationale for planned approach.
Naming conventions	Standards for naming computer resources, such as data files, program libraries, individual programs, and applications.
Network	A group of computers and associated devices that are connected by communications facilities. A network can involve permanent connections, such as cables, or temporary connections made through telephone or other communications links. A network can be as small as a local area network consisting of a few computers, printers, and other devices, or it can consist of many small and large computers distributed over a vast geographic area.
Network administration	The function responsible for maintaining secure and reliable network operations. This function serves as a liaison with user departments to resolve network needs and problems.
Network architecture	The underlying structure of a computer network, including hardware, functional layers, interfaces, and protocols (rules) used to establish communications and ensure the reliable transfer of information. Because a computer network is a mixture of hardware and software, network architectures are designed to provide both philosophical and physical standards for enabling computers and other devices to manage the complexities of establishing communications links and transferring information without conflict. Various network architectures exist, among them the internationally accepted seven-layer open systems interconnection model and International Business Machine (IBM) Systems Network Architecture. Both the open systems interconnection model and the Systems Network Architecture organize network functions in layers, each layer dedicated to a particular aspect of communication or transmission and each requiring protocols that define how functions are carried out. The ultimate objective of these and other network architectures is the creation of communications standards that will enable computers of many kinds to exchange information freely.
Network component	Devices that support a network including, workstations, servers, switches, and routers.

Network scanning	Procedure for identifying active hosts on a network, either for the purpose of attacking them or for network security assessment. Scanning procedures, such as ping sweeps and port scans, return information about which IP addresses map to live hosts that are active on the Internet and what services they offer. Another scanning method, inverse mapping, returns information about what IP addresses do not map to live hosts; this enables an attacker to make assumptions about viable addresses.
Network session	A connection between two network component peers. This provides the capability of bundling of resources needed for an instance of a service.
Node	In a local area network, a connection point that can create, receive, or repeat a message. Nodes include repeaters, file servers, and shared peripherals. In common usage, however, the term node is synonymous with workstation.
Nonrepudiation	The ability to prevent senders from denying that they have sent messages and receivers from denying that they have received messages.
Object code	The machine code generated by a source code language processor such as an assembler or compiler. A file of object code may be immediately executable or it may require linking with other object code files, e.g., libraries, to produce a complete executable program.
Object privilege	Allows the user to have access to the data within an object or allow the user to execute a stored program. These include: SELECT, INSERT, DELETE, etc. Each type of object has different privileges associated with it.
Off-the-shelf software	Software that is marketed as a commercial product, unlike custom programs that are privately developed for a specific client.
Online	A processing term that categorizes operations that are activated and ready for use. If a resource is online, it is capable of communicating with or being controlled by a computer. For example, a printer is online when it can be used for printing. An application is classified as online when users interact with the system as their information is being processed, as opposed to batch processing.
Online editors	See online program development software.
Online program development software	(TSO, ROSCOE, VOLLIE, ICCF, ISPF) Software that permits programs to be coded and compiled in an interactive mode.
Operating system	The software that controls the execution of other computer programs, schedules tasks, allocates storage, manages the interface to peripheral hardware, and presents a default interface to the user when no application program is running.

Operational controls	Relate to managing the entity's business and include policies and procedures to carry out organizational objectives, such as planning, productivity, programmatic, quality, economy, efficiency, and effectiveness objectives. Management uses these controls to provide reasonable assurance that the entity (1) meets its goals, (2) maintains quality standards, and (3) does what management directs it to do.
Output	Data/information produced by computer processing, such as graphic display on a terminal or hard copy.
Output devices	Peripheral equipment, such as a printer or tape drive, that provides the results of processing in a form that can be used outside the system.
Override	Decision made by entity management or operation staff to bypass established control(s) to allow a transaction or transactions that would otherwise be rejected by the system controls to be processed.
Owner	Manager or director who has responsibility for a computer resource, such as a data file or application program.
Packet	Data unit that is routed from source to destination in a packet-switched network. A packet contains both routing information and data. Transmission control protocol/Internet protocol (TCP/IP) is such a packet-switched network.
Packet Filtering	Controlling access to a network by analyzing the attributes of the incoming and outgoing packets and either letting them pass, or denying them, based on a list of rules
Parameter	A value that is given to a variable. Parameters provide a means of customizing programs.
Partitioning	Process of physically or logically separating different functions such as applications, security and communication activities. Separation may be accomplished by using different computers, different central processing units, different instances of the operating systems, different network addresses, or combinations of these methods.
Password	A confidential character string used to authenticate an identity or prevent unauthorized access.
Password Cracker	Specialized security checker that tests user's passwords, searching for passwords that are easy to guess by repeatedly trying words from specially crafted dictionaries. Failing that, many password crackers can brute force all possible combinations in a relatively short period of time with current desktop computer hardware.
Patch	Patches are additional pieces of code that have been developed to address specific problems or flaws in existing software. Vulnerabilities are flaws that can be exploited, enabling unauthorized access to IT systems or enabling users to have access to greater privileges than authorized.

Penetration testing	Security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation.
Peripheral	A hardware unit that is connected to and controlled by a computer, but that is external to the CPU. These devices provide input, output, or storage capabilities when used in conjunction with a computer.
Personally identifiable information	Refers to any information about an individual maintained by an entity, including any information that can be used to distinguish or trace an individual's identity, such as their name, social security number, date of birth, or biometric records, and any other information which is linked or linkable to an individual.
Personnel controls	This type of control involves screening individuals prior to their authorization to access computer resources. Such screening should be commensurate with the risk and magnitude of the harm the individual could cause.
Personnel security	See personnel controls.
Physical access control	This type of control involves restricting physical access to computer resources and protecting these resources from intentional or unintentional loss or impairment.
Physical security	See physical access control.
Plain text	Data input to the Cipher or output from the Inverse Cipher.
Plans of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Platform	The foundation technology of a computer system. Typically, a specific combination of hardware and operating system.
Privacy Impact Assessment	An analysis of how information is handled: (1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
Privileged account	Individuals who have access to set "access rights" for users on a given system. Sometimes referred to as system or network administrative accounts.
Privileged User	Individual who has access to system control, monitoring, or administration functions (e.g., system administrator, system security officer, maintainers, system programmers, etc.)
Process	Systematic sequences of operations to produce a specified result. This includes all functions performed within a computer such as editing, calculating, summarizing, categorizing, and updating.

Processing	The execution of program instructions by the computer's CPU.
Production control and scheduling	The function responsible for monitoring the information into, through, and as it leaves the computer operations area and for determining the succession of programs to be run on the computer. Often, an automated scheduling package is used in this task.
Production environment	The system environment where the entity performs its operational information processing activities.
Production programs	Programs that are being used and executed to support authorized organizational operations. Such programs are distinguished from "test" programs that are being developed or modified, but have not yet been authorized for use by management.
Profile	A set of rules that describe the nature and extent of access to available resources for a user or a group of users with similar duties, such as accounts payable clerks. (See standard profile and user profile.)
Program	A set of related instructions that, when followed and executed by a computer, perform operations or tasks. Application programs, user programs, system programs, source programs, and object programs are all software programs.
Program library	See library.
Programmer	A person who designs, codes, tests, debugs, and documents computer programs.
Proprietary	Privately owned, based on trade secrets, privately developed technology, or specifications that the owner refuses to divulge, which prevents others from duplicating a product or program unless an explicit license is purchased.
Protocol	In data communications and networking, a standard that specifies the format of data as well as the rules to be followed when performing specific functions, such as establishing a connection and exchanging data.
Public access controls	A subset of access controls that apply when an entity application promotes or permits public access. These controls protect the integrity of the application and public confidence in the application and include segregating the information made directly available to the public from official entity records.
Public domain software	Software that has been distributed with an explicit notification from the program's author that the work has been released for unconditional use, including for-profit distribution or modification by any party under any circumstances.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

Quality assurance	The function that reviews software project activities and tests software products throughout the software life cycle to determine if (1) the software project is adhering to its established plans, standards, and procedures and (2) the software meets the functional specifications defined by the user.
Query	The process of extracting data from a database and presenting it for use.
Read access	This level of access provides the ability to look at and copy data or a software program.
Real-time system	A computer and/or a software system that reacts to events before they become obsolete. This type of system is generally interactive and updates files as transactions are processed.
Record	A unit of related data fields. The group of data fields that can be accessed by a program and contains the complete set of information on a particular item.
Reliability	The capability of hardware or software to perform as the user expects and to do so consistently, without failures or erratic behavior.
Remote access	The process of communicating with a computer located in another place over a communications link.
Remote job entry (RJE)	With respect to computer systems with locations geographically separate from the main computer center, submitting batch processing jobs via a data communications link.
Remote Maintenance	Maintenance activities conducted by individuals communicating external to an information system security perimeter.
Reportable condition – A 123	Reportable conditions include matters coming to the auditor's attention that, in the auditor's judgment, should be communicated because they represent significant deficiencies in the design or operation of internal controls, which could adversely affect the entity's ability to meet its internal control objectives.
Repudiation	The denial by one of the parties to a transaction or participation in all or part of that transaction or of the content of communications related to that transaction.
Residual risk	Portion of risk remaining after security measures have been applied.
Resource	Something that is needed to support computer operations, including hardware, software, data, telecommunications services, computer supplies such as paper stock and preprinted forms, and other resources such as people, office facilities, and noncomputerized records.
Risk	The level of impact on entity operations (including mission, functions, image, or reputation), entity assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

Risk analysis	The process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment.
Risk assessment	The identification and analysis of possible risks in meeting the entity's objectives that forms a basis for managing the risks identified and implementing deterrents.
Risk management	A management approach designed to reduce risks inherent in systems development and operations.
Router	An intermediary device on a communications network that expedites message delivery. As part of a LAN, a router receives transmitted messages and forwards them to their destination over the most efficient available route.
Run	A popular, idiomatic expression for program execution.
Run manual	A manual that provides application-specific operating instructions, such as instructions on job setup, console and error messages, job checkpoints, and restart and recovery steps after system failures.
Safeguards	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.
Sanitization	Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.
SAS 70	Statement on Auditing Standards No. 70: Service Organizations, commonly abbreviated as SAS 70, is an auditing statement issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA), officially titled "Reports on the Processing of Transactions by Service Organizations". SAS 70 defines the professional standards used by a service auditor to assess the internal controls of a service organization and issue a service auditor's report. Service organizations are typically entities that provide outsourcing services that impact the control environment of their customers.
SDLC methodology	See system development life cycle methodology.
Security administrator	Person who is responsible for managing the security program for computer facilities, computer systems, and/or data that are stored on computer systems or transmitted via computer networks.

Security Category	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.
Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Security Label	Explicit or implicit marking of a data structure or output media associated with an information system representing the FIPS 199 security category, or distribution limitations or handling caveats of the information contained therein.
Security management function	The function responsible for the development and administration of an entity's information security program. This includes assessing risks, implementing appropriate security policies and related controls, establishing a security awareness and education program for employees, and monitoring and evaluating policy and control effectiveness.
Security Objective	Confidentiality, integrity, or availability.
Security plan	A written plan that clearly describes the entity's security program and policies and procedures that support it. The plan and related policies should cover all major systems and facilities and should outline the duties of those who are responsible for overseeing security (the security management function) as well as those who own, use, or rely on the entity's computer resources.
Security policy	The set of management statements that documents an organization's philosophy of protecting its computing and information assets. The set of security rules enforced by the system's security features
Security profile	See profile.
Security requirements	Requirements levied on an information system that are derived from laws, executive orders, directives, policies, instructions, regulations, or organizational (mission) needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
Security software	See access control software.
Segregation/separation of duties	A basic control that prevents or detects errors and irregularities by assigning responsibility for initiating transactions, recording transactions and custody of assets to separate individuals. Commonly used in large IT organizations so that no single person is in a position to introduce fraudulent or malicious code without detection.

Sensitive information	Any information that an entity has determined requires heightened protection from unauthorized access, use, disclosure, disruption, modification, or destruction [e.g., by using specific access controls] because of the nature of the information (e.g., personal information required to be protected by the Privacy Act, proprietary commercial information, information critical to law enforcement activities, and information that has or may be determined to be exempt from public release under the Freedom of Information Act).
Sensitivity accounts	See privileged account
Server	A computer running administrative software that controls access to all or part of the network and its resources, such as disk drives or printers. A computer acting as a server makes resources available to computers acting as workstations on the network.
Service	Refers to customer or product-related business functions such as file transfer protocol (FTP), hypertext transfer protocol (HTTP), and mainframe supervisor calls. Each system provides a set of services. For example, a computer network alls its users to send packets to specified destinations and a database system responds to queries.
Service auditor	An independent auditor hired by the service organization to provide a report on internal controls at the service provider. See Service Organization.
Service Bureau	A computer facility that provides data processing services to clients on a continual basis
Service organization	Outside organizations used to support business processes. Service organizations provide services ranging from performing a specific task (e.g., payroll processing) to replacing entire business units or functions of an entity.
Significant deficiency – FISMA	A weakness in an agency's overall information systems security program or management control structure, or within one or more information systems, that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets.
Significant deficiency – A-123	OMB Circular A-123 uses the same definition for significant deficiency as financial reporting (See Significant Deficiency – Financial Reporting), but continues to refer to it as a reportable condition.
Significant Deficiency – financial reporting	A deficiency in internal control, or combination of deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected.

Significant deficiency – Single Audit compliance	A control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to administer a federal program such that there is more than a remote likelihood that noncompliance with a type of compliance requirement of a federal program that is more than inconsequential will not be prevented or detected by the entity's internal control.
Simultaneous peripheral operations online (SPOOL)	In the mainframe environment, a component of system software that controls the transfer of data between computer storage areas with different speed capabilities. Usually, an intermediate device, such as a buffer, exists between the transfer source and the destination (e.g., a printer).
Single Audit	The Single Audit is intended to provide a cost-effective audit for nonfederal entities in that one audit is conducted in lieu of multiple audits of individual programs. Such audits are performed in accordance with the Single Audit Act (31USC ch75) of 1984 (with amendment in 1996) and OMB Circular A-133 (*Audits of States, Local Governments, and Non-Profit Organizations*) to ensure that federal funds to nonfederal entities are expended properly.
Smart card	A credit card-sized token that contains a microprocessor and memory circuits for authenticating a user of computer, banking, or transportation services.
SMTP (Simple Mail Transport Protocol)	The standard e-mail protocol on the Internet
Sniffer	Synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.
Social engineering	A method used by hackers to obtain passwords for unauthorized access. For example, a hacker may call an authorized user of a computer system and pose as a network administrator to gain access.
Software	A computer program or programs, in contrast to the physical environment on which programs run (hardware).
Source code	Human-readable program statements written in a high-level or assembly language, as opposed to object code, which is derived from source code and designed to be machine-readable.
Spyware	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge.
Standard	In computing, a set of detailed technical guidelines used as a means of establishing uniformity in an area of hardware or software development.
Standard profile	A set of rules that describe the nature and extent of access to each resource that is available to a group of users with similar duties, such as accounts payable clerks.

Supervisor call (SVC)	A supervisor call instruction interrupts a program being executed and passes control to the supervisor so that it can perform a specific service indicated by the instruction.
Switch	A device that forwards packets between LAN devices or segments. LANs that use switches are called switched LANs.
System	See information system.
System administrator	The person responsible for administering use of a multi-user computer system, communications system, or both.
System analyst	A person who designs systems.
System designer	See system analyst.
System developer	See programmer.
System development life cycle (SDLC) methodology	The policies and procedures that govern software development and modification as a software product goes through each phase of its life cycle.
System level	Controls consist of processes for managing specific system resources related to either a general support system or business process application systems. Three sublevels include network, operating system, and infrastructure.
System management facility	An IBM control program that provides the means for gathering and recording information that can be used to evaluate the extent of computer system usage.
System privilege	Ability of the user within the database to interact with the database itself. They include: CREATE, ALTER, DROP, CONNECT, and AUDIT, among many others.
System programmer	A person who develops and maintains system software.
System security plan	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
System software	The set of computer programs and related routines designed to operate and control the processing activities of computer equipment. It includes the operating system and utility programs and is distinguished from application software.
System testing	Testing to determine that the results generated by the enterprise's information systems and their components are accurate and the systems perform to specifications.
System utilities	Software used to perform system maintenance routines that are frequently required during normal processing operations. Some of the utilities have powerful features that will allow a user to access and view or modify data or program code.
TCP (transmission control protocol)	A connection-based Internet protocol that supports reliable data transfer connections. Packet data is verified using checksums and retransmitted if it is missing or corrupted. The application plays no part in validating the transfer.

TCP/IP protocol	Transmission Control Protocol/Internet Protocol) A set of communications protocols that encompasses media access, packet transport, session communications, file transfer, electronic mail, terminal emulation, remote file access and network management. TCP/IP provides the basis for the Internet.
Technical controls	See logical access control.
Telecommunications	A general term for the electronic transmission of information of any type, such as data, television pictures, sound, or facsimiles, over any medium, such as telephone lines, microwave relay, satellite link, or physical cable.
Teleprocessing monitor	In the mainframe environment, a component of the operating system that provides support for online terminal access to application programs. This type of software can be used to restrict access to online applications and may provide an interface to security software to restrict access to certain functions within the application.
Terminal	A device consisting of a video adapter, a monitor, and a keyboard.
Test facility	A processing environment that is isolated from the production environment and dedicated to testing and validating systems and/or their components.
Those charged with governance	Are those responsible for overseeing the strategic direction of the entity and the entity's fulfillment of its obligations related to accountability. This includes overseeing the financial reporting process, subject matter, or program under audit including related internal controls.
Threat	Any circumstance or event with the potential to adversely impact entity operations (including mission, functions, image, or reputation), entity assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Token	In authentication systems, some type of physical device (such as a card with a magnetic strip or a smart card) that must be in the individual's possession in order to gain access. The token itself is not sufficient; the user must also be able to supply something memorized, such as a personal identification number (PIN).
Transaction	A discrete activity captured by a computer system, such as the entry of a customer order or an update of an inventory item. In financial systems, a transaction generally represents a business event that can be measured in money and entered in accounting records.
Transaction data	The finite data pertaining to a given event occurring in a business process. The result of this process is in the form of documents or postings, such as purchase orders and obligations.

Transaction data input	Relates to controls over data that enter the application (e.g., data validation and edit checks).
Transaction data output	Relates to controls over data output and distribution (e.g., output reconciliation and review).
Transaction data processing	Relates to controls over data integrity within the application (e.g., review of transaction processing logs).
Transaction file	A group of one or more computerized records containing current business activity and processed with an associated master file. Transaction files are sometimes accumulated during the day and processed in batch production overnight or during off-peak processing periods.
Trusted communication Path	A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can only be activated by the user or the security functions of the information system and cannot be imitated by untrusted software.
Uninterruptible power supply (UPS)	Provides short-term backup power from batteries for a computer system when the electrical power fails or drops to an unacceptable voltage level
Unit testing	Testing individual program modules to determine if they perform to specifications.
UNIX	A multitasking operating system originally designed for scientific purposes that have subsequently become a standard for midrange computer systems with the traditional terminal/host architecture. UNIX is also a major server operating system in the client/server environment.
Update access	This access level includes the ability to change data or a software program.
Upload	The process of transferring a copy of a file from a local computer to a remote computer by means of a modem or network.
User	The person who uses a computer system and its application programs to perform tasks.
User auditor	The auditor of the user organization.
User control	Portions of controls that are performed by people interacting with IS controls. The effectiveness of information systems processing or the reliability of information processed by IS controls.
User-defined processing	The user is allowed to establish or modify processing steps. This frequently occurs in application based spreadsheets and report writer/data extraction tools.
User identification (ID)	A unique identifier assigned to each authorized computer user.
User privilege	Right to execute a particular type of Microsoft SQL server statement, or a right to access another user's object

User profile	A set of rules that describes the nature and extent of access to each resource that is available to each user.
Utility program	Generally considered to be system software designed to perform a particular function (e.g., an editor or debugger) or system maintenance (e.g., file backup and recovery).
Validation	The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements.
Validity	See Validity Control.
Validity Control	Controls designed to provide reasonable assurance (1) that all recorded transactions actually occurred (are real), relate to the entity, and were properly approved in accordance with management's authorization, and (2) that output contains only valid data.
Virtual Private Network (VPN)	Protected IS link utilizing tunneling, security controls (see information assurance), and end-point address translation giving the impression of a dedicated line.
Virus	A program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the "infected" file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Vulnerability Assessment	Formal description and evaluation of the vulnerabilities in an information system.
Vulnerability scanning	Type of network security testing that among others enumerates the network structure and determines the set of active hosts and associated software and verifies that software (e.g., operating system and major applications) is up-to-date with security patches and software version.
Wide area network (WAN)	A group of computers and other devices dispersed over a wide geographical area that is connected by communications links.
WAN	See wide area network.
War Dialer	Software packages that sequentially dial telephone numbers, recording any numbers that answer.
Web application	Is an application that is accessed via web over a network such as the Internet or an intranet. The ability to update and maintain Web applications without distributing and installing software on potentially thousands of client computers is a key reason for their popularity.

Wired Equivalent Privacy (WEP)	The Wired Equivalent Privacy (WEP) security protocol for wireless local area networks (LANs) uses encryption to provide similar security to that of a wired LAN. WEP is defined in the IEEE 802.11b standard.
Wi-Fi Protected Access (WPA)	The Wi-Fi Protected Access (WPA) security protocol was designed to improve upon the security features of WEP for wireless communications. It is defined in IEEE's 802.11i standard.
Workstation	A microcomputer or terminal connected to a network. Workstation can also refer to a powerful, stand-alone computer that has considerable calculating or graphics capability.
World Wide Web (WWW)	A sub-network of the Internet through which information is exchanged by text, graphics, audio and video.
Worm	An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.

Appendix XII – Bibliography

Committee on National Security Systems, *National Information Assurance (IA) Glossary*, CNSS Instruction No. 4009 (Ft Meade, Maryland: Revised Draft 2005).

Information System Audit and Control Association (ISACA), *Glossary of Terms*, http://www.isaca.org/glossary.htm.

Information System Audit and Control Foundation, *CobiT: Control Objectives for Information and Related Technology*, 2007.

Institute of Internal Auditors, *Global Technology Audit Guide (GTAG) series.*

Office of Management and Budget, *Management Responsibility for Internal Control*, Circular A-123, Appendix A, (Washington, D.C. July 2005).

Office of Management and Budget, *Financial Management Systems*, Circular A-127, (Washington, D.C.: January 9, 2009).

Office of Management and Budget, *Security of Federal Automated Resources*, Circular A-130, Appendix III, (Washington, D.C.: November 2000).

Office of Management and Budget, *Reporting Instructions for the Federal Information Management Security Act and Updated Guidance on Quarterly IT Security Reporting*, Memorandum M-03-19 (Washington, D.C.: November 25, 2003).

Office of Management and Budget, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, Memorandum M-03-22 (Washington, D.C.: September 23, 2003).

Office of Management and Budget, *E-Authentication Guidance for Federal Agencies*, Memorandum M-04-04 (Washington, D.C.: December 16, 2003).

Office of Management and Budget, *Service Organization Audits*, Memorandum M-04-11 (Washington, D.C.: April 30, 2004).

Office of Management and Budget, *Personal Use Policies and "File Sharing" Technology*, Memorandum-04-26 (Washington, D.C.: September 8, 2004).

Office of Management and Budget, *Designation of Senior Agency Officials for Privacy*, Memorandum M-05-08 (Washington, D.C.: February 11, 2005).

Office of Management and Budget, *FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, Memorandum M-05-15 (Washington, D.C.: June 13, 2005).

Office of Management and Budget, *Safeguarding Personally Identifiable Information*, Memorandum M-06-15 (Washington, D.C.: May 22, 2006).

Office of Management and Budget, *Protection of Sensitive Agency Information*, Memorandum M-06-16 (Washington, D.C.: June 23, 2006).

Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, Memorandum M-06-19 (Washington, D.C.: July 12, 2006).

Office of Management and Budget, *Use of Commercial Credit Monitoring Services Blanket Purchase Agreements*, Memorandum M-07-04 (Washington, D.C.: December 22, 2006).

Office of Management and Budget, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*, Memorandum M-07-11 (Washington, D.C.: March 22, 2007).

Office of Management and Budget, *Safeguarding Against and Responding to the Breach of Personally identifiable Information*, Memorandum M-07-16 (Washington, D.C.: May 22, 2007).

Office of Management and Budget, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, Memorandum M-08-21 (Washington, D.C. July 14, 2008)[125].

Office of Management and Budget, *Guidance on the Federal Desktop Core Configuration (FDCC)*, Memorandum M-08-22 (Washington, D.C.: August 11, 2008).

U.S. Department of Commerce, National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules*, Federal Information Processing Standards 140-2, (Washington, D.C.: May 2001).

U.S. Department of Commerce, National Institute of Standards and Technology, *Advance Encryption Standard (AES)*, Federal Information Processing Standards 197, (Washington, D.C.: November 2001).

U.S. Department of Commerce, National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards 199, (Washington, D.C.: February 2004).

U.S. Department of Commerce, National Institute of Standards and Technology, *Minimum Security Requirements for Federal Information and Information Systems*, Federal Information Processing Standards 200, (Washington, D.C.: March 2006).

U.S. Department of Commerce, National Institute of Standards and Technology, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, Federal Information Processing Standards 201, (Washington, D.C.: March 2006).

U.S. Department of Commerce, National Institute of Standards and Technology, *Glossary of Key Information Security Terms*, (Washington, D.C.: April 2006).

[125]OMB generally issues updated guidance annually.

U.S. Department of Commerce, National Institute of Standards and Technology, *Introduction to Computer Security*, Special Publication 800-12, (Washington, D.C.: October 1995).

U.S. Department of Commerce, National Institute of Standards and Technology, *Information Technology Security Training Requirements: A Role-Performance-Based Model*, Special Publication 800-16, (Washington, D.C.: April 1998).

U.S. Department of Commerce, National Institute of Standards and Technology, *Guide for Developing Security Plans for Federal Information Systems*, Special Publication 800-18, (Washington, D.C.: February 2006).

U.S. Department of Commerce, National Institute of Standards and Technology, *Guideline for Implementing Cryptography in the Federal Government*, Special Publication 800-21, (Washington, D.C.): December 2005).

U.S. Department of Commerce, National Institute of Standards and Technology, *Engineering Principles for Information Technology Security*, Special Publication 800-27, (Washington, D.C.: June 2004).

U.S. Department of Commerce, National Institute of Standards and Technology, *Risk Management Guide for Information Technology Systems*, Special Publication 800-30, (Washington, D.C.: July 2002).

U.S. Department of Commerce, National Institute of Standards and Technology, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, Special Publication 800-32, (Washington D.C.: February 2001).

U.S. Department of Commerce, National Institute of Standards and Technology, *Contingency Planning Guide for Information Technology Systems*, Special Publication 800-34, (Washington, D.C.: June 2002).

U.S. Department of Commerce, National Institute of Standards and Technology, *Guide to Information Technology Security Services*, Special Publication 800-35, (Washington, D.C.: October 2003).

U.S. Department of Commerce, National Institute of Standards and Technology, *Guide for Security Certification and Accreditation of Federal Information Systems*, Special Publication 800-37, (Washington, D.C.: May 2004).

U.S. Department of Commerce, National Institute of Standards and Technology, *Creating a Patch and Vulnerability Management Program*, Special Publication 800-40, (Washington, D.C.: November 2005).

U.S. Department of Commerce, National Institute of Standards and Technology, *Guideline on Network Security*, Special Publication 800-42, (Washington, D.C.: November 2002).

U.S. Department of Commerce, National Institute of Standards and Technology, *Security for Telecommuting and Broadband Communications*, Special Publication 800-46, (Washington, D.C.: August 2002).

U.S. Department of Commerce, National Institute of Standards and Technology, *Security Guide for Interconnecting Information Technology Systems*, Special Publication 800-47, (Washington, D.C.: August 2002).

U.S. Department of Commerce, National Institute of Standards and Technology, *Building an Information Technology Security Awareness and Training Program*, Special Publication 800-50, (Washington, D.C.: October 2003).

U.S. Department of Commerce, National Institute of Standards and Technology, R*ecommended Security Controls for Federal Information*, Special Publication 800-53. (Washington, D.C.: December 2007).

U.S. Department of Commerce, National Institute of Standards and Technology, *Security Metrics Guide for Information Technology Systems*, Special Publication 800-55, (Washington, D.C.: July 2003).

U.S. Department of Commerce, National Institute of Standards and Technology, *Recommendation for Pair-Wise Key Established*

Schemes Using Discrete Logarithm Cryptography, Special Publication 800-56, (Washington, D.C.: March 2006).

U.S. Department of Commerce, National Institute of Standards and Technology, *Recommendation for Key Management*, Special Publication 800-57, (Washington, D.C.: August 2005).

U.S. Department of Commerce, National Institute of Standards and Technology, *Security Considerations for Voice over IP Systems*, Special Publication 800-58, (Washington, D.C.: January 2005).

U.S. Department of Commerce, National Institute of Standards and Technology, *Guide for Mapping Types of Information and Information System Security Categories*, Special Publication 800-60 Revision 1, (Washington, D.C.: August 2008).

U.S. Department of Commerce, National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61, (Washington, D.C.: January 2004).

U.S. Department of Commerce, National Institute of Standards and Technology, *Electronic Authentication Guidelines*, Special Publication 800-63, (Washington, D.C.: April 2006).

U.S. Department of Commerce, National Institute of Standards and Technology, *Security Considerations in the Information System Development Life Cycle*, Special Publication 800-64, (Washington, D.C.: June 2004).

U.S. Department of Commerce, National Institute of Standards and Technology, *Security Configuration Checklists Program for IT Products*, Special Publication 800-70, (Washington, D.C.: May 2005).

U.S. Department of Commerce, National Institute of Standards and Technology, *Interfaces for Personal Identity Verification*, Special Publication 800-73-2, (Washington, D.C.: September 2008).

U.S. Department of Commerce, National Institute of Standards and Technology, *Biometric Data Specifications for Personal Identity Verification*, Special Publication 800-76, (Washington, D.C.: January 2007).

U.S. Department of Commerce, National Institute of Standards and Technology, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, Special Publication 800-78, (Washington, D.C.: August 2007).

U.S. Department of Commerce, National Institute of Standards and Technology, *Guide to Intrusion Detection and Prevention Systems*, Special Publication 800-94, (Washington, D.C.: February 2007).

U.S. Department of Commerce, National Institute of Standards and Technology, *Establishing Wireless Robust Security Networks*, Special Publication 800-97, (Washington, D.C.: February 2007).

U.S. Department of Commerce, National Institute of Standards and Technology, *Information Security Handbook: A Guide for Managers*, Special Publication 800-100, (Washington, D.C.: March 2007).

U.S. Department of Commerce, National Institute of Standards and Technology, *Technical Guide to Information Security Testing and Assessment*, Special Publication 800-115, (Washington, D.C.: September 2008).

U.S. Department of Justice, *Vulnerability Assessment of Federal Facilities*, (Washington, D.C.: June 28, 1995).

U.S. General Accounting Office, *Executive Guide: Information Security Management, Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

U.S. General Accounting Office, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-01.3.1 (Washington, D.C.: November 1999).

U.S. General Accounting Office, *Key Elements of a Risk Management Approach*, GAO-02-150T (Washington, D.C.: October 2001).

U.S. General Accounting Office, *Technologies to Secure Federal Buildings*, GAO-02-687T (Washington, D.C.: April 2002).

U.S. General Accounting Office, *Assessing the Reliability of Computer-Processed Data*, (Washington, D.C. October 2002).

U.S. Government Accountability Office, *Federal Information System Controls Audit Manual*, GAO/AIMD-12.19.6. (Washington, D.C.: January 1999).

U.S. Government Accountability Office, *Government Auditing Standards*, GAO-07-162G (Washington, D.C.: July 2007).

United States General Accounting Office

GAO

Internal Control

November 1999

Standards for Internal Control in the Federal Government

(b) (5)

(b) (5)

GAO/AIMD-00-21.3.1

Foreword

Federal policymakers and program managers are continually seeking ways to better achieve agencies' missions and program results, in other words, they are seeking ways to improve accountability. A key factor in helping achieve such outcomes and minimize operational problems is to implement appropriate internal control. Effective internal control also helps in managing change to cope with shifting environments and evolving demands and priorities. As programs change and as agencies strive to improve operational processes and implement new technological developments, management must continually assess and evaluate its internal control to assure that the control activities being used are effective and updated when necessary.

The Federal Managers' Financial Integrity Act of 1982 (FMFIA) requires the General Accounting Office (GAO) to issue standards for internal control in government. The standards provide the overall framework for establishing and maintaining internal control and for identifying and addressing major performance and management challenges and areas at greatest risk of fraud, waste, abuse, and mismanagement. Office of Management and Budget (OMB) Circular A-123, Management Accountability and Control, revised June 21, 1995, provides the specific requirements for assessing and reporting on controls. The term internal control in this document is synonymous with the term management control (as used in OMB Circular A-123) that covers all aspects of an agency's operations (programmatic, financial, and compliance).

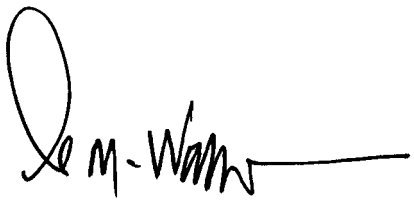
Recently, other laws have prompted renewed focus on internal control. The Government Performance and Results Act of 1993 requires agencies to clarify their missions, set strategic and annual performance goals, and measure and report on performance

toward those goals. Internal control plays a significant role in helping managers achieve those goals. Also, the Chief Financial Officers Act of 1990 calls for financial management systems to comply with internal control standards, and the Federal Financial Management Improvement Act of 1996 identifies internal control as an integral part of improving financial management systems.

Rapid advances in information technology have highlighted the need for updated internal control guidance related to modern computer systems. The management of human capital has gained recognition as a significant part of internal control. Furthermore, the private sector has updated its internal control guidance with the issuance of Internal Control — Integrated Framework, published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). Consequently, we have developed this standards update which supersedes our previously issued "Standards for Internal Controls in the Federal Government."

This update gives greater recognition to the increasing use of information technology to carry out critical government operations, recognizes the importance of human capital, and incorporates, as appropriate, the relevant updated internal control guidance developed in the private sector. The standards are effective beginning with fiscal year 2000 and the Federal Managers Financial Integrity Act reports covering that year.

We appreciate the efforts of government officials, public accounting professionals, and other members of the financial community and academia who provided valuable assistance in developing these standards.



David M. Walker
Comptroller General
of the United States

Introduction

The following definition, objectives, and fundamental concepts provide the foundation for the internal control standards.

Definition and Objectives

Internal Control

An integral component of an organization's management that provides reasonable assurance that the following objectives are being achieved:

- effectiveness and efficiency of operations,
- reliability of financial reporting, and
- compliance with applicable laws and regulations.

Internal control is a major part of managing an organization. It comprises the plans, methods, and procedures used to meet missions, goals, and objectives and, in doing so, supports performance-based management. Internal control also serves as the first line of defense in safeguarding assets and preventing and detecting errors and fraud. In short, internal control, which is synonymous with management control, helps government program managers achieve desired results through effective stewardship of public resources.

Internal control should provide reasonable assurance that the objectives of the agency are being achieved in the following categories:

- Effectiveness and efficiency of operations including the use of the entity's resources.
- Reliability of financial reporting, including reports on budget execution, financial statements, and other reports for internal and external use.
- Compliance with applicable laws and regulations.

A subset of these objectives is the safeguarding of assets. Internal control should be designed to provide reasonable assurance regarding prevention of or prompt detection of unauthorized acquisition, use, or disposition of an agency's assets.

Fundamental Concepts

Internal Control

- A continuous built-in component of operations.
- Effected by people.
- Provides reasonable assurance, not absolute assurance.

The fundamental concepts provide the underlying framework for designing and applying the standards.

Internal Control Is a Continuous Built-in Component of Operations

Internal control is not one event, but a series of actions and activities that occur throughout an entity's operations and on an ongoing basis. Internal control should be recognized as an integral part of each system that management uses to regulate and guide its operations rather than as a separate system within an agency. In this sense, internal control is management control that is built into the entity as a

part of its infrastructure to help managers run the entity and achieve their aims on an ongoing basis.

Internal Control Is Effected by People

People are what make internal control work. The responsibility for good internal control rests with all managers. Management sets the objectives, puts the control mechanisms and activities in place, and monitors and evaluates the control. However, all personnel in the organization play important roles in making it happen.

Internal Control Provides Reasonable Assurance, Not Absolute Assurance

Management should design and implement internal control based on the related cost and benefits. No matter how well designed and operated, internal control cannot provide absolute assurance that all agency objectives will be met. Factors outside the control or influence of management can affect the entity's ability to achieve all of its goals. For example, human mistakes, judgment errors, and acts of collusion to circumvent control can affect meeting agency objectives. Therefore, once in place, internal control provides reasonable, not absolute, assurance of meeting agency objectives.

Internal Control Standards

Presentation of the Standards

The Five Standards for Internal Control

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communications
- Monitoring

These standards define the minimum level of quality acceptable for internal control in government and provide the basis against which internal control is to be evaluated. These standards apply to all aspects of an agency's operations: programmatic, financial, and compliance. However, they are not intended to limit or interfere with duly granted authority related to developing legislation, rule-making, or other discretionary policy-making in an agency. These standards provide a general framework. In implementing these standards, management is responsible for developing the detailed policies, procedures, and practices to fit their agency's operations and to ensure that they are built into and an integral part of operations.

In the following material, each of these standards is presented in a short, concise statement. Additional information is provided to help managers incorporate the standards into their daily operations.

Control Environment

Management and employees should establish and maintain an environment throughout the organization that sets a positive and supportive attitude toward internal control and conscientious management.

A positive control environment is the foundation for all other standards. It provides discipline and structure as well as the climate which influences the quality of internal control. Several key factors affect the control environment.

One factor is the integrity and ethical values maintained and demonstrated by management and staff. Agency management plays a key role in providing leadership in this area, especially in setting and maintaining the organization's ethical tone, providing guidance for proper behavior, removing temptations for unethical behavior, and providing discipline when appropriate.

Another factor is management's commitment to competence. All personnel need to possess and maintain a level of competence that allows them to accomplish their assigned duties, as well as understand the importance of developing and implementing good internal control. Management needs to identify appropriate knowledge and skills needed for various jobs and provide needed training, as well as candid and constructive counseling, and performance appraisals.

Management's philosophy and operating style also affect the environment. This factor determines the degree of risk the agency is willing to take and management's philosophy towards performance-based management. Further, the attitude and philosophy of management toward information systems, accounting, personnel functions, monitoring, and audits and evaluations can have a profound effect on internal control.

Another factor affecting the environment is the agency's organizational structure. It provides management's framework for planning, directing, and controlling operations to achieve agency objectives. A good internal control environment requires that the agency's organizational structure clearly define key areas of authority and responsibility and establish appropriate lines of reporting.

The environment is also affected by the manner in which the agency delegates authority and responsibility throughout the organization. This delegation covers authority and responsibility for operating activities, reporting relationships, and authorization protocols.

Good human capital policies and practices are another critical environmental factor. This includes establishing appropriate practices for hiring, orienting, training, evaluating, counseling, promoting, compensating, and disciplining personnel. It also includes providing a proper amount of supervision.

A final factor affecting the environment is the agency's relationship with the Congress and central oversight agencies such as OMB. Congress mandates the programs that agencies undertake and monitors their progress and central agencies provide policy and guidance on many different matters. In addition,

Inspectors General and internal senior management councils can contribute to a good overall control environment.

Risk Assessment

> Internal control should provide for an assessment of the risks the agency faces from both external and internal sources.

A precondition to risk assessment is the establishment of clear, consistent agency objectives. Risk assessment is the identification and analysis of relevant risks associated with achieving the objectives, such as those defined in strategic and annual performance plans developed under the Government Performance and Results Act, and forming a basis for determining how risks should be managed.

Management needs to comprehensively identify risks and should consider all significant interactions between the entity and other parties as well as internal factors at both the entitywide and activity level. Risk identification methods may include qualitative and quantitative ranking activities, management conferences, forecasting and strategic planning, and consideration of findings from audits and other assessments.

Once risks have been identified, they should be analyzed for their possible effect. Risk analysis generally includes estimating the risk's significance, assessing the likelihood of its occurrence, and

deciding how to manage the risk and what actions should be taken. The specific risk analysis methodology used can vary by agency because of differences in agencies' missions and the difficulty in qualitatively and quantitatively assigning risk levels.

Because governmental, economic, industry, regulatory, and operating conditions continually change, mechanisms should be provided to identify and deal with any special risks prompted by such changes.

Control Activities

> Internal control activities help ensure that management's directives are carried out. The control activities should be effective and efficient in accomplishing the agency's control objectives.

Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives, such as the process of adhering to requirements for budget development and execution. They help ensure that actions are taken to address risks. Control activities are an integral part of an entity's planning, implementing, reviewing, and accountability for stewardship of government resources and achieving effective results.

Control activities occur at all levels and functions of the entity. They include a wide range of diverse activities such as approvals, authorizations, verifications, reconciliations, performance reviews,

maintenance of security, and the creation and maintenance of related records which provide evidence of execution of these activities as well as appropriate documentation. Control activities may be applied in a computerized information system environment or through manual processes.

Activities may be classified by specific control objectives, such as ensuring completeness and accuracy of information processing.

Examples of Control Activities

- Top level reviews of actual performance,
- Reviews by management at the functional or activity level,
- Management of human capital,
- Controls over information processing,
- Physical control over vulnerable assets,
- Establishment and review of performance measures and indicators,
- Segregation of duties,
- Proper execution of transactions and events,
- Accurate and timely recording of transactions and events,
- Access restrictions to and accountability for resources and records, and
- Appropriate documentation of transactions and internal control.

There are certain categories of control activities that are common to all agencies. Examples include the following:

Top Level Reviews of Actual Performance	Management should track major agency achievements and compare these to the plans, goals, and objectives established under the Government Performance and Results Act.
Reviews by Management at the Functional or Activity Level	Managers also need to compare actual performance to planned or expected results throughout the organization and analyze significant differences.
Management of Human Capital	Effective management of an organization's workforce—its human capital—is essential to achieving results and an important part of internal control. Management should view human capital as an asset rather than a cost. Only when the right personnel for the job are on board and are provided the right training, tools, structure, incentives, and responsibilities is operational success possible. Management should ensure that skill needs are continually assessed and that the organization is able to obtain a workforce that has the required skills that match those necessary to achieve organizational goals. Training should be aimed at developing and retaining employee skill levels to meet changing organizational needs. Qualified and continuous supervision should be provided to ensure that internal control objectives are achieved. Performance evaluation and feedback, supplemented by an effective reward system, should be designed to help employees understand the connection between their performance and the organization's success. As a part of its human capital planning, management should also consider how best to retain valuable employees, plan for their eventual succession, and ensure continuity of needed skills and abilities.
Controls Over Information Processing	A variety of control activities are used in information processing. Examples include edit checks of data entered, accounting for transactions in numerical sequences, comparing file totals with control

	accounts, and controlling access to data, files, and programs. Further guidance on control activities for information processing is provided below under "Control Activities Specific for Information Systems."
Physical Control Over Vulnerable Assets	An agency must establish physical control to secure and safeguard vulnerable assets. Examples include security for and limited access to assets such as cash, securities, inventories, and equipment which might be vulnerable to risk of loss or unauthorized use. Such assets should be periodically counted and compared to control records.
Establishment and Review of Performance Measures and Indicators	Activities need to be established to monitor performance measures and indicators. These controls could call for comparisons and assessments relating different sets of data to one another so that analyses of the relationships can be made and appropriate actions taken. Controls should also be aimed at validating the propriety and integrity of both organizational and individual performance measures and indicators.
Segregation of Duties	Key duties and responsibilities need to be divided or segregated among different people to reduce the risk of error or fraud. This should include separating the responsibilities for authorizing transactions, processing and recording them, reviewing the transactions, and handling any related assets. No one individual should control all key aspects of a transaction or event.
Proper Execution of Transactions and Events	Transactions and other significant events should be authorized and executed only by persons acting within the scope of their authority. This is the principal means of assuring that only valid transactions to exchange, transfer, use, or commit resources and other events are initiated or entered

	into. Authorizations should be clearly communicated to managers and employees.
Accurate and Timely Recording of Transactions and Events	Transactions should be promptly recorded to maintain their relevance and value to management in controlling operations and making decisions. This applies to the entire process or life cycle of a transaction or event from the initiation and authorization through its final classification in summary records. In addition, control activities help to ensure that all transactions are completely and accurately recorded.
Access Restrictions to and Accountability for Resources and Records	Access to resources and records should be limited to authorized individuals, and accountability for their custody and use should be assigned and maintained. Periodic comparison of resources with the recorded accountability should be made to help reduce the risk of errors, fraud, misuse, or unauthorized alteration.
Appropriate Documentation of Transactions and Internal Control	Internal control and all transactions and other significant events need to be clearly documented, and the documentation should be readily available for examination. The documentation should appear in management directives, administrative policies, or operating manuals and may be in paper or electronic form. All documentation and records should be properly managed and maintained.

These examples are meant only to illustrate the range and variety of control activities that may be useful to agency managers. They are not all-inclusive and may not include particular control activities that an agency may need.

Furthermore, an agency's internal control should be flexible to allow agencies to tailor control activities to fit their special needs. The specific control activities used by a given agency may be different from those

used by others due to a number of factors. These could include specific threats they face and risks they incur; differences in objectives; managerial judgment; size and complexity of the organization; operational environment; sensitivity and value of data; and requirements for system reliability, availability, and performance.

Control Activities Specific for Information Systems

- General Control
- Application Control

There are two broad groupings of information systems control - general control and application control. General control applies to all information systems—mainframe, minicomputer, network, and end-user environments. Application control is designed to cover the processing of data within the application software.

General Control

This category includes entitywide security program planning, management, control over data center operations, system software acquisition and maintenance, access security, and application system development and maintenance. More specifically:

- Data center and client-server operations controls include backup and recovery procedures, and contingency and disaster planning. In addition, data center operations controls also include job set-up and scheduling procedures and controls over operator activities.

- System software control includes control over the acquisition, implementation, and maintenance of all system software including the operating system, data-based management systems, telecommunications, security software, and utility programs.
- Access security control protects the systems and network from inappropriate access and unauthorized use by hackers and other trespassers or inappropriate use by agency personnel. Specific control activities include frequent changes of dial-up numbers; use of dial-back access; restrictions on users to allow access only to system functions that they need; software and hardware "firewalls" to restrict access to assets, computers, and networks by external persons; and frequent changes of passwords and deactivation of former employees' passwords.
- Application system development and maintenance control provides the structure for safely developing new systems and modifying existing systems. Included are documentation requirements; authorizations for undertaking projects; and reviews, testing, and approvals of development and modification activities before placing systems into operation. An alternative to in-house development is the procurement of commercial software, but control is necessary to ensure that selected software meets the user's needs, and that it is properly placed into operation.

Application Control

This category of control is designed to help ensure completeness, accuracy, authorization, and validity of all transactions during application processing. Control should be installed at an application's interfaces with other systems to ensure that all inputs are received and are valid and outputs are correct and properly distributed. An example is computerized edit checks built into the system to review the format, existence, and reasonableness of data.

General and application control over computer systems are interrelated. General control supports the functioning of application control, and both are needed to ensure complete and accurate information processing. If the general control is inadequate, the application control is unlikely to function properly and could be overridden.

Because information technology changes rapidly, controls must evolve to remain effective. Changes in technology and its application to electronic commerce and expanding Internet applications will change the specific control activities that may be employed and how they are implemented, but the basic requirements of control will not have changed. As more powerful computers place more responsibility for data processing in the hands of the end users, the needed controls should be identified and implemented.

Information and Communications

Information should be recorded and communicated to management and others within the entity who need it and in a form and within a time frame that enables them to carry out their internal control and other responsibilities.

For an entity to run and control its operations, it must have relevant, reliable, and timely communications relating to internal as well as external events. Information is needed throughout the agency to achieve all of its objectives.

Program managers need both operational and financial data to determine whether they are meeting their agencies' strategic and annual performance plans and meeting their goals for accountability for effective and efficient use of resources. For example, operating information is required for development of financial reports. This covers a broad range of data from purchases, subsidies, and other transactions to data on fixed assets, inventories, and receivables. Operating information is also needed to determine whether the agency is achieving its compliance requirements under various laws and regulations. Financial information is needed for both external and internal uses. It is required to develop financial statements for periodic external reporting, and, on a day-to-day basis, to make operating decisions, montinor performance, and allocate resources. Pertinent information should be identified, captured, and distributed in a form and time frame that permits people to perform their duties efficiently.

Effective communications should occur in a broad sense with information flowing down, across, and up the organization. In additional to internal communications, management should ensure there are adequate means of communicating with, and obtaining information from, external stakeholders that may have a significant impact on the agency achieving its goals. Moreover, effective information technology management is critical to achieving useful, reliable, and continuous recording and communication of information.

Monitoring

Internal control monitoring should assess the quality of performance over time and ensure that the findings of audits and other reviews are promptly resolved.

Internal control should generally be designed to assure that ongoing monitoring occurs in the course of normal operations. It is performed continually and is ingrained in the agency's operations. It includes regular management and supervisory activities, comparisons, reconciliations, and other actions people take in performing their duties.

Separate evaluations of control can also be useful by focusing directly on the controls' effectiveness at a specific time. The scope and frequency of separate evaluations should depend primarily on the assessment of risks and the effectiveness of ongoing monitoring procedures. Separate evaluations may take the form of self-assessments as well as review of control design and direct testing of internal control. Separate evaluations also may be performed by the agency Inspector General or an external auditor. Deficiencies found during ongoing monitoring or through separate evaluations should be communicated to the individual responsible for the function and also to at least one level of management above that individual. Serious matters should be reported to top management.

Monitoring of internal control should include policies and procedures for ensuring that the findings of audits and other reviews are promptly resolved. Managers are to (1) promptly evaluate findings from

audits and other reviews, including those showing deficiencies and recommendations reported by auditors and others who evaluate agencies' operations, (2) determine proper actions in response to findings and recommendations from audits and reviews, and (3) complete, within established time frames, all actions that correct or otherwise resolve the matters brought to management's attention. The resolution process begins when audit or other review results are reported to management, and is completed only after action has been taken that (1) corrects identified deficiencies, (2) produces improvements, or (3) demonstrates the findings and recommendations do not warrant management action.

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th & G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to: info@www.gao.gov

or visit GAO's World Wide Web Home Page at: http://www.gao.gov

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Correction Requested

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100

United States Government Accountability Office

GAO

By the Comptroller General of the United States

December 2011

Government Auditing Standards

2011 Revision

GAO-12-331G

United States Government Accountability Office

GAO

By the Comptroller General of the United States

December 2011

Government Auditing Standards

2011 Revision

The 2011 revision of Government Auditing Standards supersedes the 2007 revision. The 2011 revision should be used by government auditors until further updates and revisions are made. An electronic version of this document can be accessed on GAO's Yellow Book Web page at http://www.gao.gov/yellowbook.

The 2011 revision of Government Auditing Standards is effective for financial audits and attestation engagements for periods ending on or after December 15, 2012, and for performance audits beginning on or after December 15, 2011. Early implementation is not permitted.

Revised on January 20, 2012, to correct a typo in paragraph 7.19.

GAO-12-331G

Contents

Abbreviations

AICPA	American Institute of Certified Public Accountants
AU-C	AICPA *Codification of Statements on Auditing Standards for Auditing*
AT	AICPA *Codification of Statements on Standards for Attestation Engagements*
CPA	certified public accountants
CPE	continuing professional education
COSO	Committee of Sponsoring Organizations of the Treadway Commission
ERISA	Employee Retirement Income Security Act
FISCAM	*Federal Information System Controls Audit Manual*
GAAP	generally accepted accounting principles
GAGAS	generally accepted government auditing standards
GAO	Government Accountability Office
IT	information technology
IAASB	International Auditing and Assurance Standards Board
IIA	Institute of Internal Auditors
ISAE	International Standards on Assurance Engagements
ISA	International Standards on Auditing
MD&A	management's discussion and analysis
OMB	Office of Management and Budget
PCAOB	Public Company Accounting Oversight Board
SAS	Statements on Auditing Standards
SSAE	Statements on Standards for Attestation Engagements

Audits provide essential accountability and transparency over government programs. Given the current challenges facing governments and their programs, the oversight provided through auditing is more critical than ever. Government auditing provides objective analysis and information needed to make the decisions necessary to help create a better future. The professional standards presented in this 2011 revision of Government Auditing Standards provide a framework for performing high-quality audit work with competence, integrity, objectivity, and independence to provide accountability and to help improve government operations and services. These standards provide the foundation for government auditors to lead by example in the areas of independence, transparency, accountability, and quality through the audit process.

The 2011 revision of Government Auditing Standards represents a modernized version of the standards, taking into account recent changes in other auditing standards, including international standards. This revision supersedes the 2007 revision. It contains the following major changes from the 2007 revision that reinforce the principles of transparency and accountability and provide the framework for high-quality government audits that add value.

- A conceptual framework for independence was added to provide a means for auditors to assess their independence for activities that are not expressly prohibited in the standards. This more principles-based approach to analyzing independence provides the framework for auditors to assess the unique facts and circumstances that arise during their work.

- This revision drops discussion surrounding certain AICPA Statements on Auditing Standards (SAS) and

Statements on Standards for Attestation Engagements (SSAE) requirements that were incorporated by reference and included in the 2007 revision, as the standards have converged in those areas.

- The definition of validity as an aspect of the quality of evidence has been clarified for performance audits.

Effective with the implementation dates for the 2011 revision of Government Auditing Standards, GAO is also retiring Government Auditing Standards: Answers to Independence Standard Questions (GAO-02-870G, July 2002).

This revision of the standards has gone through an extensive deliberative process, including public comments and input from the Comptroller General's Advisory Council on Government Auditing Standards. The Advisory Council generally consists of about 25 experts in financial and performance auditing and reporting drawn from federal, state, and local government; the private sector; and academia. The views of all parties were thoroughly considered in finalizing the standards.

The 2011 revision of Government Auditing Standards will be effective for financial audits and attestation engagements for periods ending on or after December 15, 2012, and for performance audits beginning on or after December 15, 2011. Early implementation is not permitted.

An electronic version of this document and any interpretive publications can be accessed at http://www.gao.gov/yellowbook.

I extend special thanks to the members of the Advisory Council for their extensive input and feedback through the entire process of developing and finalizing the standards.

Gene L. Dodaro
Comptroller General
of the United States

December 2011

Government Auditing: Foundation and Ethical Principles

Introduction

1.01 The concept of accountability for use of public resources and government authority is key to our nation's governing processes. Management and officials entrusted with public resources are responsible for carrying out public functions and providing service to the public effectively, efficiently, economically, ethically, and equitably within the context of the statutory boundaries of the specific government program.

1.02 As reflected in applicable laws, regulations, agreements, and standards, management and officials of government programs are responsible for providing reliable, useful, and timely information for transparency and accountability of these programs and their operations.[1] Legislators, oversight bodies, those charged with governance,[2] and the public need to know whether (1) management and officials manage government resources and use their authority properly and in compliance with laws and regulations; (2) government programs are achieving their objectives and desired outcomes; and (3) government services are provided effectively, efficiently, economically, ethically, and equitably.

1.03 Government auditing is essential in providing accountability to legislators, oversight bodies, those charged with governance, and the public. Audits[3] provide an independent, objective, nonpartisan assessment of the stewardship, performance, or cost of government policies, programs, or operations, depending upon the type and scope of the audit.

[1]See paragraph A1.08 for additional information on management's responsibilities.

[2]See paragraphs A1.05 through A1.07 for additional discussion on the role of those charged with governance.

[3]See paragraph 1.07c for discussion of the term "audit" as it is used in chapters 1 through 3 and corresponding sections of the Appendix.

Purpose and Applicability of GAGAS

1.04 The professional standards and guidance contained in this document, commonly referred to as generally accepted government auditing standards (GAGAS), provide a framework for conducting high quality audits with competence, integrity, objectivity, and independence. These standards are for use by auditors of government entities and entities that receive government awards and audit organizations performing GAGAS audits. Overall, GAGAS contains standards for audits, which are comprised of individual requirements that are identified by terminology as discussed in paragraphs 2.14 through 2.18. GAGAS contains requirements and guidance dealing with ethics, independence, auditors' professional judgment and competence, quality control, performance of the audit, and reporting.

1.05 Audits performed in accordance with GAGAS provide information used for oversight, accountability, transparency, and improvements of government programs and operations. GAGAS contains requirements and guidance to assist auditors in objectively acquiring and evaluating sufficient, appropriate evidence and reporting the results. When auditors perform their work in this manner and comply with GAGAS in reporting the results, their work can lead to improved government management, better decision making and oversight, effective and efficient operations, and accountability and transparency for resources and results.

1.06 Provisions of laws, regulations, contracts, grant agreements, or policies frequently require audits be conducted in accordance with GAGAS. In addition, many auditors and audit organizations voluntarily choose to perform their work in accordance with GAGAS. The requirements and guidance in GAGAS apply to audits of government entities, programs, activities, and functions, and of government assistance administered by contractors, nonprofit entities, and other nongovernmental entities when the use of GAGAS is required or is voluntarily followed.[4]

1.07 This paragraph describes the use of the following terms in GAGAS.

a. The term "auditor" as it is used throughout GAGAS describes individuals performing work in accordance with GAGAS (including audits and attestation engagements) regardless of job title. Therefore, individuals who may have the titles auditor, analyst, practitioner, evaluator, inspector, or other similar titles are considered auditors in GAGAS.

b. The term "audit organization" as it is used throughout GAGAS refers to government audit organizations as well as public accounting or other firms that perform audits and attestation engagements using GAGAS.

c. The term "audit" as it is used in chapters 1 through 3 and corresponding sections of the Appendix refers to financial audits, attestation engagements, and performance audits conducted in accordance with GAGAS.

[4]See paragraphs A1.02 through A1.04 for discussion of laws, regulations, and guidelines that require use of GAGAS.

1.08 A government audit organization can be structurally located within or outside the audited entity.[5] Audit organizations that are external to the audited entity and report to third parties are considered to be external audit organizations. Audit organizations that are accountable to senior management and those charged with governance of the audited entity, and do not generally issue their reports to third parties external to the audited entity, are considered internal audit organizations.

1.09 Some government audit organizations represent a unique hybrid of external auditing and internal auditing in their oversight role for the entities they audit. These audit organizations have external reporting requirements consistent with the reporting requirements for external auditors while at the same time being part of their respective agencies. These audit organizations often have a dual reporting responsibility to their legislative body as well as to the agency head and management.

Ethical Principles

1.10 The ethical principles presented in this section provide the foundation, discipline, and structure, as well as the climate that influence the application of GAGAS. This section sets forth fundamental principles rather than establishing specific standards or requirements.

1.11 Because auditing is essential to government accountability to the public, the public expects audit organizations and auditors who conduct their work in accordance with GAGAS to follow ethical principles. Management of the audit organization sets the tone for

[5]See paragraph 1.19 for a discussion of objectivity and paragraphs 3.27 through 3.32 for requirements related to independence considerations for government auditors and audit organization structure.

ethical behavior throughout the organization by maintaining an ethical culture, clearly communicating acceptable behavior and expectations to each employee, and creating an environment that reinforces and encourages ethical behavior throughout all levels of the organization. The ethical tone maintained and demonstrated by management and staff is an essential element of a positive ethical environment for the audit organization.

1.12 Conducting audit work in accordance with ethical principles is a matter of personal and organizational responsibility. Ethical principles apply in preserving auditor independence,[6] taking on only work that the audit organization is competent[7] to perform, performing high-quality work, and following the applicable standards cited in the auditors' report. Integrity and objectivity are maintained when auditors perform their work and make decisions that are consistent with the broader interest of those relying on the auditors' report, including the public.

1.13 Other ethical requirements or codes of professional conduct may also be applicable to auditors who conduct audits in accordance with GAGAS. For example, individual auditors who are members of professional organizations or are licensed or certified professionals may also be subject to ethical requirements of those professional organizations or licensing bodies. Auditors employed by government entities may also be subject to government ethics laws and regulations.

[6]See paragraphs 3.02 through 3.59 for requirements related to independence.

[7]See paragraphs 3.69 through 3.81 for additional information on competence.

1.14 The ethical principles that guide the work of auditors who conduct audits in accordance with GAGAS are

a. the public interest;

b. integrity;

c. objectivity;

d. proper use of government information, resources, and positions; and

e. professional behavior.

The Public Interest

1.15 The public interest is defined as the collective well-being of the community of people and entities the auditors serve. Observing integrity, objectivity, and independence in discharging their professional responsibilities assists auditors in meeting the principle of serving the public interest and honoring the public trust. The principle of the public interest is fundamental to the responsibilities of auditors and critical in the government environment.

1.16 A distinguishing mark of an auditor is acceptance of responsibility to serve the public interest. This responsibility is critical when auditing in the government environment. GAGAS embodies the concept of accountability for public resources, which is fundamental to serving the public interest.

Integrity

1.17 Public confidence in government is maintained and strengthened by auditors performing their professional responsibilities with integrity. Integrity includes auditors conducting their work with an attitude that is objective, fact-based, nonpartisan, and nonideological with regard

to audited entities and users of the auditors' reports. Within the constraints of applicable confidentiality laws, rules, or policies, communications with the audited entity, those charged with governance, and the individuals contracting for or requesting the audit are expected to be honest, candid, and constructive.

1.18 Making decisions consistent with the public interest of the program or activity under audit is an important part of the principle of integrity. In discharging their professional responsibilities, auditors may encounter conflicting pressures from management of the audited entity, various levels of government, and other likely users. Auditors may also encounter pressures to inappropriately achieve personal or organizational gain. In resolving those conflicts and pressures, acting with integrity means that auditors place priority on their responsibilities to the public interest.

Objectivity

1.19 The credibility of auditing in the government sector is based on auditors' objectivity in discharging their professional responsibilities. Objectivity includes independence of mind and appearance when providing audits, maintaining an attitude of impartiality, having intellectual honesty, and being free of conflicts of interest. Maintaining objectivity includes a continuing assessment of relationships with audited entities and other stakeholders in the context of the auditors' responsibility to the public. The concepts of objectivity and independence are closely related. Independence impairments impact objectivity.[8]

[8]See independence standards at paragraphs 3.02 through 3.59.

Proper Use of Government Information, Resources, and Positions

1.20 Government information, resources, and positions are to be used for official purposes and not inappropriately for the auditor's personal gain or in a manner contrary to law or detrimental to the legitimate interests of the audited entity or the audit organization. This concept includes the proper handling of sensitive or classified information or resources.

1.21 In the government environment, the public's right to the transparency of government information has to be balanced with the proper use of that information. In addition, many government programs are subject to laws and regulations dealing with the disclosure of information. To accomplish this balance, exercising discretion in the use of information acquired in the course of auditors' duties is an important part in achieving this goal. Improperly disclosing any such information to third parties is not an acceptable practice.

1.22 Accountability to the public for the proper use and prudent management of government resources is an essential part of auditors' responsibilities. Protecting and conserving government resources and using them appropriately for authorized activities is an important element in the public's expectations for auditors.

1.23 Misusing the position of an auditor for financial gain or other benefits violates an auditor's fundamental responsibilities. An auditor's credibility can be damaged by actions that could be perceived by an objective third party with knowledge of the relevant information as improperly benefiting an auditor's personal financial interests or those of an immediate or close family member; a general partner; an organization for which the auditor serves as an officer, director, trustee, or employee; or an organization with which the auditor is negotiating concerning future employment.

Professional Behavior

1.24 High expectations for the auditing profession include compliance with all relevant legal, regulatory, and professional obligations and avoidance of any conduct that might bring discredit to auditors' work, including actions that would cause an objective third party with knowledge of the relevant information to conclude that the auditors' work was professionally deficient. Professional behavior includes auditors putting forth an honest effort in performance of their duties and professional services in accordance with the relevant technical and professional standards.

Standards for Use and Application of GAGAS

Introduction

2.01 This chapter establishes requirements and provides guidance for audits[9] performed in accordance with generally accepted government auditing standards (GAGAS). This chapter also identifies the types of audits that may be performed in accordance with GAGAS, explains the terminology that GAGAS uses to identify requirements, explains the relationship between GAGAS and other professional standards, and provides requirements for stating compliance with GAGAS in the auditors' report.

Types of GAGAS Audits and Attestation Engagements

2.02 This section describes the types of audits that audit organizations may perform in accordance with GAGAS. This description is not intended to limit or require the types of audits that may be performed in accordance with GAGAS.

2.03 All audits begin with objectives, and those objectives determine the type of audit to be performed and the applicable standards to be followed. The types of audits that are covered by GAGAS, as defined by their objectives, are classified in this document as financial audits, attestation engagements, and performance audits.

2.04 In some audits, the standards applicable to the specific objective will be apparent. For example, if the objective is to express an opinion on financial statements, the standards for financial audits apply. However, some audits may have multiple or overlapping objectives. For example, if the objectives are to determine the reliability of performance measures, this work can be done in accordance with either the standards for attestation engagements or performance

[9]See paragraph 1.07c for discussion of the term "audit" as it is used in chapters 1 through 3 and corresponding sections of the Appendix.

audits. In cases in which there is a choice between applicable standards, auditors should evaluate users' needs and the auditors' knowledge, skills, and experience in deciding which standards to follow.

2.05 GAGAS requirements apply to the types of audits that may be performed in accordance with GAGAS as follows:

a. Financial audits: the requirements and guidance in chapters 1 through 4 apply.

b. Attestation engagements: the requirements and guidance in chapters 1 through 3, and 5 apply.

c. Performance audits: the requirements and guidance in chapters 1 through 3, 6, and 7 apply.

2.06 Appendix I includes supplemental guidance for auditors and audited entities to assist in the implementation of GAGAS. Appendix I does not establish auditor requirements but instead is intended to facilitate implementation of the standards contained in chapters 2 through 7. Appendix II includes a flowchart which may assist in the application of the conceptual framework for independence.[10]

Financial Audits

2.07 Financial audits provide an independent assessment of whether an entity's reported financial information (e.g., financial condition, results, and use of resources) are presented fairly in accordance with recognized criteria. Financial audits performed in accordance with GAGAS include financial statement audits and other related financial audits:

[10]See paragraphs 3.07 through 3.32 for discussion of the conceptual framework.

a. Financial statement audits: The primary purpose of a financial statement audit is to provide an opinion about whether an entity's financial statements are presented fairly in all material respects in conformity with an applicable financial reporting framework. Reporting on financial statement audits performed in accordance with GAGAS also includes reports on internal control over financial reporting and on compliance with provisions of laws, regulations, contracts, and grant agreements that have a material effect on the financial statements.

b. Other types of financial audits: Other types of financial audits conducted in accordance with GAGAS entail various scopes of work, including: (1) obtaining sufficient, appropriate evidence to form an opinion on single financial statements, specified elements, accounts, or items of a financial statement;[11] (2) issuing letters for underwriters and certain other requesting parties;[12] and (3) auditing compliance with applicable compliance requirements relating to one or more government programs.[13]

2.08 GAGAS incorporates by reference the American Institute of Certified Public Accountants (AICPA)

[11]See American Institute of Certified Public Accountants (AICPA) *Codification of Statements on Auditing Standards* for Auditing (AU-C) Section 805, *Special Considerations – Audits of Single Financial Statements and Specific Elements, Accounts, or Items of a Financial Statement*.

[12]See AICPA AU-C Section 920, *Letters for Underwriters and Certain Other Requesting Parties.*

[13]See AICPA AU-C Section 935, *Compliance Audits.*

Statements on Auditing Standards (SAS).[14] Additional requirements for performing financial audits in accordance with GAGAS are contained in chapter 4. For financial audits performed in accordance with GAGAS, auditors should also comply with chapters 1 through 3.

Attestation Engagements

2.09 Attestation engagements can cover a broad range of financial or nonfinancial objectives about the subject matter or assertion depending on the users' needs.[15] GAGAS incorporates by reference the AICPA's Statements on Standards for Attestation Engagements (SSAE).[16] Additional requirements for performing attestation engagements in accordance with GAGAS are contained in chapter 5. The AICPA's standards recognize attestation engagements that result in an examination, a review, or an agreed-upon procedures report on a subject matter or on an assertion about a subject matter that is the responsibility of another party.[17] The three types of attestation engagements are:

a. Examination: Consists of obtaining sufficient, appropriate evidence to express an opinion on whether the subject matter is based on (or in conformity with) the

[14]See AICPA *Codification of Statements on Auditing Standards* and paragraph 2.20 for additional discussion on the relationship between GAGAS and other professional standards. References to the AICPA *Codification of Statements on Auditing Standards* use an "AU-C" identifier to refer to the clarified SASs instead of an "AU" identifier. "AU-C" is a temporary identifier to avoid confusion with references to existing "AU" sections, which remain effective through 2013. The "AU-C" identifier will revert to "AU" in 2014 AICPA *Codification of Statements on Auditing Standards*, by which time the clarified SASs become fully effective for all engagements.

[15]See A2.01 for examples of objectives for attestation engagements.

[16]See the AICPA *Codification of Statements on Standards for Attestation Engagements* (AT) Sections.

[17]See AICPA AT Section 101, *Attest Engagements* and AT Section 201, *Agreed-Upon Procedures Engagements*.

criteria in all material respects or the assertion is presented (or fairly stated), in all material respects, based on the criteria.

b. Review: Consists of sufficient testing to express a conclusion about whether any information came to the auditors' attention on the basis of the work performed that indicates the subject matter is not based on (or not in conformity with) the criteria or the assertion is not presented (or not fairly stated) in all material respects based on the criteria. Auditors should not perform review-level work for reporting on internal control or compliance with provisions of laws and regulations.[18]

c. Agreed-Upon Procedures: Consists of auditors performing specific procedures on the subject matter and issuing a report of findings based on the agreed-upon procedures. In an agreed-upon procedures engagement, the auditor does not express an opinion or conclusion, but only reports on agreed-upon procedures in the form of procedures and findings related to the specific procedures applied.

Performance Audits

2.10 Performance audits are defined as audits that provide findings or conclusions based on an evaluation of sufficient, appropriate evidence against criteria.[19] Performance audits provide objective analysis to assist management and those charged with governance and oversight in using the information to improve program performance and operations, reduce costs, facilitate decision making by parties with responsibility to oversee or initiate corrective action, and contribute to public accountability. The term "program" is used in

[18]See AICPA AT Sections 501, *Reporting on an Entity's Internal Control Over Financial Reporting* and 601, *Compliance Attestation.*

[19]See paragraphs 6.37 and A6.02 for discussion of criteria.

GAGAS to include government entities, organizations, programs, activities, and functions.

2.11 Performance audit objectives vary widely and include assessments of program effectiveness, economy, and efficiency; internal control; compliance; and prospective analyses. These overall objectives are not mutually exclusive. Thus, a performance audit may have more than one overall objective. For example, a performance audit with an objective of determining or evaluating program effectiveness may also involve an additional objective of evaluating internal controls to determine the reasons for a program's lack of effectiveness or how effectiveness can be improved. Examples of the various types of the performance audit objectives discussed below are included in Appendix I.[20]

a. Program effectiveness and results audit objectives are frequently interrelated with economy and efficiency objectives. Audit objectives that focus on program effectiveness and results typically measure the extent to which a program is achieving its goals and objectives. Audit objectives that focus on economy and efficiency address the costs and resources used to achieve program results.

b. Internal control audit objectives relate to an assessment of one or more components of an organization's system of internal control that is designed to provide reasonable assurance of achieving effective and efficient operations, reliable financial and performance reporting, or compliance with applicable laws and regulations. Internal control objectives also may be relevant when determining the cause of unsatisfactory program performance. Internal control

[20]See paragraphs A2.02 through A2.05 for discussion of performance audit objectives.

comprises the plans, policies, methods, and procedures used to meet the organization's mission, goals, and objectives. Internal control includes the processes and procedures for planning, organizing, directing, and controlling program operations, and management's system for measuring, reporting, and monitoring program performance.[21]

c. Compliance audit objectives relate to an assessment of compliance with criteria established by provisions of laws, regulations, contracts, or grant agreements, or other requirements that could affect the acquisition, protection, use, and disposition of the entity's resources and the quantity, quality, timeliness, and cost of services the entity produces and delivers. Compliance requirements can be either financial or nonfinancial.

d. Prospective analysis audit objectives provide analysis or conclusions about information that is based on assumptions about events that may occur in the future, along with possible actions that the entity may take in response to the future events.

Nonaudit Services Provided by Audit Organizations

2.12 GAGAS does not cover nonaudit services, which are defined as professional services other than audits or attestation engagements. Therefore, auditors do not report that the nonaudit services were conducted in accordance with GAGAS. When performing nonaudit services for an entity for which the audit organization performs a GAGAS audit, audit organizations should communicate with requestors and those charged with governance to clarify that the work performed does not constitute an audit conducted in accordance with GAGAS.

[21]See paragraphs A.03 through A.04 for additional discussion of internal control.

2.13 When audit organizations provide nonaudit services to entities for which they also provide GAGAS audits, they should assess the impact that providing those nonaudit services may have on auditor and audit organization independence and respond to any identified threats to independence in accordance with the GAGAS independence standard.[22]

Use of Terminology to Define GAGAS Requirements

2.14 GAGAS contains requirements together with related guidance in the form of application and other explanatory material. The terminology is consistent with the terminology defined in the AICPA's *Codification of Statements on Auditing Standards*.[23] Auditors have a responsibility to consider the entire text of GAGAS in carrying out their work and in understanding and applying the requirements in GAGAS. Not every paragraph of GAGAS carries a requirement that auditors and audit organizations are expected to fulfill. Rather, the requirements are identified through use of specific language.

2.15 GAGAS uses two categories of requirements, identified by specific terms, to describe the degree of responsibility they impose on auditors and audit organizations, as follows:

a. Unconditional requirements: Auditors and audit organizations must comply with an unconditional requirement in all cases where such requirement is relevant. GAGAS uses the word *must* to indicate an unconditional requirement.

[22]See paragraphs 3.02 through 3.59 for the GAGAS independence standard.

[23]See AICPA AU-C Section 200, *Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance With Generally Accepted Auditing Standards*.

b. Presumptively mandatory requirements: Auditors and audit organizations must comply with a presumptively mandatory requirement in all cases where such a requirement is relevant except in rare circumstances discussed in paragraph 2.16. GAGAS uses the word *should* to indicate a presumptively mandatory requirement.[24]

2.16 In rare circumstances, auditors and audit organizations may determine it necessary to depart from a relevant presumptively mandatory requirement. In such rare circumstances, auditors should perform alternative procedures to achieve the intent of that requirement. The need for the auditors to depart from a relevant presumptively mandatory requirement is expected to arise only when the requirement is for a specific procedure to be performed and, in the specific circumstances of the audit, that procedure would be ineffective in achieving the intent of the requirement. If, in rare circumstances, auditors judge it necessary to depart from a relevant presumptively mandatory requirement, they must document their justification for the departure and how the alternative procedures performed in the circumstances were sufficient to achieve the intent of that requirement.

2.17 In addition to requirements as identified in paragraph 2.15, GAGAS contains related guidance in the form of application and other explanatory material. The application and other explanatory material provides further explanation of the requirements and guidance for carrying them out. In particular, it may explain more precisely what a requirement means or is intended to cover or include examples of procedures that may be appropriate in the circumstances. Although such guidance does not in itself impose a requirement, it is

[24]See paragraph 2.25 for additional documentation requirements for departures from GAGAS requirements.

relevant to the proper application of the requirements. Auditors should have an understanding of the application and other explanatory material; how auditors apply the guidance in the audit depends on the exercise of professional judgment in the circumstances consistent with the objective of the requirement. The words "may," "might," and "could" are used to describe these actions and procedures. The application and other explanatory material may also provide background information on matters addressed in GAGAS.

2.18 Auditors also use "interpretive publications" in planning and performing GAGAS audits. Interpretive publications are recommendations on the application of GAGAS in specific circumstances, including audits for entities in specialized industries. Interpretive publications, such as related GAGAS guidance documents and interpretations, are issued under the authority of the Government Accountability Office (GAO) to provide additional guidance on the application of GAGAS.[25] Interpretive publications are not auditing standards, but have the same level of authority as application and other explanatory material in GAGAS.

Relationship between GAGAS and Other Professional Standards

2.19 Auditors may use GAGAS in conjunction with professional standards issued by other authoritative bodies.

2.20 The relationship between GAGAS and other professional standards for financial audits and attestation engagements is as follows:

[25]See http://www.gao.gov/yellowbook for a listing of related GAGAS interpretive publications.

a. The AICPA has established professional standards that apply to financial audits and attestation engagements for nonissuers (entities other than issuers[26] under the Sarbanes-Oxley Act of 2002, such as privately held companies, nonprofit entities, and government entities) performed by certified public accountants (CPA). For financial audits and attestation engagements, GAGAS incorporates by reference AICPA standards, as discussed in paragraph 2.08.

b. The International Auditing and Assurance Standards Board (IAASB) has established professional standards that apply to financial audits and assurance engagements. Auditors may elect to use the IAASB standards and the related International Standards on Auditing (ISA) and International Standards on Assurance Engagements (ISAE) in conjunction with GAGAS.

c. The Public Company Accounting Oversight Board (PCAOB) has established professional standards that apply to financial audits and attestation engagements for issuers (generally, publicly traded companies with a reporting obligation under the Securities Exchange Act of 1934). Auditors may elect to use the PCAOB standards in conjunction with GAGAS.

2.21 For performance audits, GAGAS does not incorporate other standards by reference, but recognizes that auditors may use or may be required to use other professional standards in conjunction with GAGAS, such as the following:

[26]See the Sarbanes-Oxley Act of 2002 (Public Law 107-204) for discussion of issuers.

a. *International Standards for the Professional Practice of Internal Auditing*, The Institute of Internal Auditors, Inc.;

b. *Guiding Principles for Evaluators*, American Evaluation Association;

c. *The Program Evaluation Standards*, Joint Committee on Standards for Education Evaluation;

d. *Standards for Educational and Psychological Testing*, American Psychological Association; and

e. *IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals*, ISACA.

2.22 When auditors cite compliance with both GAGAS and another set of standards, such as those listed in paragraphs 2.20 and 2.21, auditors should refer to paragraph 2.24 for the requirements for citing compliance with GAGAS. In addition to citing GAGAS, auditors may also cite the use of other standards in their reports when they have also met the requirements for citing compliance with the other standards.[27] Auditors should refer to the other set of standards for the basis for citing compliance with those standards.

Stating Compliance with GAGAS in the Auditors' Report

2.23 When auditors are required to perform an audit in accordance with GAGAS or are representing to others that they did so, they should cite compliance with GAGAS in the auditors' report as set forth in paragraphs 2.24 through 2.25.

[27]See paragraphs 4.18, 5.19, 5.51, and 5.61 for additional requirements for citing compliance with standards of the AICPA.

2.24 Auditors should include one of the following types of GAGAS compliance statements in reports on GAGAS audits, as appropriate.[28]

a. Unmodified GAGAS compliance statement: Stating that the auditor performed the audit in accordance with GAGAS. Auditors should include an unmodified GAGAS compliance statement in the auditors' report when they have (1) followed unconditional and applicable presumptively mandatory GAGAS requirements, or (2) have followed unconditional requirements, and documented justification for any departures from applicable presumptively mandatory requirements and have achieved the objectives of those requirements through other means.

b. Modified GAGAS compliance statement: Stating either that (1) the auditor performed the audit in accordance with GAGAS, except for specific applicable requirements that were not followed, or (2) because of the significance of the departure(s) from the requirements, the auditor was unable to and did not perform the audit in accordance with GAGAS. Situations when auditors use modified compliance statements also include scope limitations, such as restrictions on access to records, government officials, or other individuals needed to conduct the audit. When auditors use a modified GAGAS statement, they should disclose in the report the applicable requirement(s) not followed, the reasons for not following the requirement(s), and how not following the requirement(s) affected, or could have affected, the audit and the assurance provided.

[28]See paragraph A2.06 for additional discussion of GAGAS compliance statements.

2.25 When auditors do not comply with applicable requirement(s), they should (1) assess the significance of the noncompliance to the audit objectives, (2) document the assessment, along with their reasons for not following the requirement(s), and (3) determine the type of GAGAS compliance statement. The auditors' determination is a matter of professional judgment, which is affected by the significance of the requirement(s) not followed in relation to the audit objectives.

General Standards

Introduction

3.01 This chapter establishes general standards and provides guidance for performing financial audits, attestation engagements, and performance audits under generally accepted government auditing standards (GAGAS). These general standards, along with the overarching ethical principles presented in chapter 1, establish a foundation for the credibility of auditors' work. These general standards emphasize the importance of the independence of the audit organization and its individual auditors; the exercise of professional judgment in the performance of work and the preparation of related reports; the competence of staff; and quality control and assurance.

Independence

3.02 In all matters relating to the audit work, the audit organization and the individual auditor, whether government or public, must be independent.

3.03 Independence comprises:

a. Independence of Mind
The state of mind that permits the performance of an audit without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism.

b. Independence in Appearance
The absence of circumstances that would cause a reasonable and informed third party, having knowledge of the relevant information, to reasonably conclude that the integrity, objectivity, or professional skepticism of an audit organization or member of the audit team had been compromised.

3.04 Auditors and audit organizations maintain independence so that their opinions, findings,

conclusions, judgments, and recommendations will be impartial and viewed as impartial by reasonable and informed third parties. Auditors should avoid situations that could lead reasonable and informed third parties to conclude that the auditors are not independent and thus are not capable of exercising objective and impartial judgment on all issues associated with conducting the audit and reporting on the work.

3.05 Except under the limited circumstances discussed in paragraphs 3.47 and 3.48, auditors should be independent from an audited entity during:

a. any period of time that falls within the period covered by the financial statements or subject matter of the audit, and

b. the period of the professional engagement, which begins when the auditors either sign an initial engagement letter or other agreement to perform an audit or begin to perform an audit, whichever is earlier. The period lasts for the entire duration of the professional relationship (which, for recurring audits, could cover many periods) and ends with the formal or informal notification, either by the auditors or the audited entity, of the termination of the professional relationship or by the issuance of a report, whichever is later. Accordingly, the period of professional engagement does not necessarily end with the issuance of a report and recommence with the beginning of the following year's audit or a subsequent audit with a similar objective.

3.06 GAGAS's practical consideration of independence consists of four interrelated sections, providing:

a. a conceptual framework for making independence determinations based on facts and circumstances that are often unique to specific environments;

b. requirements for and guidance on independence for audit organizations that are structurally located within the entities they audit;

c. requirements for and guidance on independence for auditors performing nonaudit services, including indication of specific nonaudit services that always impair independence and others that would not normally impair independence; and

d. requirements for and guidance on documentation necessary to support adequate consideration of auditor independence.

GAGAS Conceptual Framework Approach to Independence

3.07 Many different circumstances, or combinations of circumstances, are relevant in evaluating threats to independence. Therefore, GAGAS establishes a conceptual framework that auditors use to identify, evaluate, and apply safeguards to address threats to independence.[29] The conceptual framework assists auditors in maintaining both independence of mind and independence in appearance. It can be applied to many variations in circumstances that create threats to independence and allows auditors to address threats to independence that result from activities that are not specifically prohibited by GAGAS.

3.08 Auditors should apply the conceptual framework at the audit organization, audit, and individual auditor levels to:

a. identify threats to independence;

[29]See Appendix II for a flowchart to assist in the application of the conceptual framework for independence.

b. evaluate the significance of the threats identified, both individually and in the aggregate; and

c. apply safeguards as necessary to eliminate the threats or reduce them to an acceptable level.

3.09 If no safeguards are available to eliminate an unacceptable threat or reduce it to an acceptable level, independence would be considered impaired.

3.10 The use of the term “audit organization” in GAGAS is described in paragraph 1.07. For consideration of auditor independence, offices or units of an audit organization, or related or affiliated entities under common control, are not differentiated from one another. Consequently, for the purposes of independence evaluation using the conceptual framework, an audit organization that includes multiple offices or units, or includes multiple entities related or affiliated through common control, is considered to be one audit organization. Common ownership may also affect independence in appearance regardless of the level of control.

3.11 The GAGAS section on nonaudit services in paragraphs 3.33 through 3.58 provides requirements and guidance on evaluating threats to independence related to nonaudit services provided by auditors to audited entities. That section also enumerates specific nonaudit services that always impair auditor independence with respect to audited entities and that auditors are prohibited from providing to audited entities.

3.12 The following sections discuss threats to independence, safeguards or controls to eliminate or reduce threats, and application of the conceptual framework for independence.

Threats

3.13 Threats to independence are circumstances that could impair independence. Whether independence is impaired depends on the nature of the threat, whether the threat is of such significance that it would compromise an auditor's professional judgment or create the appearance that the auditor's professional judgment may be compromised, and on the specific safeguards applied to eliminate the threat or reduce it to an acceptable level. Threats are conditions to be evaluated using the conceptual framework. Threats do not necessarily impair independence.

3.14 Threats to independence may be created by a wide range of relationships and circumstances. Auditors should evaluate the following broad categories of threats to independence when threats are being identified and evaluated:[30]

a. Self-interest threat - the threat that a financial or other interest will inappropriately influence an auditor's judgment or behavior;

b. Self-review threat - the threat that an auditor or audit organization that has provided nonaudit services will not appropriately evaluate the results of previous judgments made or services performed as part of the nonaudit services when forming a judgment significant to an audit;

c. Bias threat - the threat that an auditor will, as a result of political, ideological, social, or other convictions, take a position that is not objective;

d. Familiarity threat - the threat that aspects of a relationship with management or personnel of an

[30]See A3.02 through A3.09 for further discussion and examples of threats.

audited entity, such as a close or long relationship, or that of an immediate or close family member, will lead an auditor to take a position that is not objective;

e. Undue influence threat - the threat that external influences or pressures will impact an auditor's ability to make independent and objective judgments;

f. Management participation threat - the threat that results from an auditor's taking on the role of management or otherwise performing management functions on behalf of the entity undergoing an audit; and

g. Structural threat - the threat that an audit organization's placement within a government entity, in combination with the structure of the government entity being audited, will impact the audit organization's ability to perform work and report results objectively.

3.15 Circumstances that result in a threat to independence in one of the above categories may result in other threats as well. For example, a circumstance resulting in a structural threat to independence may also expose auditors to undue influence and management participation threats.

Safeguards

3.16 Safeguards are controls designed to eliminate or reduce to an acceptable level threats to independence. Under the conceptual framework, the auditor applies safeguards that address the specific facts and circumstances under which threats to independence exist. In some cases, multiple safeguards may be necessary to address a threat. The list of safeguards in this section provides examples that may be effective under certain circumstances. The list cannot provide safeguards for all circumstances. It may, however, provide a starting point for auditors who have identified threats to independence and are considering what

safeguards could eliminate those threats or reduce them to an acceptable level.

3.17 Examples of safeguards include:

a. consulting an independent third party, such as a professional organization, a professional regulatory body, or another auditor;

b. involving another audit organization to perform or reperform part of the audit;

c. having a professional staff member who was not a member of the audit team review the work performed; and

d. removing an individual from an audit team when that individual's financial or other interests or relationships pose a threat to independence.

3.18 Depending on the nature of the audit, an auditor may also be able to place limited reliance on safeguards that the entity has implemented. It is not possible to rely solely on such safeguards to eliminate threats or reduce them to an acceptable level.

3.19 Examples of safeguards within the entity's systems and procedures include:

a. an entity requirement that persons other than management ratify or approve the appointment of an audit organization to perform an audit;

b. internal procedures at the entity that ensure objective choices in commissioning nonaudit services; and

c. a governance structure at the entity that provides appropriate oversight and communications regarding the audit organization's services.

Application of the Conceptual Framework

3.20 Auditors should evaluate threats to independence using the conceptual framework when the facts and circumstances under which the auditors perform their work may create or augment threats to independence. Auditors should evaluate threats both individually and in the aggregate because threats can have a cumulative effect on an auditor's independence.

3.21 Facts and circumstances that create threats to independence can result from events such as the start of a new audit; assignment of new staff to an ongoing audit; and acceptance of a nonaudit service at an audited entity. Many other events can result in threats to independence. Auditors use professional judgment to determine whether the facts and circumstances created by an event warrant use of the conceptual framework. Whenever relevant new information about a threat to independence comes to the attention of the auditor during the audit, the auditor should evaluate the significance of the threat in accordance with the conceptual framework.

3.22 Auditors should determine whether identified threats to independence are at an acceptable level or have been eliminated or reduced to an acceptable level. A threat to independence is not acceptable if it either (a) could impact the auditor's ability to perform an audit without being affected by influences that compromise professional judgment or (b) could expose the auditor or audit organization to circumstances that would cause a reasonable and informed third party to conclude that the integrity, objectivity, or professional skepticism of the audit organization, or a member of the audit team, had been compromised.

3.23 When an auditor identifies threats to independence and, based on an evaluation of those threats, determines that they are not at an acceptable level, the auditor should determine whether appropriate

safeguards are available and can be applied to eliminate the threats or reduce them to an acceptable level. The auditor should exercise professional judgment in making that determination, and should take into account whether both independence of mind and independence in appearance are maintained. The auditor should evaluate both qualitative and quantitative factors when determining the significance of a threat.

3.24 In cases where threats to independence are not at an acceptable level, thereby requiring the application of safeguards, the auditors should document the threats identified and the safeguards applied to eliminate the threats or reduce them to an acceptable level.

3.25 Certain conditions may lead to threats that are so significant that they cannot be eliminated or reduced to an acceptable level through the application of safeguards, resulting in impaired independence. Under such conditions, auditors should decline to perform a prospective audit or terminate an audit in progress.[31]

3.26 If a threat to independence is initially identified after the auditors' report is issued, the auditor should evaluate the threat's impact on the audit and on GAGAS compliance. If the auditors determine that the newly identified threat had an impact on the audit that would have resulted in the auditors' report being different from the report issued had the auditors been aware of it, they should communicate in the same manner as that used to originally distribute the report to those charged with governance, the appropriate officials of the audited entity, the appropriate officials of the

[31]See paragraph 3.44 for a discussion of conditions under which an auditor may be required by law or regulation to perform both an audit and a nonaudit service and cannot decline to perform or terminate the service. See the discussion of nonaudit services beginning in paragraph 3.45 for consideration of threats related to nonaudit services that cannot be eliminated or reduced to an appropriate level.

organizations requiring or arranging for the audits, and other known users, so that they do not continue to rely on findings or conclusions that were impacted by the threat to independence. If the report was previously posted to the auditors' publicly accessible website, the auditors should remove the report and post a public notification that the report was removed. The auditors should then determine whether to conduct additional audit work necessary to reissue the report, including any revised findings or conclusions or repost the original report if the additional audit work does not result in a change in findings or conclusions.

Government Auditors and Audit Organization Structure

3.27 The ability of audit organizations in government entities to perform work and report the results objectively can be affected by placement within government and the structure of the government entity being audited. The independence standard applies to auditors in government entities whether they report to third parties externally (external auditors), to senior management within the audited entity (internal auditors), or to both.

External Auditor Independence

3.28 Audit organizations that are structurally located within government entities are often subject to constitutional or statutory safeguards that mitigate the effects of structural threats to independence. For external audit organizations, such safeguards may include governmental structures under which a government audit organization is:

a. at a level of government other than the one of which the audited entity is part (federal, state, or local); for example, federal auditors auditing a state government program; or

b. placed within a different branch of government from that of the audited entity; for example, legislative auditors auditing an executive branch program.

3.29 Safeguards other than those described above may mitigate threats resulting from governmental structures. For external auditors or auditors who report both externally and internally, structural threats may be mitigated if the head of an audit organization meets any of the following criteria in accordance with constitutional or statutory requirements:

a. directly elected by voters of the jurisdiction being audited;

b. elected or appointed by a legislative body, subject to removal by a legislative body, and reports the results of audits to and is accountable to a legislative body;

c. appointed by someone other than a legislative body, so long as the appointment is confirmed by a legislative body and removal from the position is subject to oversight or approval by a legislative body, and reports the results of audits to and is accountable to a legislative body; or

d. appointed by, accountable to, reports to, and can only be removed by a statutorily created governing body, the majority of whose members are independently elected or appointed and are outside the organization being audited.

3.30 In addition to the criteria in paragraphs 3.28 and 3.29, GAGAS recognizes that there may be other organizational structures under which external audit organizations in government entities could be considered to be independent. If appropriately designed and implemented, these structures provide safeguards that prevent the audited entity from interfering with the

audit organization's ability to perform the work and report the results impartially. For an external audit organization or one that reports both externally and internally to be considered independent under a structure different from the ones listed in paragraphs 3.28 and 3.29, the audit organization should have all of the following safeguards. In such situations, the audit organization should document how each of the following safeguards was satisfied and provide the documentation to those performing quality control monitoring and to the external peer reviewers to determine whether all the necessary safeguards are in place. The following safeguards may also be used to augment those listed in paragraphs 3.28 and 3.29:

a. statutory protections that prevent the audited entity from abolishing the audit organization;

b. statutory protections that require that if the head of the audit organization is removed from office, the head of the agency reports this fact and the reasons for the removal to the legislative body;

c. statutory protections that prevent the audited entity from interfering with the initiation, scope, timing, and completion of any audit;

d. statutory protections that prevent the audited entity from interfering with audit reporting, including the findings and conclusions or the manner, means, or timing of the audit organization's reports;

e. statutory protections that require the audit organization to report to a legislative body or other independent governing body on a recurring basis;

f. statutory protections that give the audit organization sole authority over the selection, retention, advancement, and dismissal of its staff; and

g. statutory access to records and documents related to the agency, program, or function being audited and access to government officials or other individuals as needed to conduct the audit.

Internal Auditor Independence

3.31 Certain entities employ auditors to work for entity management. These auditors may be subject to administrative direction from persons involved in the entity management process. Such audit organizations are internal audit functions and are encouraged to use the Institute of Internal Auditors (IIA) *International Standards for the Professional Practice of Internal Auditing* in conjunction with GAGAS. In accordance with GAGAS, internal auditors who work under the direction of the audited entity's management are considered independent for the purposes of reporting internally if the head of the audit organization meets all of the following criteria:

a. is accountable to the head or deputy head of the government entity or to those charged with governance;

b. reports the audit results both to the head or deputy head of the government entity and to those charged with governance;

c. is located organizationally outside the staff or line-management function of the unit under audit;

d. has access to those charged with governance; and

e. is sufficiently removed from political pressures to conduct audits and report findings, opinions, and conclusions objectively without fear of political reprisal.

3.32 When internal audit organizations perform audits of external parties such as auditing contractors or outside party agreements, and no impairments to independence exist, the audit organization can be

considered independent as an external audit organization of those external parties.

Provision of Nonaudit Services to Audited Entities

3.33 Auditors have traditionally provided a range of nonaudit services that are consistent with their skills and expertise to entities at which they perform audits. Providing such nonaudit services may create threats to an auditor's independence.

Requirements for Performing Nonaudit Services

3.34 Before an auditor agrees to provide a nonaudit service to an audited entity, the auditor should determine whether providing such a service would create a threat to independence, either by itself or in aggregate with other nonaudit services provided, with respect to any GAGAS audit it performs. A critical component of this determination is consideration of management's ability to effectively oversee the nonaudit service to be performed. The auditor should determine that the audited entity has designated an individual who possesses suitable skill, knowledge, or experience, and that the individual understands the services to be performed sufficiently to oversee them. The individual is not required to possess the expertise to perform or reperform the services. The auditor should document consideration of management's ability to effectively oversee nonaudit services to be performed.

3.35 If an auditor were to assume management responsibilities for an audited entity, the management participation threats created would be so significant that no safeguards could reduce them to an acceptable level. Management responsibilities involve leading and directing an entity, including making decisions regarding the acquisition, deployment and control of human, financial, physical, and intangible resources.

3.36 Whether an activity is a management responsibility depends on the facts and circumstances and auditors

exercise professional judgment in identifying these activities. Examples of activities that are considered management responsibilities and would therefore impair independence if performed for an audited entity include:

a. setting policies and strategic direction for the audited entity;

b. directing and accepting responsibility for the actions of the audited entity's employees in the performance of their routine, recurring activities;

c. having custody of an audited entity's assets;

d. reporting to those charged with governance on behalf of management;

e. deciding which of the auditor's or outside third party's recommendations to implement;

f. accepting responsibility for the management of an audited entity's project;

g. accepting responsibility for designing, implementing, or maintaining internal control;

h. providing services that are intended to be used as management's primary basis for making decisions that are significant to the subject matter of the audit;

i. developing an audited entity's performance measurement system when that system is material or significant to the subject matter of the audit; and

j. serving as a voting member of an audited entity's management committee or board of directors.

3.37 Auditors performing nonaudit services for entities for which they perform audits should obtain assurance that audited entity management performs the following functions in connection with the nonaudit services:

a. assumes all management responsibilities;

b. oversees the services, by designating an individual, preferably within senior management, who possess suitable skill, knowledge, or experience;[32]

c. evaluates the adequacy and results of the services performed; and

d. accepts responsibility for the results of the services.

3.38 In cases where the audited entity is unable or unwilling to assume these responsibilities (for example, the audited entity does not have an individual with suitable skill, knowledge, or experience to oversee the nonaudit services provided, or is unwilling to perform such functions due to lack of time or desire), the auditor's provision of these services would impair independence.

3.39 In connection with nonaudit services, auditors should establish and document their understanding with the audited entity's management or those charged with governance, as appropriate, regarding the following:

a. objectives of the nonaudit service;

b. services to be performed;

c. audited entity's acceptance of its responsibilities;

[32]See paragraph 3.34 for additional discussion of management's ability to effectively oversee the nonaudit service.

d. the auditor's responsibilities; and

e. any limitations of the nonaudit service.

3.40 Routine activities performed by auditors that relate directly to the performance of an audit, such as providing advice and responding to questions as part of an audit, are not considered nonaudit services under GAGAS. Such routine activities generally involve providing advice or assistance to the entity on an informal basis as part of an audit. Routine activities typically are insignificant in terms of time incurred or resources expended and generally do not result in a specific project or engagement or in the auditors producing a formal report or other formal work product. However, activities such as financial statement preparation, cash to accrual conversions, and reconciliations are considered nonaudit services under GAGAS, not routine activities related to the performance of an audit, and are evaluated using the conceptual framework as discussed in paragraph 3.46.

3.41 Routine activities directly related to an audit include the following:

a. providing advice to the audited entity on an accounting matter as an ancillary part of the overall financial audit;

b. researching and responding to the audited entity's technical questions on relevant tax laws as an ancillary part of providing tax services;

c. providing advice to the audited entity on routine business matters;

d. educating the audited entity on matters within the technical expertise of the auditors; and

e. providing information to the audited entity that is readily available to the auditors, such as best practices and benchmarking studies.

3.42 An auditor who previously performed nonaudit services for an entity that is a prospective subject of an audit should evaluate the impact of those nonaudit services on independence before accepting an audit. If the nonaudit services were performed in the period to be covered by the audit, the auditor should (1) determine if the nonaudit service is expressly prohibited by GAGAS and, if not, (2) determine whether a threat to independence exists and address any threats noted in accordance with the conceptual framework.

3.43 Nonaudit services provided by auditors can impact independence of mind and in appearance in periods subsequent to the period in which the nonaudit service was provided. For example, if auditors have designed and implemented an accounting and financial reporting system that is expected to be in place for many years, a threat to independence in appearance for future financial audits or attestation engagements performed by those auditors may exist in subsequent periods. For recurring audits, having another independent audit organization perform an audit of the areas affected by the nonaudit service may provide a safeguard that allows the audit organization that provided the nonaudit service to mitigate the threat to its independence. Auditors use professional judgment to determine whether the safeguards adequately mitigate the threats.

3.44 An auditor in a government entity may be required to perform a nonaudit service that could impair the auditor's independence with respect to a required audit. If the auditor cannot, as a consequence of constitutional or statutory requirements over which the auditor has no control, implement safeguards to reduce the resulting

threat to an acceptable level, or decline to perform or terminate a nonaudit service that is incompatible with audit responsibilities, the auditor should disclose the nature of the threat that could not be eliminated or reduced to an acceptable level and modify the GAGAS compliance statement accordingly.[33]

Consideration of Specific Nonaudit Services

3.45 By their nature, certain nonaudit services directly support the entity's operations and impair auditors' ability to maintain independence in mind and appearance. The nonaudit services discussed below are among those frequently requested of auditors working in a government environment. Some aspects of these services will impair an auditor's ability to perform audits for the entities for which the services are provided. The specific services indicated are not the only nonaudit services that would impair an auditor's independence.

3.46 Auditors may be able to provide nonaudit services in the broad areas indicated in paragraphs 3.49 through 3.58 without impairing independence if (1) the nonaudit services are not expressly prohibited, (2) the auditor has determined that the requirements for performing nonaudit services in paragraphs 3.34 through 3.44 have been met, and (3) any significant threats to independence have been eliminated or reduced to an acceptable level through the application of safeguards. Auditors should use the conceptual framework to evaluate independence given the facts and circumstances of individual services not specifically prohibited in this section.

3.47 For performance audits and agreed-upon procedures engagements, nonaudit services that are

[33]See paragraphs 2.24 and 2.25 for the discussion of modifications to the GAGAS compliance statement.

otherwise prohibited by GAGAS may be provided when such services do not relate to the specific subject matter of the engagement.

3.48 For financial statement audits and examination or review engagements, a nonaudit service performed during the period covered by the financial statements may not impair an auditor's independence with respect to those financial statements provided that the following conditions exist:

a. the nonaudit service was provided prior to the period of professional engagement;

b. the nonaudit service related only to periods prior to the period covered by the financial statements; and

c. the financial statements for the period to which the nonaudit service did relate were audited by another auditor (or in the case of an examination or review engagement, examined, reviewed, or audited by another auditor as appropriate).

Management Responsibilities

3.49 If performed on behalf of an audited entity by the entity's auditor, management responsibilities such as those listed in paragraph 3.36 would create management participation threats so significant that no safeguards could reduce them to an acceptable level. Consequently the auditor's independence would be impaired with respect to that entity.

Preparing Accounting Records and Financial Statements

3.50 Some services involving preparation of accounting records always impair an auditor's independence with respect to an audited entity. These services include:

a. determining or changing journal entries, account codes or classifications for transactions, or other accounting records for the entity without obtaining management's approval;

b. authorizing or approving the entity's transactions; and

c. preparing or making changes to source documents without management approval. Source documents include those providing evidence that transactions have occurred (for example, purchase orders, payroll time records, customer orders, and contracts). Such records also include an audited entity's general ledger and subsidiary records or equivalent.

3.51 Management is responsible for the preparation and fair presentation of the financial statements in accordance with the applicable financial reporting framework, even if the auditor assisted in drafting those financial statements. Consequently, an auditor's acceptance of responsibility for the preparation and fair presentation of financial statements that the auditor will subsequently audit would impair the auditor's independence.

3.52 Services related to preparing accounting records and financial statements that an auditor may be able to provide to an audited entity if the conditions in paragraph 3.46 are met include:

a. recording transactions for which management has determined or approved the appropriate account classification, or posting coded transactions to an audited entity's general ledger;

b. preparing financial statements based on information in the trial balance;

c. posting entries that have been approved by an audited entity's management to the entity's trial balance;

d. preparing account reconciliations that identify reconciling items for the audited entity management's evaluation; and

e. proposing standard, adjusting, or correcting journal entries or other changes affecting the financial statements to an audited entity's management provided management reviews and accepts the entries and the auditor is satisfied that management understands the nature of the proposed entries and the impact the entries have on the financial statements.

Internal Audit Assistance Services Provided by External Auditors

3.53 Internal audit assistance services involve assisting an entity in the performance of its internal audit activities. Certain internal audit assistance activities always impair an external auditor's independence with respect to an audited entity. These activities include:

a. setting internal audit policies or the strategic direction of internal audit activities;

b. performing procedures that form part of the internal control, such as reviewing and approving changes to employee data access privileges; and

c. determining the scope of the internal audit function and resulting work.

Internal Control Monitoring as a Nonaudit Service

3.54 Accepting responsibility for designing, implementing or maintaining internal control includes accepting responsibility for designing, implementing, or maintaining monitoring procedures.[34] Monitoring involves the use of either ongoing monitoring procedures or separate evaluations to gather and analyze persuasive information supporting conclusions about the effectiveness of the internal control system.

[34]See A.03 and A.04 for a discussion of internal control.

Ongoing monitoring procedures performed on behalf of management are built into the routine, recurring operating activities of an organization. Therefore, the management participation threat created if an auditor performs or supervises ongoing monitoring procedures is so significant that no safeguards could reduce the threat to an acceptable level.

3.55 Separate evaluations are sometimes performed as nonaudit services by individuals who are not directly involved in the operation of the controls being monitored. As such, it is possible for an auditor to provide an objective analysis of control effectiveness by performing separate evaluations without creating a management participation threat that would impair independence. However, in all such cases, the significance of the threat created by performing separate evaluations should be evaluated and safeguards applied when necessary to eliminate the threat or reduce it to an acceptable level. Auditors should assess the frequency of the separate evaluations as well as the scope or extent of the controls (in relation to the scope of the audit performed) being tested when evaluating the significance of the threat. An evaluation prepared as a nonaudit service is not a substitute for audit procedures in a GAGAS audit.

Information Technology Systems Services

3.56 Services related to information technology (IT) systems include the design or implementation of hardware or software systems. The systems may aggregate source data, form part of the internal control over the subject matter of the audit, or generate information that affects the subject matter of the audit. IT services that would impair independence if provided by an audit organization to an audited entity include:

a. designing or developing a financial or other IT system that will play a significant role in the management of an

area of operations that is or will be the subject matter of an audit;

b. providing services that entail making other than insignificant modifications to the source code underlying such a system; and

c. operating or supervising the operation of such a system.

Valuation Services

3.57 A valuation comprises the making of assumptions with regard to future developments, the application of appropriate methodologies and techniques, and the combination of both to compute a certain value, or range of values, for an asset, a liability, or an entity as a whole. If an audit organization provides valuation services to an audited entity and the valuations would have a material effect, separately or in the aggregate, on the financial statements or other information on which it is reporting, and the valuation involves a significant degree of subjectivity, the audit organization's independence would be impaired.

Other Nonaudit Services

3.58 Provision of certain other nonaudit services always impairs an external auditor's independence with respect to an audited entity. These activities include:

a. Non tax disbursement – prohibited nonaudit services

(1) Accepting responsibility to authorize payment of audited entity funds, electronically or otherwise.

(2) Accepting responsibility for signing or cosigning audited entity checks, even if only in emergency situations.

(3) Maintaining an audited entity's bank account or otherwise having custody of an audited entity's funds or

making credit or banking decisions for the audited entity.

(4) Approving vendor invoices for payment.

b. Benefit plan administration – prohibited nonaudit services

(1) Making policy decisions on behalf of audited entity management.

(2) When dealing with plan participants, interpreting the plan document on behalf of management without first obtaining management's concurrence.

(3) Making disbursements on behalf of the plan.

(4) Having custody of a plan's assets.

(5) Serving a plan as a fiduciary as defined by the Employee Retirement Income Security Act (ERISA).

c. Investment—advisory or management—prohibited nonaudit services

(1) Making investment decisions on behalf of audited entity management or otherwise having discretionary authority over an audited entity's investments.

(2) Executing a transaction to buy or sell an audited entity's investment.

(3) Having custody of an audited entity's assets, such as taking temporary possession of securities purchased by an audited entity.

d. Corporate finance—consulting or advisory – prohibited nonaudit services

(1) Committing the audited entity to the terms of a transaction or consummating a transaction on behalf of the audited entity.

(2) Acting as a promoter, underwriter, broker-dealer, or guarantor of audited entity securities, or distributor of private placement memoranda or offering documents.

(3) Maintaining custody of an audited entity's securities.

e. Executive or employee personnel matters – prohibited nonaudit services

(1) Committing the audited entity to employee compensation or benefit arrangements.

(2) Hiring or terminating audited entity employees.

f. Business risk consulting – prohibited nonaudit services

(1) Making or approving business risk decisions.

(2) Presenting business risk considerations to those charged with governance or others on behalf of management.

Documentation

3.59 Documentation of independence considerations provides evidence of the auditor's judgments in forming conclusions regarding compliance with independence requirements. GAGAS contains specific requirements for documentation related to independence which may be in addition to the documentation that auditors have previously maintained. While insufficient documentation of an auditor's compliance with the independence standard does not impair independence, appropriate documentation is required under the GAGAS quality

control and assurance requirements.[35] The independence standard includes the following documentation requirements:

a. document threats to independence that require the application of safeguards, along with safeguards applied, in accordance with the conceptual framework for independence as required by paragraph 3.24;

b. document the safeguards required by paragraph 3.30 if an audit organization is structurally located within a government entity and is considered independent based on those safeguards;

c. document consideration of audited entity management's ability to effectively oversee a nonaudit service to be provided by the auditor as indicated in paragraph 3.34; and

d. document the auditor's understanding with an audited entity for which the auditor will perform a nonaudit service as indicated in paragraph 3.39.

Professional Judgment

3.60 Auditors must use professional judgment in planning and performing audits and in reporting the results.

3.61 Professional judgment includes exercising reasonable care and professional skepticism. Reasonable care includes acting diligently in accordance with applicable professional standards and ethical principles. Professional skepticism is an attitude that includes a questioning mind and a critical

[35]See paragraph 3.84 for additional discussion of documenting compliance with quality control policies and procedures and paragraph 3.88 for additional discussion of policies and procedures on independence, legal, and ethical requirements.

assessment of evidence. Professional skepticism includes a mindset in which auditors assume neither that management is dishonest nor of unquestioned honesty.

3.62 Using the auditors' professional knowledge, skills, and experience to diligently perform, in good faith and with integrity, the gathering of information and the objective evaluation of the sufficiency and appropriateness of evidence is a critical component of audits. Professional judgment and competence are interrelated because judgments made are dependent upon the auditors' competence.

3.63 Professional judgment represents the application of the collective knowledge, skills, and experiences of all the personnel involved with an audit, as well as the professional judgment of individual auditors. In addition to personnel directly involved in the audit, professional judgment may involve collaboration with other stakeholders, external specialists, and management in the audit organization.

3.64 Using professional judgment is important to auditors in carrying out all aspects of their professional responsibilities, including following the independence standards and related conceptual framework; maintaining objectivity and credibility; assigning competent staff to the audit; defining the scope of work; evaluating, documenting, and reporting the results of the work; and maintaining appropriate quality control over the audit process.

3.65 Using professional judgment is important to auditors in applying the conceptual framework to determine independence in a given situation. This includes the consideration of any threats to the auditor's independence and related safeguards which may mitigate the identified threats. Auditors use professional

judgment in identifying and evaluating any threats to independence, including threats to the appearance of independence.[36]

3.66 Using professional judgment is important to auditors in determining the required level of understanding of the audit subject matter and related circumstances. This includes consideration about whether the audit team's collective experience, training, knowledge, skills, abilities, and overall understanding are sufficient to assess the risks that the subject matter of the audit may contain a significant inaccuracy or could be misinterpreted.

3.67 An auditor's consideration of the risk level of each audit, including the risk of arriving at improper conclusions, is also important. Within the context of audit risk, exercising professional judgment in determining the sufficiency and appropriateness of evidence to be used to support the findings and conclusions based on the audit objectives and any recommendations reported is an integral part of the audit process.

3.68 While this standard places responsibility on each auditor and audit organization to exercise professional judgment in planning and performing an audit, it does not imply unlimited responsibility, nor does it imply infallibility on the part of either the individual auditor or the audit organization. Absolute assurance is not attainable due to factors such as the nature of evidence and characteristics of fraud. Professional judgment does not mean eliminating all possible limitations or weaknesses associated with a specific audit, but rather identifying, assessing, mitigating, and explaining them.

[36]See paragraph 3.03 for a description of independence in appearance.

Competence

3.69 The staff assigned to perform the audit must collectively possess adequate professional competence needed to address the audit objectives and perform the work in accordance with GAGAS.

3.70 The audit organization's management should assess skill needs to consider whether its workforce has the essential skills that match those necessary to perform the particular audit. Accordingly, audit organizations should have a process for recruitment, hiring, continuous development, assignment, and evaluation of staff to maintain a competent workforce. The nature, extent, and formality of the process will depend on various factors such as the size of the audit organization, its structure, and its work.

3.71 Competence is derived from a blending of education and experience. Competencies are not necessarily measured by years of auditing experience because such a quantitative measurement may not accurately reflect the kinds of experiences gained by an auditor in any given time period. Maintaining competence through a commitment to learning and development throughout an auditor's professional life is an important element for auditors. Competence enables an auditor to make sound professional judgments.

Technical Knowledge

3.72 The staff assigned to conduct an audit in accordance with GAGAS should collectively possess the technical knowledge, skills, and experience necessary to be competent for the type of work being performed before beginning work on that audit. The staff assigned to a GAGAS audit should collectively possess

a. knowledge of GAGAS applicable to the type of work they are assigned and the education, skills, and

experience to apply this knowledge to the work being performed;

b. general knowledge of the environment in which the audited entity operates and the subject matter;

c. skills to communicate clearly and effectively, both orally and in writing; and

d. skills appropriate for the work being performed; for example, skills in

(1) statistical or nonstatistical sampling if the work involves use of sampling;

(2) information technology if the work involves review of information systems;

(3) engineering if the work involves review of complex engineering data;

(4) specialized audit methodologies or analytical techniques, such as the use of complex survey instruments, actuarial-based estimates, or statistical analysis tests, as applicable; or

(5) specialized knowledge in subject matters, such as scientific, medical, environmental, educational, or any other specialized subject matter, if the work calls for such expertise.

Additional Qualifications for Financial Audits and Attestation Engagements

3.73 Auditors performing financial audits should be knowledgeable in U.S. generally accepted accounting principles (GAAP), or with the applicable financial reporting framework being used, and the American Institute of Certified Public Accountants' (AICPA)

Statements on Auditing Standards (SAS)[37] and they should be competent in applying these SASs to the audit work.

3.74 Similarly, auditors performing attestation engagements should be knowledgeable in the AICPA general attestation standard related to criteria, the AICPA attestation standards for field work and reporting, and the related Statements on Standards for Attestation Engagements (SSAE),[38] and they should be competent in applying these standards and SSAE to the attestation work.[39]

3.75 Auditors engaged to perform financial audits or attestation engagements should be licensed certified public accountants, persons working for a licensed certified public accounting firm or for a government auditing organization, or licensed accountants in states that have multi-class licensing systems that recognize licensed accountants other than certified public accountants.

Continuing Professional Education

3.76 Auditors performing work in accordance with GAGAS, including planning, directing, performing audit procedures, or reporting on an audit conducted in accordance with GAGAS, should maintain their professional competence through continuing professional education (CPE). Therefore, each auditor performing work in accordance with GAGAS should complete, every 2 years, at least 24 hours of CPE that

[37]See paragraph 2.08 and 4.01 for discussion of the AICPA standards incorporated into GAGAS for financial audits.

[38]See paragraphs 2.09 and 5.01 for discussion of the AICPA standards incorporated into GAGAS for attestation engagements.

[39]See paragraphs 2.19 through 2.22 for additional information on the relationship between GAGAS and other professional standards for financial audits and attestation engagements.

directly relates to government auditing, the government environment, or the specific or unique environment in which the audited entity operates. Auditors who are involved in any amount of planning, directing, or reporting on GAGAS audits and auditors who are not involved in those activities but charge 20 percent or more of their time annually to GAGAS audits should also obtain at least an additional 56 hours of CPE (for a total of 80 hours of CPE in every 2-year period) that enhances the auditor's professional proficiency to perform audits. Auditors required to take the total 80 hours of CPE should complete at least 20 hours of CPE in each year of the 2-year periods. Auditors hired or initially assigned to GAGAS audits after the beginning of an audit organization's 2-year CPE period should complete a prorated number of CPE hours.

3.77 CPE programs are structured educational activities with learning objectives designed to maintain or enhance participants' knowledge, skills, and abilities in areas applicable to performing audits. Determining what subjects are appropriate for individual auditors to satisfy both the 80-hour and the 24-hour requirements is a matter of professional judgment to be exercised by auditors in consultation with appropriate officials in their audit organizations. Among the considerations in exercising that judgment are the auditors' experience, the responsibilities they assume in performing GAGAS audits, and the operating environment of the audited entity.

3.78 Meeting CPE requirements is primarily the responsibility of individual auditors. The audit organization should have quality control procedures to help ensure that auditors meet the continuing education requirements, including documentation of the CPE completed. The Government Accountability Office (GAO) has developed guidance pertaining to CPE requirements to assist auditors and audit organizations

in exercising professional judgment in complying with the CPE requirements.[40]

CPE Requirements for Specialists

3.79 The audit team should determine that external specialists assisting in performing a GAGAS audit are qualified and competent in their areas of specialization; however, external specialists are not required to meet the GAGAS CPE requirements.

3.80 The audit team should determine that internal specialists consulting on a GAGAS audit who are not involved in directing, performing audit procedures, or reporting on a GAGAS audit, are qualified and competent in their areas of specialization; however, these internal specialists are not required to meet the GAGAS CPE requirements.

3.81 The audit team should determine that internal specialists, who are performing work in accordance with GAGAS as part of the audit team, including directing, performing audit procedures, or reporting on a GAGAS audit, comply with GAGAS, including the CPE requirements.[41] The GAGAS CPE requirements become effective for internal specialists when an audit organization first assigns an internal specialist to an audit. Because internal specialists apply specialized knowledge in government audits, training in their areas of specialization qualify under the requirement for 24 hours of CPE that directly relates to government auditing, the government environment, or the specific or unique environment in which the audited entity operates.

[40]*Government Auditing Standards: Guidance on GAGAS Requirements for Continuing Professional Education*, GAO-05-568G (Washington, D.C.: April 2005), http://www.gao.gov/yellowbook.

[41]See paragraphs 3.76 through 3.81 for discussion of the CPE requirements.

Quality Control and Assurance

3.82 Each audit organization performing audits in accordance with GAGAS must:

a. establish and maintain a system of quality control that is designed to provide the audit organization with reasonable assurance that the organization and its personnel comply with professional standards and applicable legal and regulatory requirements,[42] and

b. have an external peer review performed by reviewers independent of the audit organization being reviewed at least once every 3 years.

System of Quality Control

3.83 An audit organization's system of quality control encompasses the audit organization's leadership, emphasis on performing high quality work, and the organization's policies and procedures designed to provide reasonable assurance of complying with professional standards and applicable legal and regulatory requirements. The nature, extent, and formality of an audit organization's quality control system will vary based on the audit organization's circumstances, such as the audit organization's size, number of offices and geographic dispersion, knowledge and experience of its personnel, nature and complexity of its audit work, and cost-benefit considerations.

3.84 Each audit organization should document its quality control policies and procedures and communicate those policies and procedures to its personnel. The audit organization should document compliance with its quality control policies and procedures and maintain such documentation for a

[42]See paragraph A3.10 for additional discussion of the system of quality control.

period of time sufficient to enable those performing monitoring procedures and peer reviews to evaluate the extent of the audit organization's compliance with its quality control policies and procedures. The form and content of such documentation are a matter of professional judgment and will vary based on the audit organization's circumstances.

3.85 An audit organization should establish policies and procedures in its system of quality control that collectively address

a. leadership responsibilities for quality within the audit organization,

b. independence, legal, and ethical requirements,

c. initiation, acceptance, and continuance of audits,

d. human resources,

e. audit performance, documentation, and reporting, and

f. monitoring of quality.

Leadership Responsibilities for Quality within the Audit Organization

3.86 Audit organizations should establish policies and procedures on leadership responsibilities for quality within the audit organization that include the designation of responsibility for quality of audits performed in accordance with GAGAS and communication of policies and procedures relating to quality. Appropriate policies and communications encourage a culture that recognizes that quality is essential in performing GAGAS audits and that leadership of the audit organization is ultimately responsible for the system of quality control.

3.87 The audit organization should establish policies and procedures designed to provide it with reasonable assurance that those assigned operational responsibility for the audit organization's system of quality control have sufficient and appropriate experience and ability, and the necessary authority, to assume that responsibility.

Independence, Legal, and Ethical Requirements

3.88 Audit organizations should establish policies and procedures on independence, legal, and ethical requirements that are designed to provide reasonable assurance that the audit organization and its personnel maintain independence and comply with applicable legal and ethical requirements.[43] Such policies and procedures assist the audit organization to

a. communicate its independence requirements to its staff, and

b. identify and evaluate circumstances and relationships that create threats to independence, and take appropriate action to eliminate those threats or reduce them to an acceptable level by applying safeguards, or, if considered appropriate, withdraw from the audit where withdrawal is not prohibited by law or regulation.

Initiation, Acceptance, and Continuance of Audits

3.89 Audit organizations should establish policies and procedures for the initiation, acceptance, and continuance of audits that are designed to provide reasonable assurance that the audit organization will undertake audits only if it can comply with professional standards, legal requirements, and ethical principles

[43]See paragraphs 3.02 through 3.59 for GAGAS independence requirements. See chapter 1 for GAGAS ethical principles.

and is acting within the legal mandate or authority of the audit organization.[44]

Human Resources

3.90 Audit organizations should establish policies and procedures for human resources that are designed to provide the audit organization with reasonable assurance that it has personnel with the capabilities and competence to perform its audits in accordance with professional standards and legal and regulatory requirements.[45]

Audit Performance, Documentation, and Reporting

3.91 Audit organizations should establish policies and procedures for audit performance, documentation, and reporting that are designed to provide the audit organization with reasonable assurance that audits are performed and reports are issued in accordance with professional standards and legal and regulatory requirements.[46]

3.92 When performing GAGAS audits, audit organizations should have policies and procedures for the safe custody and retention of audit documentation for a time sufficient to satisfy legal, regulatory, and administrative requirements for records retention. Whether audit documentation is in paper, electronic, or other media, the integrity, accessibility, and retrievability of the underlying information could be compromised if the documentation is altered, added to, or deleted without the auditors' knowledge, or if the documentation is lost or damaged. For audit documentation that is retained electronically, the audit organization should

[44]See paragraph A3.10a for discussion of initiation of audits by government audit organizations.

[45]See paragraphs 3.69 through 3.81 for requirements related to professional competence.

[46]For financial audits, chapters 2 through 4 apply; for attestation engagements, chapters 2, 3 and 5 apply; for performance audits, chapters 2, 3, 6, and 7 apply.

establish effective information systems controls concerning accessing and updating the audit documentation.

Monitoring of Quality

3.93 Audit organizations should establish policies and procedures for monitoring of quality in the audit organization.[47] Monitoring of quality is an ongoing, periodic assessment of work completed on audits designed to provide management of the audit organization with reasonable assurance that the policies and procedures related to the system of quality control are suitably designed and operating effectively in practice. The purpose of monitoring compliance with quality control policies and procedures is to provide an evaluation of whether the:

a. professional standards and legal and regulatory requirements have been followed,

b. quality control system has been appropriately designed, and

c. quality control policies and procedures are operating effectively and complied with in practice.

3.94 Monitoring procedures will vary based on the audit organization's facts and circumstances. The audit organization should perform monitoring procedures that enable it to assess compliance with applicable professional standards and quality control policies and procedures for GAGAS audits. Individuals performing monitoring should collectively have sufficient expertise and authority for this role.

3.95 The audit organization should analyze and summarize the results of its monitoring process at least

[47]See paragraph A3.10c for additional discussion of monitoring.

annually, with identification of any systemic or repetitive issues needing improvement, along with recommendations for corrective action. The audit organization should communicate to appropriate personnel any deficiencies noted during the monitoring process and make recommendations for appropriate remedial action.

External Peer Review

3.96 The audit organization should obtain an external peer review at least once every 3 years that is sufficient in scope to provide a reasonable basis for determining whether, for the period under review, the reviewed audit organization's system of quality control was suitably designed and whether the audit organization is complying with its quality control system in order to provide the audit organization with reasonable assurance of conforming with applicable professional standards.

3.97 The first peer review for an audit organization not already subject to a peer review requirement covers a review period ending no later than 3 years from the date an audit organization begins its first audit in accordance with GAGAS. The period under review generally covers 1 year, although peer review programs may choose a longer review period. Generally, the deadlines for peer review reports are established by the entity that administers the peer review program. Extensions of the deadlines for submitting the peer review report exceeding 3 months beyond the due date are granted by the entity that administers the peer review program and GAO.

3.98 The peer review team should include the following elements in the scope of the peer review:

a. review of the audit organization's quality control policies and procedures;

b. consideration of the adequacy and results of the audit organization's internal monitoring procedures;

c. review of selected auditors' reports and related documentation;

d. review of other documents necessary for assessing compliance with standards, for example, independence documentation, CPE records, and relevant human resource management files; and

e. interviews with a selection of the reviewed audit organization's professional staff at various levels to assess their understanding of and compliance with relevant quality control policies and procedures.

3.99 The peer review team should perform an assessment of peer review risk to help determine the number and types of audits to select for review.[48] Based on the risk assessment, the team should use one or a combination of the following approaches to select individual audits for review with greater emphasis on those audits with higher assessed levels of peer review risk: (1) select GAGAS audits that provide a reasonable cross-section of the GAGAS audits performed by the reviewed audit organization; or (2) select audits that provide a reasonable cross-section from all types of work subject to the reviewed audit organization's quality control system, including one or more audits performed in accordance with GAGAS. The second approach is generally applicable to audit organizations that perform only a small number of GAGAS audits in relation to other types of audits. In these cases, one or more GAGAS audits may represent more than what would be

[48]See paragraph A3.11 for examples of factors to consider in assessing peer review risk.

selected when looking at a cross-section of the audit organization's work as a whole.

3.100 The peer review team should prepare one or more written reports communicating the results of the peer review, including the following:

a. a description of the scope of the peer review, including any limitations;

b. an opinion on whether the system of quality control of the reviewed audit organization's audit practices was adequately designed and complied with during the period reviewed to provide the audit organization with reasonable assurance of conforming with applicable professional standards;

c. specification of the professional standards to which the reviewed audit organization is being held; and

d. reference to a separate written communication, if issued under the peer review program.

3.101 The peer review team uses professional judgment in deciding the type of peer review report. The following are the types of peer review reports.

a. Peer Review Rating of Pass: A conclusion that the audit organization's system of quality control has been suitably designed and complied with to provide the audit organization with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects.

b. Peer Review Rating of Pass with Deficiencies: A conclusion that the audit organization's system of quality control has been suitably designed and complied with to provide the audit organization with reasonable assurance of performing and reporting in conformity

with applicable professional standards in all material respects with the exception of a certain deficiency or deficiencies that are described in the report.

c. Peer Review Rating of Fail: A conclusion, based on the significant deficiencies that are described in the report, that the audit organization's system of quality control is not suitably designed to provide the audit organization with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects, or the audit organization has not complied with its system of quality control to provide the audit organization with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects.

3.102 When the scope of the review is limited by conditions that preclude the application of one or more peer review procedures considered necessary in the circumstances and the peer reviewer cannot accomplish the objectives of those procedures through alternative procedures, the types of reports described in paragraphs 3.101 a-c are modified by including statements in the report's scope paragraph, body and opinion paragraph. These statements describe the relationship of the excluded audit(s) or functional area(s) to the reviewed organization's full scope of practice and system of quality control and the effects of the exclusion on the scope and results of the review.

3.103 For any deficiencies or significant deficiencies included in the peer review report or other written communication, the peer review team should include, either in the peer review report or in a separate written communication, a detailed description of the findings, conclusions, and recommendations related to the deficiencies or significant deficiencies.

3.104 The peer review team should meet the following criteria:

a. The review team collectively has current knowledge of GAGAS and government auditing.

b. The organization conducting the peer review and individual review team members are independent (as defined in GAGAS)[49] of the audit organization being reviewed, its staff, and the audits selected for the peer review.

c. The review team collectively has sufficient knowledge of how to perform a peer review. Such knowledge may be obtained from on-the-job training, training courses, or a combination of both. Having personnel on the peer review team with prior experience on a peer review or internal inspection team is desirable.

3.105 An external audit organization[50] should make its most recent peer review report publicly available.[51] For example, an audit organization may satisfy this requirement by posting the peer review report on a publicly available web site or to a publicly available file designed for public transparency of peer review results. Alternatively, if neither of these options is available to the audit organization, then it should use the same transparency mechanism it uses to make other information public. The audit organization should provide the peer review report to others upon request. If a separate communication detailing findings, conclusions, and recommendations is issued, public

[49]See paragraphs 3.02 through 3.32 for discussion of independence.

[50]See paragraph 1.07b for the definition of "audit organizations" and paragraph 1.08 for discussion of external audit organizations.

[51]See paragraph A3.12 for additional discussion of peer review report transparency.

availability of that communication is not required. Internal audit organizations that report internally to management and those charged with governance should provide a copy of the peer review report to those charged with governance.

3.106 Information in peer review reports may be relevant to decisions on procuring audits. Therefore, audit organizations seeking to enter into a contract to perform an audit in accordance with GAGAS should provide the following to the party contracting for such services when requested:

a. the audit organization's most recent peer review report, and

b. any subsequent peer review reports received during the period of the contract.

3.107 Auditors who are using another audit organization's work should request a copy of the audit organization's latest peer review report and any other written communication issued, and the audit organization should provide these documents when requested.[52]

[52]See paragraphs 6.40 through 6.44 for additional discussion on using the work of other auditors.

Standards for Financial Audits

Introduction

4.01 This chapter contains requirements, guidance, and considerations for performing and reporting on financial audits conducted in accordance with generally accepted government auditing standards (GAGAS). GAGAS incorporates by reference the American Institute of Certified Public Accountants (AICPA) Statements on Auditing Standards (SAS), as discussed in paragraph 2.08.[53] All sections of the SASs are incorporated, including the introduction, objectives, definitions, requirements, and application and other explanatory material. Auditors performing financial audits in accordance with GAGAS should comply with the incorporated SASs and the additional requirements in this chapter. The requirements and guidance contained in chapters 1 through 3 also apply to financial audits performed in accordance with GAGAS.

Additional GAGAS Requirements for Performing Financial Audits

4.02 GAGAS establishes requirements for performing financial audits in addition to the requirements contained in the AICPA standards. Auditors should comply with these additional requirements, along with the incorporated SASs, when citing GAGAS in their reports. The additional requirements for performing financial audits relate to:

a. auditor communication;

b. previous audits and attestation engagements;

[53]See the AICPA *Codification of Statements on Auditing Standards* and paragraph 2.20 for additional discussion on the relationship between GAGAS and other professional standards. References to the AICPA *Codification of Statements on Auditing Standards* use an "AU-C" identifier to refer to the clarified SASs instead of an "AU" identifier. "AU-C" is a temporary identifier to avoid confusion with references to existing "AU" sections, which remain effective through 2013. The "AU-C" identifier will revert to "AU" in 2014 AICPA *Codification of Statements on Auditing Standards*, by which time the clarified SASs become fully effective for all engagements.

c. fraud, noncompliance with provisions of laws, regulations, contracts, and grant agreements, and abuse;

d. developing elements of a finding; and

e. audit documentation.[54]

Auditor Communication

4.03 In addition to the AICPA requirements for auditor communication,[55] when performing a GAGAS financial audit, auditors should communicate pertinent information that in the auditors' professional judgment needs to be communicated to individuals contracting for or requesting the audit, and to cognizant legislative committees when auditors perform the audit pursuant to a law or regulation, or they conduct the work for the legislative committee that has oversight of the audited entity. This requirement does not apply if the law or regulation requiring an audit of the financial statements does not specifically identify the entities to be audited, such as audits required by the Single Audit Act Amendments of 1996.

4.04 In those situations where there is not a single individual or group that both oversees the strategic direction of the audited entity and the fulfillment of its accountability obligations or in other situations where the identity of those charged with governance is not clearly evident, auditors should document the process followed and conclusions reached for identifying the appropriate individuals to receive the required auditor communications.

[54]See paragraphs 4.03 through 4.16 for additional discussion of paragraph 4.02 a-e.

[55]See AICPA AU-C Section 260, *The Auditor's Communication With Those Charged With Governance.*

Previous Audits and Attestation Engagements

4.05 When performing a GAGAS audit, auditors should evaluate whether the audited entity has taken appropriate corrective action to address findings and recommendations from previous engagements that could have a material effect on the financial statements or other financial data significant to the audit objectives. When planning the audit, auditors should ask management of the audited entity to identify previous audits, attestation engagements, and other studies that directly relate to the objectives of the audit, including whether related recommendations have been implemented. Auditors should use this information in assessing risk and determining the nature, timing, and extent of current audit work, including determining the extent to which testing the implementation of the corrective actions is applicable to the current audit objectives.

Fraud, Noncompliance with Provisions of Laws, Regulations, Contracts, and Grant Agreements, and Abuse

4.06 In addition to the AICPA requirements concerning fraud[56] and noncompliance with provisions of laws and regulations,[57] when performing a GAGAS financial audit, auditors should extend the AICPA requirements pertaining to the auditors' responsibilities for laws and regulations to also apply to consideration of compliance with provisions of contracts or grant agreements.

4.07 Abuse involves behavior that is deficient or improper when compared with behavior that a prudent person would consider reasonable and necessary business practice given the facts and circumstances. Abuse also includes misuse of authority or position for personal financial interests or those of an immediate or

[56]See AICPA AU-C Section 240, *Consideration of Fraud in a Financial Statement Audit*.

[57]See AICPA AU-C Section 250, *Consideration of Laws and Regulations in an Audit of Financial Statements.*

close family member or business associate.[58] Abuse does not necessarily involve fraud, or noncompliance with provisions of laws, regulations, contracts, or grant agreements.

4.08 Because the determination of abuse is subjective, auditors are not required to detect abuse in financial audits. However, as part of a GAGAS audit, if auditors become aware of abuse that could be quantitatively or qualitatively material to the financial statements or other financial data significant to the audit objectives, auditors should apply audit procedures specifically directed to ascertain the potential effect on the financial statements or other financial data significant to the audit objectives. After performing additional work, auditors may discover that the abuse represents potential fraud or noncompliance with provisions of laws, regulations, contracts, or grant agreements.

4.09 Avoiding interference with investigations or legal proceedings is important in pursuing indications of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse. Laws, regulations, or policies may require auditors to report indications of certain types of fraud, noncompliance with provisions of laws, regulations, contracts or grant agreements, or abuse to law enforcement or investigatory authorities before performing additional audit procedures. When investigations or legal proceedings are initiated or in process, auditors should evaluate the impact on the current audit. In some cases, it may be appropriate for the auditors to work with investigators or legal authorities, or withdraw from or defer further work on the audit engagement or a portion of the engagement to

[58]See paragraph A.08 for additional examples of abuse.

avoid interfering with an ongoing investigation or legal proceeding.

Developing Elements of a Finding

4.10 In a financial audit, findings may involve deficiencies in internal control; noncompliance with provisions of laws, regulations, contracts, or grant agreements; fraud; or abuse. As part of a GAGAS audit, when auditors identify findings, auditors should plan and perform procedures to develop the elements of the findings that are relevant and necessary to achieve the audit objectives. The elements of a finding are discussed in paragraphs 4.11 through 4.14 below.

4.11 Criteria: The laws, regulations, contracts, grant agreements, standards, measures, expected performance, defined business practices, and benchmarks against which performance is compared or evaluated. Criteria identify the required or desired state or expectation with respect to the program or operation. Criteria provide a context for evaluating evidence and understanding the findings.

4.12 Condition: Condition is a situation that exists. The condition is determined and documented during the audit.

4.13 Cause: The cause identifies the reason or explanation for the condition or the factor or factors responsible for the difference between the situation that exists (condition) and the required or desired state (criteria), which may also serve as a basis for recommendations for corrective actions. Common factors include poorly designed policies, procedures, or criteria; inconsistent, incomplete, or incorrect implementation; or factors beyond the control of program management. Auditors may assess whether the evidence provides a reasonable and convincing argument for why the stated cause is the key factor or

factors contributing to the difference between the condition and the criteria.

4.14 Effect or potential effect: The effect is a clear, logical link to establish the impact or potential impact of the difference between the situation that exists (condition) and the required or desired state (criteria). The effect or potential effect identifies the outcomes or consequences of the condition. When the audit objectives include identifying the actual or potential consequences of a condition that varies (either positively or negatively) from the criteria identified in the audit, "effect" is a measure of those consequences. Effect or potential effect may be used to demonstrate the need for corrective action in response to identified problems or relevant risks.

Audit Documentation

4.15 In addition to the AICPA requirements for audit documentation,[59] auditors should comply with the following additional requirements when performing a GAGAS financial audit.[60]

a. Document supervisory review, before the report release date, of the evidence that supports the findings, conclusions, and recommendations contained in the auditors' report.

b. Document any departures from the GAGAS requirements and the impact on the audit and on the auditors' conclusions when the audit is not in compliance with applicable GAGAS requirements due to law, regulation, scope limitations, restrictions on access to records, or other issues impacting the audit.

[59]See AICPA AU-C Section 230, *Audit Documentation.*

[60]See paragraphs 4.04, 4.06, 4.26, and 4.45 for additional documentation requirements regarding financial audits.

This applies to departures from unconditional requirements and presumptively mandatory requirements when alternative procedures performed in the circumstances were not sufficient to achieve the objectives of the requirements.[61]

4.16 When performing GAGAS financial audits and subject to applicable provisions of laws and regulations, auditors should make appropriate individuals, as well as audit documentation, available upon request and in a timely manner to other auditors or reviewers. Underlying GAGAS audits is the premise that audit organizations in federal, state, and local governments and public accounting firms engaged to perform a financial audit in accordance with GAGAS cooperate in auditing programs of common interest so that auditors may use others' work and avoid duplication of efforts. The use of auditors' work by other auditors may be facilitated by contractual arrangements for GAGAS audits that provide for full and timely access to appropriate individuals, as well as audit documentation.

Additional GAGAS Requirements for Reporting on Financial Audits

4.17 In addition to the AICPA requirements for reporting,[62] auditors should comply with the following additional requirements when citing GAGAS in their reports. The additional requirements relate to

a. reporting auditors' compliance with GAGAS;

[61]See paragraphs 2.24 and 2.25 for additional requirements on citing compliance with GAGAS.

[62]See AICPA AU-C Sections 700 *Forming an Opinion and Reporting on Financial Statements;* 705 *Modifications to the Opinion in the Independent Auditor's Report,* and 706 *Emphasis-of-Matter Paragraphs and Other-Matter Paragraphs in the Independent Auditor's Report.*

b. reporting on internal control and compliance with provisions of laws, regulations, contracts, and grant agreements;

c. communicating deficiencies in internal control, fraud, noncompliance with provisions of laws, regulations, contracts, and grant agreements, and abuse;

d. reporting views of responsible officials;

e. reporting confidential or sensitive information; and

f. distributing reports.[63]

Reporting Auditors' Compliance with GAGAS

4.18 When auditors comply with all applicable GAGAS requirements for financial audits, they should include a statement in the auditors' report that they performed the audit in accordance with GAGAS.[64] Because GAGAS incorporates by reference the AICPA SASs,[65] GAGAS does not require auditors to cite compliance with the AICPA standards when citing compliance with GAGAS. Additionally, an entity receiving a GAGAS auditors' report may also request auditors to issue a financial audit report for purposes other than complying with requirements for a GAGAS audit. GAGAS does not prohibit auditors from issuing a separate report conforming only to AICPA or other standards.[66]

[63]See paragraphs 4.18 through 4.45 for additional discussion paragraph of 4.17 a-f.

[64]See paragraphs 2.24 and 2.25 for additional requirements on citing compliance with GAGAS.

[65]See paragraph 2.08 for a discussion of the AICPA SASs incorporated into GAGAS.

[66]See AICPA AU-C Section 700, *Forming an Opinion and Reporting on Financial Statements.*

Reporting on Internal Control and Compliance with Provisions of Laws, Regulations, Contracts, and Grant Agreements

4.19 When providing an opinion or a disclaimer on financial statements, auditors should also report on internal control over financial reporting[67] and on compliance with provisions of laws, regulations, contracts, or grant agreements that have a material effect on the financial statements.[68] Auditors report on internal control and compliance, regardless of whether or not they identify internal control deficiencies or instances of noncompliance.

4.20 Auditors should include either in the same or in separate report(s) a description of the scope of the auditors' testing of internal control over financial reporting and of compliance with provisions of laws, regulations, contracts, or grant agreements. Auditors should also state in the reports whether the tests they performed provided sufficient, appropriate evidence to support opinions on the effectiveness of internal control and on compliance with provisions of laws, regulations, contracts, or grant agreements.

4.21 The objective of the GAGAS requirement for reporting on internal control over financial reporting differs from the objective of an examination of internal control in accordance with the AICPA Statement on Standards for Attestation Engagements (SSAE), which is to express an opinion on the design or the design and operating effectiveness of an entity's internal control, as applicable. To form a basis for expressing such an opinion, the auditor would need to plan and perform the examination to provide a high level of assurance about whether the entity maintained, in all material respects, effective internal control over financial reporting as of a

[67]See paragraph A.05 for examples of deficiencies in internal control.

[68]See paragraph A.11 for additional discussion of laws, regulations, and provisions of contract and grant agreements.

point in time or for a specified period of time.[69] If auditors issue an opinion on internal control, the opinion would satisfy the GAGAS requirement for reporting on internal control.

4.22 If auditors report separately (including separate reports bound in the same document) on internal control over financial reporting and on compliance with provisions of laws, regulations, contracts, and grant agreements, they should state in the auditors' report on the financial statements that they are issuing those additional reports. They should include a reference to the separate reports and also state that the reports on internal control over financial reporting and on compliance with provisions of laws, regulations, contracts, and grant agreements are an integral part of a GAGAS audit in considering the audited entity's internal control over financial reporting and compliance.

Communicating Deficiencies in Internal Control, Fraud, Noncompliance with Provisions of Laws, Regulations, Contracts, and Grant Agreements, and Abuse

4.23 When performing GAGAS financial audits, auditors should communicate in the report on internal control over financial reporting and compliance, based upon the work performed, (1) significant deficiencies and material weaknesses in internal control; (2) instances of fraud and noncompliance with provisions of laws or regulations that have a material effect on the audit and any other instances that warrant the attention of those charged with governance; (3) noncompliance with provisions of contracts or grant agreements that has a material effect on the audit; and (4) abuse that has a material effect on the audit.

Deficiencies in Internal Control

4.24 The AICPA requirements to communicate in writing significant deficiencies and material weaknesses

[69]See AICPA AT Section 501, *An Examination of an Entity's Internal Control Over Financial Reporting That Is Integrated With an Audit of Its Financial Statements.*

identified during an audit[70] form the basis for reporting significant deficiencies and material weaknesses in the GAGAS report on internal control over financial reporting when deficiencies are identified during the audit.

Fraud, Noncompliance with Provisions of Laws, Regulations, Contracts, and Grant Agreements, and Abuse

4.25 When performing a GAGAS financial audit, and auditors conclude, based on sufficient, appropriate evidence, that any of the following either has occurred or is likely to have occurred, they should include in their report on internal control and compliance the relevant information about

a. fraud[71] and noncompliance with provisions of laws or regulations that have a material effect on the financial statements or other financial data significant to the audit objectives and any other instances that warrant the attention of those charged with governance;

b. noncompliance with provisions of contracts or grant agreements that has a material effect on the determination of financial statement amounts or other financial data significant to the audit objectives; or

c. abuse[72] that is material, either quantitatively or qualitatively.[73]

4.26 When auditors detect instances of noncompliance with provisions of contracts or grant agreements or abuse that have an effect on the financial statements or other financial data significant to the audit objectives

[70]See AICPA AU-C Section 265, *Communicating Internal Control Related Matters Identified in an Audit.*

[71]See paragraph A.10 for examples of indicators of fraud risk.

[72]See paragraph A.08 for examples of abuse.

[73]See paragraphs 4.07 and 4.08 for a discussion of abuse.

that are less than material but warrant the attention of those charged with governance, they should communicate those findings in writing to audited entity officials. When auditors detect any instances of fraud, noncompliance with provisions of laws, regulations, contracts or grant agreements, or abuse that do not warrant the attention of those charged with governance, the auditors' determination of whether and how to communicate such instances to audited entity officials is a matter of professional judgment.

4.27 When fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse either have occurred or are likely to have occurred, auditors may consult with authorities or legal counsel about whether publicly reporting such information would compromise investigative or legal proceedings. Auditors may limit their public reporting to matters that would not compromise those proceedings, and for example, report only on information that is already a part of the public record.

Presenting Findings in the Auditors' Report

4.28 When performing a GAGAS financial audit and presenting findings such as deficiencies in internal control, fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse, auditors should develop the elements of the findings to the extent necessary, including findings related to deficiencies from the previous year that have not been remediated. Clearly developed findings, as discussed in paragraphs 4.10 through 4.14, assist management or oversight officials of the audited entity in understanding the need for taking corrective action, and assist auditors in making recommendations for corrective action. If auditors sufficiently develop the elements of a finding, they may provide recommendations for corrective action.

4.29 Auditors should place their findings in perspective by describing the nature and extent of the issues being reported and the extent of the work performed that resulted in the finding. To give the reader a basis for judging the prevalence and consequences of these findings, auditors should, as appropriate, relate the instances identified to the population or the number of cases examined and quantify the results in terms of dollar value or other measures. If the results cannot be projected, auditors should limit their conclusions appropriately.

Reporting Findings Directly to Parties Outside the Audited Entity

4.30 Auditors should report known or likely fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse directly to parties outside the audited entity in the following two circumstances.

a. When entity management fails to satisfy legal or regulatory requirements to report such information to external parties specified in law or regulation, auditors should first communicate the failure to report such information to those charged with governance. If the audited entity still does not report this information to the specified external parties as soon as practicable after the auditors' communication with those charged with governance, then the auditors should report the information directly to the specified external parties.

b. When entity management fails to take timely and appropriate steps to respond to known or likely fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that (1) is likely to have a material effect on the financial statements and (2) involves funding received directly or indirectly from a government agency, auditors should first report management's failure to take timely and appropriate steps to those charged with governance. If the audited entity still does not take timely and

appropriate steps as soon as practicable after the auditors' communication with those charged with governance, then the auditors should report the entity's failure to take timely and appropriate steps directly to the funding agency.

4.31 The reporting in paragraph 4.30 is in addition to any legal requirements to report such information directly to parties outside the audited entity. Auditors should comply with these requirements even if they have resigned or been dismissed from the audit prior to its completion.

4.32 Auditors should obtain sufficient, appropriate evidence, such as confirmation from outside parties, to corroborate assertions by management of the audited entity that it has reported such findings in accordance with laws, regulations, or funding agreements. When auditors are unable to do so, they should report such information directly as discussed in paragraphs 4.30 and 4.31.

Reporting Views of Responsible Officials

4.33 When performing a GAGAS financial audit, if the auditors' report discloses deficiencies in internal control, fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse, auditors should obtain and report the views of responsible officials of the audited entity concerning the findings, conclusions, and recommendations, as well as any planned corrective actions.

4.34 Providing a draft report with findings for review and comment by responsible officials of the audited entity and others helps the auditors develop a report that is fair, complete, and objective. Including the views of responsible officials results in a report that presents not only the auditors' findings, conclusions, and recommendations, but also the perspectives of the

responsible officials of the audited entity and the corrective actions they plan to take. Obtaining the comments in writing is preferred, but oral comments are acceptable.

4.35 When auditors receive written comments from the responsible officials, they should include in their report a copy of the officials' written comments, or a summary of the comments received. When the responsible officials provide oral comments only, auditors should prepare a summary of the oral comments and provide a copy of the summary to the responsible officials to verify that the comments are accurately stated.

4.36 Auditors should also include in the report an evaluation of the comments, as appropriate. In cases in which the audited entity provides technical comments in addition to its written or oral comments on the report, auditors may disclose in the report that such comments were received.

4.37 Obtaining oral comments may be appropriate when, for example, there is a reporting date critical to meeting a user's needs; auditors have worked closely with the responsible officials throughout the work and the parties are familiar with the findings and issues addressed in the draft report; or the auditors do not expect major disagreements with findings, conclusions, or recommendations in the draft report, or major controversies with regard to the issues discussed in the draft report.

4.38 When the audited entity's comments are inconsistent or in conflict with the findings, conclusions, or recommendations in the draft report, or when planned corrective actions do not adequately address the auditors' recommendations, the auditors should evaluate the validity of the audited entity's comments. If the auditors disagree with the comments, they should

explain in the report their reasons for disagreement. Conversely, the auditors should modify their report as necessary if they find the comments valid and supported with sufficient, appropriate evidence.

4.39 If the audited entity refuses to provide comments or is unable to provide comments within a reasonable period of time, the auditors may issue the report without receiving comments from the audited entity. In such cases, the auditors should indicate in the report that the audited entity did not provide comments.

Reporting Confidential and Sensitive Information

4.40 When performing a GAGAS financial audit, if certain pertinent information is prohibited from public disclosure or is excluded from a report due to the confidential or sensitive nature of the information, auditors should disclose in the report that certain information has been omitted and the reason or other circumstances that make the omission necessary.

4.41 Certain information may be classified or may otherwise be prohibited from general disclosure by federal, state, or local laws or regulations. In such circumstances, auditors may issue a separate, classified, or limited use report containing such information and distribute the report only to persons authorized by law or regulation to receive it.

4.42 Additional circumstances associated with public safety, privacy, or security concerns could also justify the exclusion of certain information from a publicly available or widely distributed report. For example, detailed information related to computer security for a particular program may be excluded from publicly available reports because of the potential damage that could be caused by the misuse of this information. In such circumstances, auditors may issue a limited use report containing such information and distribute the

report only to those parties responsible for acting on the auditors' recommendations. In some instances, it may be appropriate to issue both a publicly available report with the sensitive information excluded and a limited use report. The auditors may consult with legal counsel regarding any requirements or other circumstances that may necessitate the omission of certain information.

4.43 Considering the broad public interest in the program or activity under audit assists auditors when deciding whether to exclude certain information from publicly available reports. When circumstances call for omission of certain information, auditors should evaluate whether this omission could distort the audit results or conceal improper or illegal practices.

4.44 When audit organizations are subject to public records laws, auditors should determine whether public records laws could impact the availability of classified or limited use reports and determine whether other means of communicating with management and those charged with governance would be more appropriate. For example, the auditors may communicate general information in a written report and communicate detailed information orally. The auditors may consult with legal counsel regarding applicable public records laws.

Distributing Reports

4.45 Distribution of reports completed in accordance with GAGAS depends on the relationship of the auditors to the audited organization and the nature of the information contained in the report. Auditors should document any limitation on report distribution.[74] The following discussion outlines distribution for reports completed in accordance with GAGAS:

[74]See paragraphs 4.41 and 4.42 for discussion of limited use reports containing confidential or sensitive information.

a. Audit organizations in government entities should distribute auditors' reports to those charged with governance, to the appropriate audited entity officials, and to the appropriate oversight bodies or organizations requiring or arranging for the audits. As appropriate, auditors should also distribute copies of the reports to other officials who have legal oversight authority or who may be responsible for acting on audit findings and recommendations, and to others authorized to receive such reports.

b. Internal audit organizations in government entities may also follow the Institute of Internal Auditors (IIA) *International Standards for the Professional Practice of Internal Auditing*.[75] In accordance with GAGAS and IIA standards, the head of the internal audit organization should communicate results to the parties who can ensure that the results are given due consideration. If not otherwise mandated by statutory or regulatory requirements, prior to releasing results to parties outside the organization, the head of the internal audit organization should: (1) assess the potential risk to the organization, (2) consult with senior management or legal counsel as appropriate, and (3) control dissemination by indicating the intended users in the report.

c. Public accounting firms contracted to perform an audit in accordance with GAGAS should clarify report distribution responsibilities with the engaging organization. If the contracting firm is responsible for the distribution, it should reach agreement with the party contracting for the audit about which officials or

[75]See paragraph 2.21 for additional discussion about using the IIA standards in conjunction with GAGAS and paragraph 2.22 for additional discussion about citing compliance with another set of standards.

organizations will receive the report and the steps being taken to make the report available to the public.

Additional GAGAS Considerations for Financial Audits

4.46 Due to the objectives and public accountability of GAGAS audits, additional considerations for financial audits completed in accordance with GAGAS may apply. These considerations relate to

a. materiality in GAGAS financial audits; and

b. early communication of deficiencies.[76]

Materiality in GAGAS Financial Audits

4.47 The AICPA standards require the auditor to apply the concept of materiality appropriately in planning and performing the audit.[77] Additional considerations may apply to GAGAS financial audits of government entities or entities that receive government awards. For example, in audits performed in accordance with GAGAS, auditors may find it appropriate to use lower materiality levels as compared with the materiality levels used in non-GAGAS audits because of the public accountability of government entities and entities receiving government funding, various legal and regulatory requirements, and the visibility and sensitivity of government programs.

[76]See paragraphs 4.47 through 4.48 for additional discussion of paragraph 4.46 a-b.

[77]See AICPA AU-C Section 320, *Materiality in Planning and Performing an Audit.*

Early Communication of Deficiencies

4.48 For some matters, early communication to those charged with governance or management may be important because of the relative significance and the urgency for corrective follow-up action.[78] Further, when a control deficiency results in noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse, early communication is important to allow management to take prompt corrective action to prevent further noncompliance. When a deficiency is communicated early, the reporting requirements in paragraphs 4.19 through 4.23 still apply.

[78]See AICPA AU-C Section 265, *Communicating Internal Control Related Matters Identified in an Audit.*

Standards for Attestation Engagements

Introduction

5.01 This chapter contains requirements, guidance, and considerations for performing and reporting on attestation engagements conducted in accordance with generally accepted government auditing standards (GAGAS). Auditors performing attestation engagements in accordance with GAGAS should comply with the American Institute of Certified Public Accountants (AICPA) general attestation standard on criteria, the field work and reporting attestation standards, and the corresponding statements on standards for attestation engagements (SSAEs), which are incorporated in this chapter by reference.[79] Auditors performing attestation engagements in accordance with GAGAS should also comply with the additional requirements in this chapter. The requirements and guidance contained in chapters 1 through 3 also apply to attestation engagements performed in accordance with GAGAS.

5.02 An attestation engagement can provide one of three levels of service as defined by the AICPA, namely an examination engagement, a review engagement, or an agreed-upon procedures engagement.[80] Auditors performing an attestation engagement should determine which of the three levels of service apply to that engagement and refer to the appropriate AICPA standards and GAGAS section below for applicable requirements and considerations.

[79]See AICPA AT Section 50, *SSAE Hierarchy.*

[80]See paragraph 2.09 and AICPA AT Section 101, *Attest Engagements*.

Examination Engagements

Additional Field Work Requirements for Examination Engagements

5.03 GAGAS establishes field work requirements for performing examination engagements in addition to the requirements contained in the AICPA standards. Auditors should comply with these additional requirements, along with the relevant AICPA standards for examination attestation engagements, when citing GAGAS in their examination reports. The additional field work requirements relate to:

a. auditor communication;

b. previous audits and attestation engagements;

c. fraud, noncompliance with provisions of laws, regulations, contracts, and grant agreements, and abuse;

d. developing elements of a finding; and

e. examination engagement documentation.[81]

Auditor Communication

5.04 In addition to the AICPA requirements for auditor communication,[82] when performing a GAGAS examination engagement, auditors should communicate pertinent information that in the auditors' professional judgment needs to be communicated to individuals contracting for or requesting the examination engagement, and to cognizant legislative committees

[81]See paragraphs 5.04 through 5.17 for additional discussion of 5.03 a-e.

[82]See AICPA AT Section 101.14 and 101.46, *Attest Engagements.*

when auditors perform the examination engagement pursuant to a law or regulation, or they conduct the work for the legislative committee that has oversight of the audited entity.

5.05 In those situations where there is not a single individual or group that both oversees the strategic direction of the audited entity and the fulfillment of its accountability obligations or in other situations where the identity of those charged with governance is not clearly evident, auditors should document the process followed and conclusions reached for identifying the appropriate individuals to receive the required auditor communications.

Previous Audits and Attestation Engagements

5.06 When performing a GAGAS examination engagement, auditors should evaluate whether the audited entity has taken appropriate corrective action to address findings and recommendations from previous engagements that could have a material effect on the subject matter, or an assertion about the subject matter, of the examination engagement. When planning the engagement, auditors should ask audited entity management to identify previous audits, attestation engagements, and other studies that directly relate to the subject matter or an assertion about the subject matter of the examination engagement being undertaken, including whether related recommendations have been implemented. Auditors should use this information in assessing risk and determining the nature, timing, and extent of current work, including determining the extent to which testing the implementation of the corrective actions is applicable to the current examination engagement objectives.

Fraud, Noncompliance with Provisions of Laws, Regulations, Contracts, and Grant Agreements, and Abuse

5.07 In addition to the AICPA requirements concerning fraud,[83] when performing a GAGAS examination engagement, auditors should design the engagement to detect instances of fraud and noncompliance with provisions of laws, regulations, contracts, and grant agreements that may have a material effect on the subject matter or the assertion thereon of the examination engagement. Auditors should assess the risk and possible effects of fraud and noncompliance with provisions of laws, regulations, contracts, and grant agreements that could have a material effect on the subject matter or an assertion about the subject matter of the examination engagement. When risk factors are identified, auditors should document the risk factors identified, the auditors' response to those risk factors individually or in combination, and the auditors' conclusions.[84]

5.08 Abuse involves behavior that is deficient or improper when compared with behavior that a prudent person would consider a reasonable and necessary business practice given the facts and circumstances. Abuse also includes misuse of authority or position for personal financial interests or those of an immediate or close family member or business associate.[85] Abuse does not necessarily involve fraud, or noncompliance with provisions of laws, regulations, contracts, or grant agreements.

[83]See AICPA AT Sections 501.27, *An Examination of an Entity's Internal Control Over Financial Reporting That Is Integrated With an Audit of Its Financial Statements*, 601.33, *Compliance Attestation*, and 701.42, *Management's Discussion and Analysis*.

[84]See paragraphs A.09 through A.13 for additional discussion of indicators of fraud risk and significance of provisions of laws, regulations, and contracts and grant agreements.

[85]See A.08 for additional examples of abuse.

5.09 Because the determination of abuse is subjective, auditors are not required to detect abuse in examination engagements. However, as part of a GAGAS examination engagement, if auditors become aware of abuse that could be quantitatively or qualitatively material, auditors should apply procedures specifically directed to ascertain the potential effect on the subject matter, or the assertion thereon, or other data significant to the objective of the examination engagement. After performing additional work, auditors may discover that the abuse represents potential fraud or noncompliance with provisions of laws, regulations, contracts, or grant agreements.

5.10 Avoiding interference with investigations or legal proceedings is important in pursuing indications of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse. Laws, regulations, or policies may require auditors to report indications of certain types of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse to law enforcement or investigatory authorities before performing additional audit procedures. When investigations or legal proceedings are initiated or in process, auditors should evaluate the impact on the current examination engagement. In some cases, it may be appropriate for the auditors to work with investigators or legal authorities, or withdraw from or defer further work on the examination engagement or a portion of the examination engagement to avoid interfering with an ongoing investigation or legal proceeding.

Developing Elements of a Finding

5.11 In an examination engagement, findings may involve deficiencies in internal control; noncompliance with provisions of laws, regulations, contracts, or grant agreements; fraud; or abuse. As part of a GAGAS examination engagement, when auditors identify

findings, auditors should plan and perform procedures to develop the elements of the findings that are relevant and necessary to achieve the examination engagement objectives. The elements of a finding are discussed in paragraphs 5.12 through 5.15 below.

5.12 Criteria: The laws, regulations, contracts, grant agreements, standards, measures, expected performance, defined business practices, and benchmarks against which performance is compared or evaluated. Criteria identify the required or desired state or expectation with respect to the program or operation. Criteria provide a context for evaluating evidence and understanding the findings.

5.13 Condition: Condition is a situation that exists. The condition is determined and documented during the engagement.

5.14 Cause: The cause identifies the reason or explanation for the condition or the factor or factors responsible for the difference between the situation that exists (condition) and the required or desired state (criteria), which may also serve as a basis for recommendations for corrective actions. Common factors include poorly designed policies, procedures, or criteria; inconsistent, incomplete, or incorrect implementation; or factors beyond the control of program management. Auditors may assess whether the evidence provides a reasonable and convincing argument for why the stated cause is the key factor or factors contributing to the difference between the condition and the criteria.

5.15 Effect or potential effect: The effect is a clear, logical link to establish the impact or potential impact of the difference between the situation that exists (condition) and the required or desired state (criteria). The effect or potential effect identifies the outcomes or

consequences of the condition. When the engagement objectives include identifying the actual or potential consequences of a condition that varies (either positively or negatively) from the criteria identified in the engagement, "effect" is a measure of those consequences. Effect or potential effect may be used to demonstrate the need for corrective action in response to identified problems or relevant risks.

Examination Engagement Documentation

5.16 In addition to AICPA requirements for audit documentation,[86] auditors should comply with the following additional requirements when performing a GAGAS examination engagement.[87]

a. Prepare attest documentation in sufficient detail to enable an experienced auditor, having no previous connection to the examination engagement, to understand from the documentation the nature, timing, extent, and results of procedures performed and the evidence obtained and its source and the conclusions reached, including evidence that supports the auditors' significant judgments and conclusions. An experienced auditor means an individual (whether internal or external to the audit organization) who possesses the competencies and skills to be able to perform the examination engagement. These competencies and skills include an understanding of (1) examination engagement processes and related SSAEs,[88] (2) GAGAS and applicable legal and regulatory requirements, (3) the subject matter that the auditors are engaged to report on, (4) the suitability and

[86]See AICPA AT Section 101.100–101.107, *Attest Engagements.*

[87]See paragraphs 5.05, 5.07, 5.25, and 5.44 for additional documentation requirements regarding attestation engagements.

[88]See paragraphs 3.74 and 3.75 for additional discussion of qualifications for attestation engagements.

availability of criteria, and (5) issues related to the audited entity's environment.

b. Document supervisory review, before the date of the examination report, of the evidence that supports findings, conclusions, and recommendations contained in the examination report.

c. Document any departures from the GAGAS requirements and the impact on the engagement and on the auditors' conclusions when the examination engagement is not in compliance with applicable GAGAS requirements due to law, regulation, scope limitations, restrictions on access to records, or other issues impacting the audit. This applies to departures from unconditional requirements and from presumptively mandatory requirements when alternative procedures performed in the circumstances were not sufficient to achieve the objectives of the requirement.[89]

5.17 When performing GAGAS examination engagements and subject to applicable laws and regulations, auditors should make appropriate individuals, as well as attest documentation, available upon request and in a timely manner to other auditors or reviewers. Underlying GAGAS engagements is the premise that audit organizations in federal, state, and local governments and public accounting firms engaged to perform an engagement in accordance with GAGAS cooperate in performing examination engagements of programs of common interest so that auditors may use others' work and avoid duplication of efforts. The use of auditors' work by other auditors may be facilitated by contractual arrangements for GAGAS engagements

[89]See paragraph 2.15 for a definition of GAGAS requirements.

that provide for full and timely access to appropriate individuals, as well as attest documentation.

Additional GAGAS Reporting Requirements for Examination Engagements

5.18 In addition to the AICPA requirements for reporting on examination engagements,[90] auditors should comply with the following additional requirements when citing GAGAS in their examination reports. The additional reporting requirements relate to

a. reporting auditors' compliance with GAGAS;

b. reporting deficiencies in internal control, fraud, noncompliance with provisions of laws, regulations, contracts, and grant agreements, and abuse;

c. reporting views of responsible officials;

d. reporting confidential or sensitive information; and

e. distributing reports.[91]

Reporting Auditors' Compliance with GAGAS

5.19 When auditors comply with all applicable GAGAS requirements for examination engagements, they should include a statement in the examination report that they performed the examination engagement in accordance with GAGAS.[92] Because GAGAS incorporates by reference the AICPA's general attestation standard on criteria, the field work and reporting attestation standards, and the corresponding SSAEs, GAGAS does not require auditors to cite

[90]See AICPA AT Section 101.63-101.87, *Attest Engagements*.

[91]See paragraphs 5.19 through 5.44 for additional discussion of paragraph 5.18 a-e.

[92]See paragraphs 2.24 and 2.25 for additional requirements on citing compliance with GAGAS.

compliance with the AICPA standards when citing compliance with GAGAS. GAGAS does not prohibit auditors from issuing a separate report conforming only to the requirements of AICPA or other standards.[93]

Reporting Deficiencies in Internal Control, Fraud, Noncompliance with Provisions of Laws, Regulations, Contracts, and Grant Agreements, and Abuse

5.20 When performing GAGAS examination engagements, auditors should report, based upon the work performed, (1) significant deficiencies and material weaknesses in internal control;[94] (2) instances of fraud[95] and noncompliance with provisions of laws or regulations that have a material effect on the subject matter or an assertion about the subject matter and any other instances that warrant the attention of those charged with governance; (3) noncompliance with provisions of contracts or grant agreements that has a material effect on the subject matter or an assertion about the subject matter of the examination engagement; and (4) abuse that has a material effect on the subject matter or an assertion about the subject matter of the examination engagement. Auditors should include this information either in the same or in separate report(s).

5.21 If auditors report separately (including separate reports bound in the same document) on the items discussed in paragraph 5.20, they should state in the examination report that they are issuing those additional reports. They should include a reference to the separate reports and also state that the reports are an integral part of a GAGAS examination engagement.

[93]See AICPA AT Sections 101.85e, *Attest Engagements.*

[94]See paragraph A.06 for examples of deficiencies in internal control.

[95]See paragraph A.10 for examples of indicators of fraud risk.

Deficiencies in Internal Control

5.22 In addition to the AICPA requirements concerning internal control, [96] when performing GAGAS examination engagements, including attestation engagements related to internal control,[97] auditors should include in the examination report all deficiencies, even those communicated early,[98] that are considered to be significant deficiencies or material weaknesses.

5.23 Determining whether and how to communicate to officials of the audited entity internal control deficiencies that warrant the attention of those charged with governance, but are not considered significant deficiencies or material weaknesses, is a matter of professional judgment.

Fraud, Noncompliance with Provisions of Laws, Regulations, Contracts, and Grant Agreements, and Abuse

5.24 When performing a GAGAS examination engagement, and auditors conclude, based on sufficient, appropriate evidence, that any of the following either has occurred or is likely to have occurred, they should include in their examination report the relevant information about

a. fraud[99] and noncompliance with provisions of laws or regulations that have a material effect on the subject matter or an assertion about the subject matter and any other instances that warrant the attention of those charged with governance,

[96]See AICPA AT Section 101.52 through 101.53, *Attest Engagements*.

[97]See AICPA AT Section 501.07, *An Examination of an Entity's Internal Control Over Financial Reporting That Is Integrated With an Audit of Its Financial Statements*.

[98]See paragraph 5.47 for a discussion of early communication of deficiencies.

[99]See paragraph A.10 for examples of indicators of fraud risk.

b. noncompliance with provisions of contracts or grant agreements that has a material effect on the subject matter or an assertion about the subject matter, or

c. abuse[100] that is material to the subject matter or an assertion about the subject matter, either quantitatively or qualitatively.[101]

5.25 When auditors detect instances of noncompliance with provisions of contracts or grant agreements, or abuse that have an effect on the subject matter or an assertion about the subject matter that are less than material but warrant the attention of those charged with governance, they should communicate those findings in writing to audited entity officials. When auditors detect any instances of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that do not warrant the attention of those charged with governance, the auditors' determination of whether and how to communicate such instances to audited entity officials is a matter of professional judgment.

5.26 When fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse either have occurred or are likely to have occurred, auditors may consult with authorities or legal counsel about whether publicly reporting such information would compromise investigative or legal proceedings. Auditors may limit their public reporting to matters that would not compromise those proceedings and, for example, report only on information that is already a part of the public record.

[100]See paragraph A.08 for examples of abuse.

[101]See paragraphs 5.08 and 5.09 for a discussion of abuse.

Presenting Findings in the Examination Report

5.27 When performing a GAGAS examination engagement and presenting findings such as deficiencies in internal control, fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse, auditors should develop the elements of the findings to the extent necessary. Clearly developed findings, as discussed in paragraphs 5.11 through 5.15, assist management or oversight officials of the audited entity in understanding the need for taking corrective action, and assist auditors in making recommendations for corrective action. If auditors sufficiently develop the elements of a finding, they may provide recommendations for corrective action.

5.28 Auditors should place their findings in perspective by describing the nature and extent of the issues being reported and the extent of the work performed that resulted in the finding. To give the reader a basis for judging the prevalence and consequences of these findings, auditors should, as appropriate, relate the instances identified to the population or the number of cases examined and quantify the results in terms of dollar value or other measures. If the results cannot be projected, auditors should limit their conclusions appropriately.

Reporting Findings Directly to Parties Outside the Audited Entity

5.29 Auditors should report known or likely fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse directly to parties outside the audited entity in the following two circumstances.

a. When entity management fails to satisfy legal or regulatory requirements to report such information to external parties specified in law or regulation, auditors should first communicate the failure to report such information to those charged with governance. If the audited entity still does not report this information to the specified external parties as soon as practicable after

the auditors' communication with those charged with governance, then the auditors should report the information directly to the specified external parties.

b. When entity management fails to take timely and appropriate steps to respond to known or likely fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that (1) is likely to have a material effect on the subject matter or an assertion about the subject matter and (2) involves funding received directly or indirectly from a government agency, auditors should first report management's failure to take timely and appropriate steps to those charged with governance. If the audited entity still does not take timely and appropriate steps as soon as practicable after the auditors' communication with those charged with governance, then the auditors should report the entity's failure to take timely and appropriate steps directly to the funding agency.

5.30 The reporting in paragraph 5.29 is in addition to any legal requirements to report such information directly to parties outside the audited entity. Auditors should comply with these requirements even if they have resigned or been dismissed from the engagement prior to its completion.

5.31 Auditors should obtain sufficient, appropriate evidence, such as confirmation from outside parties, to corroborate assertions by management of the audited entity that it has reported such findings in accordance with laws, regulations, or funding agreements. When auditors are unable to do so, they should report such information directly as discussed in paragraph 5.29.

Reporting Views of Responsible Officials

5.32 When performing a GAGAS examination engagement, if the examination report discloses deficiencies in internal control, fraud, noncompliance

with provisions of laws, regulations, contracts, or grant agreements, or abuse, auditors should obtain and report the views of responsible officials of the audited entity concerning the findings, conclusions, and recommendations, as well as any planned corrective actions.

5.33 Providing a draft report with findings for review and comment by responsible officials of the audited entity and others helps the auditors develop a report that is fair, complete, and objective. Including the views of responsible officials results in a report that presents not only the auditors' findings, conclusions, and recommendations, but also the perspectives of the responsible officials of the audited entity and the corrective actions they plan to take. Obtaining the comments in writing is preferred, but oral comments are acceptable.

5.34 When auditors receive written comments from the responsible officials, they should include in their report a copy of the officials' written comments, or a summary of the comments received. When the responsible officials provide oral comments only, auditors should prepare a summary of the oral comments and provide a copy of the summary to the responsible officials to verify that the comments are accurately stated.

5.35 Auditors should also include in the report an evaluation of the comments, as appropriate. In cases in which the audited entity provides technical comments in addition to its written or oral comments on the report, auditors may disclose in the report that such comments were received.

5.36 Obtaining oral comments may be appropriate when, for example, there is a reporting date critical to meeting a user's needs; auditors have worked closely with the responsible officials throughout the work and

the parties are familiar with the findings and issues addressed in the draft report; or the auditors do not expect major disagreements with findings, conclusions, or recommendations in the draft report, or major controversies with regard to the issues discussed in the draft report.

5.37 When the audited entity's comments are inconsistent or in conflict with the findings, conclusions, or recommendations in the draft report, or when planned corrective actions do not adequately address the auditors' recommendations, the auditors should evaluate the validity of the audited entity's comments. If the auditors disagree with the comments, they should explain in the report their reasons for disagreement. Conversely, the auditors should modify their report as necessary if they find the comments valid and supported with sufficient, appropriate evidence.

5.38 If the audited entity refuses to provide comments or is unable to provide comments within a reasonable period of time, the auditors may issue the report without receiving comments from the audited entity. In such cases, the auditors should indicate in the report that the audited entity did not provide comments.

Reporting Confidential and Sensitive Information

5.39 When performing a GAGAS examination engagement, if certain pertinent information is prohibited from public disclosure or is excluded from a report due to the confidential or sensitive nature of the information, auditors should disclose in the report that certain information has been omitted and the reason or other circumstances that make the omission necessary.

5.40 Certain information may be classified or may be otherwise prohibited from general disclosure by federal, state, or local laws or regulations. In such circumstances, auditors may issue a separate classified

or limited use report containing such information and distribute the report only to persons authorized by law or regulation to receive it.

5.41 Additional circumstances associated with public safety, privacy, or security concerns could also justify the exclusion of certain information from a publicly available or widely distributed report. For example, detailed information related to computer security for a particular program may be excluded from publicly available reports because of the potential damage that could be caused by the misuse of this information. In such circumstances, auditors may issue a limited use report containing such information and distribute the report only to those parties responsible for acting on the auditors' recommendations. In some instances, it may be appropriate to issue both a publicly available report with the sensitive information excluded and a limited use report. The auditors may consult with legal counsel regarding any requirements or other circumstances that may necessitate the omission of certain information.

5.42 Considering the broad public interest in the program or activity under review assists auditors when deciding whether to exclude certain information from publicly available reports. When circumstances call for omission of certain information, auditors should evaluate whether this omission could distort the examination engagement results or conceal improper or illegal practices.

5.43 When audit organizations are subject to public records laws, auditors should determine whether public records laws could impact the availability of classified or limited use reports and determine whether other means of communicating with management and those charged with governance would be more appropriate. For example, the auditors may communicate general information in a written report and communicate

detailed information orally. The auditors may consult with legal counsel regarding applicable public records laws.

Distributing Reports

5.44 Distribution of reports completed in accordance with GAGAS depends on the relationship of the auditors to the audited organization and the nature of the information contained in the report. Auditors should document any limitation on report distribution.[102] The following discussion outlines distribution for reports completed in accordance with GAGAS:

a. Audit organizations in government entities should distribute reports to those charged with governance, to the appropriate audited entity officials, and to the appropriate oversight bodies or organizations requiring or arranging for the engagements. As appropriate, auditors should also distribute copies of the reports to other officials who have legal oversight authority or who may be responsible for acting on engagement findings and recommendations, and to others authorized to receive such reports.

b. Internal audit organizations in government entities may also follow the Institute of Internal Auditors (IIA) *International Standards for the Professional Practice of Internal Auditing*.[103] In accordance with GAGAS and IIA standards, the head of the internal audit organization should communicate results to the parties who can ensure that the results are given due consideration. If not otherwise mandated by statutory or regulatory

[102]See paragraphs 5.40 and 5.41 for discussion of limited use reports containing confidential or sensitive information.

[103]See paragraph 2.21 for additional discussion about using the IIA standards in conjunction with GAGAS and paragraph 2.22 for additional discussion about citing compliance with another set of standards.

requirements, prior to releasing results to parties outside the organization, the head of the internal audit organization should: (1) assess the potential risk to the organization, (2) consult with senior management or legal counsel as appropriate, and (3) control dissemination by indicating the intended users in the report.

c. Public accounting firms contracted to perform an examination engagement in accordance with GAGAS should clarify report distribution responsibilities with the engaging organization. If the contracting firm is responsible for the distribution, it should reach agreement with the party contracting for the engagement about which officials or organizations will receive the report and the steps being taken to make the report available to the public.

Additional GAGAS Considerations for Examination Engagements

5.45 Due to the objectives and public accountability of GAGAS examination engagements, additional considerations for examination engagements completed in accordance with GAGAS may apply. These considerations relate to

a. Materiality in GAGAS examination engagements, and

b. Early communication of deficiencies.[104]

Materiality in GAGAS Examination Engagements

5.46 The AICPA standards require that one of the factors to be considered when planning an attest engagement includes preliminary judgments about attestation risk and materiality for attest purposes.[105]

[104]See paragraphs 5.46 and 5.47 for additional discussion of paragraph 5.45 a-b.

[105]See AICPA AT Section 101.45b and 101.67, *Attest Engagements.*

Additional considerations may apply to GAGAS examination engagements of government entities or entities that receive government awards. For example, in engagements performed in accordance with GAGAS, auditors may find it appropriate to use lower materiality levels as compared with the materiality levels used in non-GAGAS engagements because of the public accountability of government entities and entities receiving government funding, various legal and regulatory requirements, and the visibility and sensitivity of government programs.

Early Communication of Deficiencies

5.47 For some matters, early communication to those charged with governance or management may be important because of the relative significance and the urgency for corrective follow-up action.[106] Further, when a control deficiency results in noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse, early communication is important to allow management to take prompt corrective action to prevent further noncompliance. When a deficiency is communicated early, the reporting requirements in paragraph 5.20 still apply.

[106]See AICPA AT Section 501.103, *An Examination of an Entity's Internal Control Over Financial Reporting That Is Integrated With an Audit of Its Financial Statements*.

Review Engagements

Additional GAGAS Field Work Requirements for Review Engagements

5.48 GAGAS establishes a field work requirement for review engagements in addition to the requirements contained in the AICPA standards. Auditors should comply with this additional requirement, along with the relevant AICPA standards for review engagements, when citing GAGAS in their review engagement reports. The additional requirement relates to communicating significant deficiencies, material weaknesses, instances of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that come to the auditors' attention during a review engagement.

Communicating Significant Deficiencies, Material Weaknesses, Instances of Fraud, Noncompliance with Provisions of Laws, Regulations, Contracts, and Grant Agreements, and Abuse

5.49 If, on the basis of conducting the procedures necessary to perform a review, significant deficiencies; material weaknesses; instances of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements; or abuse come to the auditors' attention that warrant the attention of those charged with governance, GAGAS requires that auditors should communicate such matters to audited entity officials. When auditors detect any instances of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that do not warrant the attention of those charged with governance, the auditors' determination of whether and how to communicate such instances to audited entity officials is a matter of professional judgment. Additionally, auditors should determine whether the existence of such matters affects the auditors' ability to conduct or report on the review.

Additional GAGAS Reporting Requirements for Review Engagements

5.50 GAGAS establishes reporting requirements for review engagements in addition to the requirements contained in the AICPA standards.[107] Auditors should comply with these additional requirements when citing GAGAS in their review engagement reports. The additional requirements relate to

a. reporting auditors' compliance with GAGAS; and

b. distributing reports.[108]

Reporting Auditors' Compliance with GAGAS

5.51 When auditors comply with all applicable requirements for a review engagement conducted in accordance with GAGAS, they should include a statement in the review report that they performed the engagement in accordance with GAGAS.[109] Because GAGAS incorporates by reference the general standard on criteria, and the field work and reporting standards of the AICPA SSAEs, GAGAS does not require auditors to cite compliance with the AICPA standards when citing compliance with GAGAS. GAGAS does not prohibit auditors from issuing a separate report conforming only to the requirements of AICPA or other standards.[110]

Distributing Reports

5.52 Distribution of reports completed in accordance with GAGAS depends on the relationship of the auditors to the audited organization and the nature of the

[107]See AICPA AT Section 101.63-101.83 and 101.88-101.90, *Attest Engagements*.

[108]See paragraphs 5.51 and 5.52 for additional discussion of paragraph 5.50 a-b.

[109]See paragraphs 2.24 and 2.25 for additional requirements on citing compliance with GAGAS.

[110]See AICPA AT Section 101.89d, *Attest Engagements.*

information contained in the report. For GAGAS review engagements, if the subject matter or the assertion involves material that is classified for security purposes or contains confidential or sensitive information, auditors should limit the report distribution. Auditors should document any limitation on report distribution. The following discussion outlines distribution for reports completed in accordance with GAGAS:

a. Audit organizations in government entities should distribute reports to those charged with governance, to the appropriate audited entity officials, and to the appropriate oversight bodies or organizations requiring or arranging for the engagements. As appropriate, auditors should also distribute copies of the reports to other officials who have legal oversight authority, and to others authorized to receive such reports.

b. Internal audit organizations in government entities may also follow the Institute of Internal Auditors (IIA) *International Standards for the Professional Practice of Internal Auditing*.[111] In accordance with GAGAS and IIA standards, the head of the internal audit organization should communicate results to the parties who can ensure that the results are given due consideration. If not otherwise mandated by statutory or regulatory requirements, prior to releasing results to parties outside the organization, the head of the internal audit organization should: (1) assess the potential risk to the organization, (2) consult with senior management or legal counsel as appropriate, and (3) control dissemination by indicating the intended users in the report.

[111]See paragraph 2.21 for additional discussion about using the IIA standards in conjunction with GAGAS and paragraph 2.22 for additional discussion about citing compliance with another set of standards.

c. Public accounting firms contracted to perform a review engagement in accordance with GAGAS should clarify report distribution responsibilities with the engaging organization. If the contracting firm is responsible for the distribution, it should reach agreement with the party contracting for the engagement about which officials or organizations will receive the report and the steps being taken to make the report available to the public.

Additional GAGAS Considerations for Review Engagements

5.53 Due to the objectives and public accountability of GAGAS review engagements, additional considerations for review engagements performed in accordance with GAGAS may apply. These considerations relate to

a. establishing an understanding regarding services to be performed; and

b. reporting on review engagements.[112]

Establishing an Understanding Regarding Services to be Performed

5.54 The AICPA standards require auditors to establish an understanding with the audited entity (client) regarding the services to be performed for each attestation engagement. Such an understanding reduces the risk that either the auditors (practitioner) or the audited entity may misinterpret the needs or expectations of the other party. The understanding includes the objectives of the engagement, responsibilities of entity management, responsibilities of auditors, and limitations of the engagement.[113]

[112]See paragraphs 5.54 through 5.57 for additional discussion of 5.53 a-b.

[113]See AICPA AT Section 101.46, *Attest Engagements*.

5.55 Auditors often perform GAGAS engagements under a contract with a party other than the officials of the audited entity or pursuant to a third-party request. In such cases, auditors may also find it appropriate to communicate information regarding the services to be performed to the individuals contracting for or requesting the engagement. Such an understanding can help auditors avoid any misunderstandings regarding the nature of the review engagement. For example, review engagements only provide a moderate level of assurance expressed as a conclusion in the form of negative assurance, and, as a result, auditors do not perform sufficient work to be able to develop elements of a finding or provide recommendations that are common in other types of GAGAS engagements. Under such circumstances, for example, requesting parties may find that a different type of attestation engagement or a performance audit may provide the appropriate level of assurance to meet their needs.

Reporting on Review Engagements

5.56 The AICPA standards require that the auditors' review report be in the form of a conclusion expressed in the form of negative assurance.[114]

5.57 Because reviews are substantially less in scope than audits and examination engagements, it is important to include all required reporting elements contained in the SSAEs.[115] For example, a required element of the review report is a statement that a review engagement is substantially less in scope than an examination, the objective of which is an expression of opinion on the subject matter, and accordingly, review reports express no such opinion. Including only those elements that the AICPA reporting standards for review

[114]See AICPA AT Section 101.68, *Attest Engagements*.

[115]See AICPA AT Section 101.89, *Attest Engagements.*

engagements require or permit ensures that auditors comply with the AICPA standards and that users of GAGAS reports have an understanding of the nature of the work performed and the results of the review engagement.

Agreed-Upon Procedures Engagements

Additional GAGAS Field Work Requirements for Agreed-Upon Procedures Engagements

5.58 GAGAS establishes a field work requirement for agreed-upon procedures engagements in addition to the requirements contained in the AICPA standards. Auditors should comply with this additional requirement, along with the relevant AICPA standards for agreed-upon procedures engagements, when citing GAGAS in their agreed-upon procedures engagement reports. The additional requirement relates to communicating significant deficiencies, material weaknesses, instances of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that comes to the auditors' attention during an agreed-upon procedures engagement.

Communicating Significant Deficiencies, Material Weaknesses, Instances of Fraud, Noncompliance with Provisions of Laws, Regulations, Contracts, and Grant Agreements, and Abuse

5.59 If, on the basis of conducting the procedures necessary to perform an agreed-upon procedures engagement,[116] significant deficiencies, material weaknesses, instances of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse come to the auditors' attention that warrant the attention of those charged with governance, GAGAS requires that auditors should communicate such matters to audited entity officials. When auditors detect any instances of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that do not warrant the attention of those charged with governance, the auditors' determination of whether and how to communicate such instances to audited entity officials is a matter of professional judgment. Additionally, auditors should determine whether the existence of such matters affects the auditors' ability to conduct or report on the agreed-upon procedures engagement.

Additional GAGAS Reporting Requirements for Agreed-Upon Procedures Engagements

5.60 GAGAS establishes reporting requirements for agreed-upon procedures engagements in addition to the requirements contained in the AICPA standards.[117] Auditors should comply with these additional requirements when citing GAGAS in their agreed-upon procedures engagement reports. The additional requirements relate to

a. reporting auditors' compliance with GAGAS; and

[116]See AICPA AT Section 201.03, *Agreed-Upon Procedures Engagements*.

[117]See AICPA AT Section 201.31-201.36, *Agreed-Upon Procedures Engagements*.

b. distributing reports.[118]

Reporting Auditors' Compliance with GAGAS

5.61 When auditors comply with all applicable GAGAS requirements for agreed-upon procedures engagements, they should include a statement in the agreed-upon procedures engagement report that they performed the engagement in accordance with GAGAS.[119] Because GAGAS incorporates by reference the AICPA's general attestation standard on criteria, the field work and reporting attestation standards, and the corresponding SSAEs, GAGAS does not require auditors to cite compliance with the AICPA standards when citing compliance with GAGAS. GAGAS does not prohibit auditors from issuing a separate report conforming only to the requirements of AICPA or other standards.[120]

Distributing Reports

5.62 Distribution of reports completed in accordance with GAGAS depends on the relationship of the auditors to the audited organization and the nature of the information contained in the report. For GAGAS agreed-upon procedures engagements, if the subject matter or the assertion involves material that is classified for security purposes or contains confidential or sensitive information, auditors should limit the report distribution. Auditors should document any limitation on report distribution. The following discussion outlines distribution for reports completed in accordance with GAGAS:

[118]See paragraphs 5.61 and 5.62 for additional discussion of paragraph 5.60 a-b.

[119]See paragraphs 2.24 and 2.25 for additional requirements on citing compliance with GAGAS.

[120]See AICPA AT Section 201.31 g, *Agreed-Upon Procedures Engagements.*

a. Audit organizations in government entities should distribute reports to those charged with governance, to the appropriate audited entity officials, and to the appropriate oversight bodies or organizations requiring or arranging for the engagements. As appropriate, auditors should also distribute copies of the reports to other officials who have legal oversight authority, and to others authorized to receive such reports.

b. Internal audit organizations in government entities may also follow the Institute of Internal Auditors (IIA) *International Standards for the Professional Practice of Internal Auditing*.[121] In accordance with GAGAS and IIA standards, the head of the internal audit organization should communicate results to the parties who can ensure that the results are given due consideration. If not otherwise mandated by statutory or regulatory requirements, prior to releasing results to parties outside the organization, the head of the internal audit organization should: (1) assess the potential risk to the organization, (2) consult with senior management or legal counsel as appropriate, and (3) control dissemination by indicating the intended users in the report.

c. Public accounting firms contracted to perform an agreed-upon procedures engagement in accordance with GAGAS should clarify report distribution responsibilities with the engaging organization. If the contracting firm is responsible for the distribution, it should reach agreement with the party contracting for the engagement about which officials or organizations will receive the report and the steps being taken to make the report available to the public.

[121]See paragraph 2.21 for additional discussion about using the IIA standards in conjunction with GAGAS and paragraph 2.22 for additional discussion about citing compliance with another set of standards.

Additional GAGAS Considerations for Agreed-Upon Procedures Engagements

5.63 Due to the objectives and public accountability of GAGAS agreed-upon procedures engagements, additional considerations for agreed-upon procedures engagements performed in accordance with GAGAS may apply. These considerations relate to

a. establishing an understanding regarding services to be performed; and

b. reporting on agreed-upon procedures engagements.[122]

Establishing an Understanding Regarding Services to be Performed

5.64 The AICPA standards require auditors to establish an understanding with the audited entity (client) regarding the services to be performed for each attestation engagement. Such an understanding reduces the risk that either the auditors (practitioner) or the audited entity may misinterpret the needs or expectations of the other party. The understanding includes the objectives of the engagement, responsibilities of entity management, responsibilities of auditors, and limitations of the engagement.[123]

5.65 Auditors often perform GAGAS engagements under a contract with a party other than the officials of the audited entity or pursuant to a third-party request. In such cases, auditors may also find it appropriate to communicate information regarding the services to be performed to the individuals contracting for or requesting the engagement. Such an understanding can help auditors avoid any misunderstandings regarding the nature of the agreed-upon procedures

[122]See paragraphs 5.64 through 5.67 for additional discussion of paragraph 5.63 a-b.

[123]See AICPA AT Sections 101.46, *Attest Engagements,* and 201.10, *Agreed-Upon Procedures Engagements*.

engagement. For example, agreed-upon procedures engagements provide neither a high nor moderate level of assurance, and, as a result, auditors do not perform sufficient work to be able to develop elements of a finding or provide recommendations that are common in other types of GAGAS engagements. Under such circumstances, for example, requesting parties may find that a different type of attestation engagement or a performance audit may provide the appropriate level of assurance to meet their needs.

Reporting on Agreed-Upon Procedures Engagements

5.66 The AICPA standards require that the auditors' report on agreed-upon procedures engagements be in the form of procedures and findings and specifies the required elements to be contained in the report.[124]

5.67 Because GAGAS agreed-upon procedures engagements are substantially less in scope than audits and examination engagements, it is important not to deviate from the required reporting elements contained in the SSAEs. For example, a required element of the report on agreed-upon procedures is a statement that the auditors were not engaged to and did not conduct an examination or a review of the subject matter, the objectives of which would be the expression of an opinion or limited assurance and that if the auditors had performed additional procedures, other matters might have come to their attention that would have been reported.[125] Another required element is a statement that the sufficiency of the procedures is solely the responsibility of the specified parties and a disclaimer of

[124]See AICPA AT Section 201.31, *Agreed-Upon Procedures Engagements*.

[125]See AICPA AT Section 201.31k, *Agreed-Upon Procedures Engagements*.

responsibility for the sufficiency of those procedures.[126] Including only those elements that the AICPA reporting standards for agreed-upon procedure engagements require or permit ensures that auditors comply with the AICPA standards and that users of GAGAS reports have an understanding of the nature of the work performed and the results of the agreed-upon procedures engagement.

[126]See AICPA AT Section 201.31h and 201.11-201.14, *Agreed-Upon Procedures Engagements*.

Field Work Standards for Performance Audits

Introduction

6.01 This chapter contains field work requirements and guidance for performance audits conducted in accordance with generally accepted government auditing standards (GAGAS). The purpose of field work requirements is to establish an overall approach for auditors to apply in obtaining reasonable assurance that the evidence is sufficient and appropriate to support the auditors' findings and conclusions. The field work requirements for performance audits relate to planning the audit; supervising staff; obtaining sufficient, appropriate evidence; and preparing audit documentation. The concepts of reasonable assurance, significance, and audit risk form a framework for applying these requirements and are included throughout the discussion of performance audits.

6.02 For performance audits conducted in accordance with GAGAS, the requirements and guidance in chapters 1 through 3, 6, and 7 apply.

Reasonable Assurance

6.03 In performance audits that comply with GAGAS, auditors obtain reasonable assurance that evidence is sufficient and appropriate to support the auditors' findings and conclusions in relation to the audit objectives.[127] Thus, the sufficiency and appropriateness of evidence needed and tests of evidence will vary based on the audit objectives, findings, and conclusions. Objectives for performance audits range from narrow to broad and involve varying types and quality of evidence. In some engagements, sufficient, appropriate evidence is available, but in others, information may have limitations. Professional judgment assists auditors in determining the audit scope and methodology needed to address the audit objectives,

[127]See paragraphs 2.11 and A2.02 for additional discussion of performance audit objectives.

and in evaluating whether sufficient, appropriate evidence has been obtained to address the audit objectives.

Significance in a Performance Audit

6.04 The concept of significance assists auditors throughout a performance audit, including when deciding the type and extent of audit work to perform, when evaluating results of audit work, and when developing the report and related findings and conclusions. Significance is defined as the relative importance of a matter within the context in which it is being considered, including quantitative and qualitative factors. Such factors include the magnitude of the matter in relation to the subject matter of the audit, the nature and effect of the matter, the relevance of the matter, the needs and interests of an objective third party with knowledge of the relevant information, and the impact of the matter to the audited program or activity. Professional judgment assists auditors when evaluating the significance of matters within the context of the audit objectives. In the performance audit requirements, the term “significant” is comparable to the term “material” as used in the context of financial statement engagements.

Audit Risk

6.05 Audit risk is the possibility that the auditors’ findings, conclusions, recommendations, or assurance may be improper or incomplete, as a result of factors such as evidence that is not sufficient and/or appropriate, an inadequate audit process, or intentional omissions or misleading information due to misrepresentation or fraud. The assessment of audit risk involves both qualitative and quantitative considerations. Factors impacting audit risk include the time frames, complexity, or sensitivity of the work; size of the program in terms of dollar amounts and number of citizens served; adequacy of the audited entity’s

systems and processes to detect inconsistencies, significant errors, or fraud; and auditors' access to records. Audit risk includes the risk that auditors will not detect a mistake, inconsistency, significant error, or fraud in the evidence supporting the audit. Audit risk can be reduced by taking actions such as increasing the scope of work; adding specialists, additional reviewers, and other resources to perform the audit; changing the methodology to obtain additional evidence, higher quality evidence, or alternative forms of corroborating evidence; or aligning the findings and conclusions to reflect the evidence obtained.

Planning

6.06 Auditors must adequately plan and document the planning of the work necessary to address the audit objectives.

6.07 Auditors must plan the audit to reduce audit risk to an appropriate level for the auditors to obtain reasonable assurance that the evidence is sufficient and appropriate[128] to support the auditors' findings and conclusions. This determination is a matter of professional judgment. In planning the audit, auditors should assess significance and audit risk and apply these assessments in defining the audit objectives and the scope and methodology to address those objectives. Planning is a continuous process throughout the audit. Therefore, auditors may need to adjust the audit objectives, scope, and methodology as work is being completed. In situations where the audit objectives are established by statute or legislative oversight, auditors may not have latitude to define or adjust the audit objectives or scope.

[128]See paragraphs 6.56 through 6.72 for a discussion about assessing the sufficiency and appropriateness of evidence.

6.08 The objectives are what the audit is intended to accomplish. They identify the audit subject matter and performance aspects to be included, and may also include the potential findings and reporting elements that the auditors expect to develop. Audit objectives can be thought of as questions about the program that the auditors seek to answer based on evidence obtained and assessed against criteria. The term “program” is used in GAGAS to include government entities, organizations, programs, activities, and functions.

6.09 Scope is the boundary of the audit and is directly tied to the audit objectives. The scope defines the subject matter that the auditors will assess and report on, such as a particular program or aspect of a program, the necessary documents or records, the period of time reviewed, and the locations that will be included.

6.10 The methodology describes the nature and extent of audit procedures for gathering and analyzing evidence to address the audit objectives. Audit procedures are the specific steps and tests auditors perform to address the audit objectives. Auditors should design the methodology to obtain reasonable assurance that the evidence is sufficient and appropriate to support the auditors’ findings and conclusions in relation to the audit objectives and to reduce audit risk to an acceptable level.

6.11 Auditors should assess audit risk and significance within the context of the audit objectives by gaining an understanding of the following:

a. the nature and profile of the programs and the needs of potential users of the audit report;

b. internal control as it relates to the specific objectives and scope of the audit;

c. information systems controls for purposes of assessing audit risk and planning the audit within the context of the audit objectives;

d. provisions of laws, regulations, contracts, and grant agreements, and potential fraud, and abuse that are significant within the context of the audit objectives;

e. ongoing investigations or legal proceedings within the context of the audit objectives; and

f. the results of previous audits and attestation engagements that directly relate to the current audit objectives.[129]

6.12 During planning, auditors should also

a. identify the potential criteria needed to evaluate matters subject to audit;

b. identify sources of audit evidence and determine the amount and type of evidence needed given audit risk and significance;

c. evaluate whether to use the work of other auditors and specialists to address some of the audit objectives;

d. assign sufficient staff and specialists with adequate collective professional competence and identify other resources needed to perform the audit;

e. communicate about planning and performance of the audit to management officials, those charged with governance, and others as applicable; and

[129]See paragraphs 6.13 through 6.36 for additional discussion of 6.11 a-f.

f. prepare a written audit plan.[130]

Nature and Profile of the Program and User Needs

6.13 Auditors should obtain an understanding of the nature of the program or program component under audit and the potential use that will be made of the audit results or report as they plan a performance audit. The nature and profile of a program include

a. visibility, sensitivity, and relevant risks associated with the program under audit;

b. age of the program or changes in its conditions;

c. the size of the program in terms of total dollars, number of citizens affected, or other measures;

d. level and extent of review or other forms of independent oversight;

e. program's strategic plan and objectives; and

f. external factors or conditions that could directly affect the program.

6.14 One group of users of the auditors' report is government officials who may have authorized or requested the audit. Other important users of the auditors' report are the audited entity, those responsible for acting on the auditors' recommendations, oversight organizations, and legislative bodies. Other potential users of the auditors' report include government legislators or officials (other than those who may have authorized or requested the audit), the media, interest groups, and individual citizens. In addition to an interest

[130]See paragraphs 6.37 through 6.52 for additional discussion of 6.12 a-f.

in the program, potential users may have an ability to influence the conduct of the program. An awareness of these potential users' interests and influence can help auditors judge whether possible findings could be significant to relevant users.

6.15 Obtaining an understanding of the program under audit helps auditors to assess the relevant risks associated with the program and the impact of the risks on the audit objectives, scope, and methodology. The auditors' understanding may come from knowledge they already have about the program or knowledge they gain from inquiries, observations, and reviewing documents while planning the audit. The extent and breadth of those inquiries and observations will vary among audits based on the audit objectives, as will the need to understand individual aspects of the program, such as the following:

a. Provisions of laws, regulations, contracts and grant agreements: Government programs are usually created by law and are subject to specific laws and regulations. Laws and regulations usually set forth what is to be done, who is to do it, the purpose to be achieved, the population to be served, and related funding guidelines or restrictions. Government programs may also be subject to contracts or grant agreements. Thus, understanding the laws and legislative history establishing a program and the provisions of any contracts or grant agreements is essential to understanding the program itself. Obtaining that understanding is also a necessary step in identifying the provisions of laws, regulations, contracts, or grant agreements that are significant within the context of the audit objectives.

b. Purpose and goals: Purpose is the result or effect that is intended or desired from a program's operation. Legislatures usually establish the program's purpose

when they provide authority for the program. Entity officials may provide more detailed information on the program's purpose to supplement the authorizing legislation. Entity officials are sometimes asked to set goals for program performance and operations, including both output and outcome goals. Auditors may use the stated program purpose and goals as criteria for assessing program performance or may develop additional criteria to use when assessing performance.

c. Internal control: Internal control, sometimes referred to as management control, in the broadest sense includes the plan, policies, methods, and procedures adopted by management to meet its missions, goals, and objectives. Internal control includes the processes for planning, organizing, directing, and controlling program operations. It includes the systems for measuring, reporting, and monitoring program performance. Internal control serves as a defense in safeguarding assets and in preventing and detecting errors; fraud; noncompliance with provisions of laws, regulations, contracts or grant agreements; or abuse.[131]

d. Inputs: Inputs are the amount of resources (in terms of money, material, personnel, etc.) that are put into a program. These resources may come from within or outside the entity operating the program. Measures of inputs can have a number of dimensions, such as cost, timing, and quality. Examples of measures of inputs are dollars spent, employee-hours expended, and square feet of building space.

e. Program operations: Program operations are the strategies, processes, and activities management uses

[131]See paragraphs 6.16 through 6.27 for guidance pertaining to internal control.

to convert inputs into outputs. Program operations may be subject to internal control.

f. Outputs: Outputs represent the quantity of goods or services produced by a program. For example, an output measure for a job training program could be the number of persons completing training, and an output measure for an aviation safety inspection program could be the number of safety inspections completed.

g. Outcomes: Outcomes are accomplishments or results of a program. For example, an outcome measure for a job training program could be the percentage of trained persons obtaining a job and still in the work place after a specified period of time. An example of an outcome measure for an aviation safety inspection program could be the percentage reduction in safety problems found in subsequent inspections or the percentage of problems deemed corrected in follow-up inspections. Such outcome measures show the progress made in achieving the stated program purpose of helping unemployable citizens obtain and retain jobs, and improving the safety of aviation operations. Outcomes may be influenced by cultural, economic, physical, or technological factors outside the program. Auditors may use approaches drawn from other disciplines, such as program evaluation, to isolate the effects of the program from these other influences. Outcomes also include unexpected and/or unintentional effects of a program, both positive and negative.

Internal Control

6.16 Auditors should obtain an understanding of internal control[132] that is significant within the context of the audit objectives. For internal control that is significant within the context of the audit objectives, auditors should assess whether internal control has been properly designed and implemented and should perform procedures designed to obtain sufficient, appropriate evidence to support their assessment about the effectiveness of those controls. Information systems controls are often an integral part of an entity's internal control. The effectiveness of significant internal controls is frequently dependent on the effectiveness of information systems controls. Thus, when obtaining an understanding of internal control significant to the audit objectives, auditors should also determine whether it is necessary to evaluate information systems controls.[133]

6.17 The effectiveness of internal control that is significant within the context of the audit objectives can affect audit risk. Consequently, auditors may determine that it is necessary to modify the nature, timing, or extent of the audit procedures based on the auditors' assessment of internal control and the results of internal control testing. For example, poorly controlled aspects of a program have a higher risk of failure, so auditors may choose to focus more efforts in these areas. Conversely, effective controls at the audited entity may enable the auditors to limit the extent and type of audit testing needed.

6.18 Auditors may obtain an understanding of internal control through inquiries, observations, inspection of documents and records, review of other auditors'

[132]See paragraphs A.03 and A.04 for additional discussion on internal control.

[133]See paragraphs 6.23 through 6.27 for additional discussion on evaluating the effectiveness of information systems controls.

reports, or direct tests. The nature and extent of procedures auditors perform to obtain an understanding of internal control may vary among audits based on audit objectives, audit risk, known or potential internal control deficiencies, and the auditors' knowledge about internal control gained in prior audits.

6.19 The following discussion of the principal types of internal control objectives is intended to help auditors better understand internal controls and determine whether or to what extent they are significant to the audit objectives.

a. Effectiveness and efficiency of program operations: Controls over program operations include policies and procedures that the audited entity has implemented to provide reasonable assurance that a program meets its objectives, while considering cost-effectiveness and efficiency. Understanding these controls can help auditors understand the program operations that convert inputs to outputs and outcomes.

b. Relevance and reliability of information: Controls over the relevance and reliability of information include policies and procedures that officials of the audited entity have implemented to provide themselves reasonable assurance that operational and financial information they use for decision making and reporting externally is relevant and reliable and fairly disclosed in reports. Understanding these controls can help auditors (1) assess the risk that the information gathered by the entity may not be relevant or reliable and (2) design appropriate tests of the information considering the audit objectives.

c. Compliance with applicable laws, regulations, contracts, and grant agreements: Controls over compliance include policies and procedures that the audited entity has implemented to provide reasonable

assurance that program implementation is in accordance with provisions of laws, regulations, contracts, and grant agreements. Understanding the relevant controls concerning compliance with those laws, regulations, contracts or grant agreements that the auditors have determined are significant within the context of the audit objectives can help them assess the risk of noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse.

6.20 A subset of these categories of internal control objectives is the safeguarding of assets and resources. Controls over the safeguarding of assets and resources include policies and procedures that the audited entity has implemented to reasonably prevent or promptly detect unauthorized acquisition, use, or disposition of assets and resources.

6.21 In performance audits, a deficiency in internal control[134] exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct (1) impairments of effectiveness or efficiency of operations, (2) misstatements in financial or performance information, or (3) noncompliance with provisions of laws, regulations, contracts, or grant agreements on a timely basis. A deficiency in design exists when (a) a control necessary to meet the control objective is missing or (b) an existing control is not properly designed so that, even if the control operates as designed, the control objective is not met. A deficiency in operation exists when a properly designed control does not operate as designed, or when the person performing the control does not possess the

[134]See paragraph A.05 for additional discussion of internal control deficiencies.

necessary authority or qualifications to perform the control effectively.

6.22 Internal auditing is an important part of overall governance, accountability, and internal control. A key role of many internal audit organizations is to provide assurance that internal controls are in place to adequately mitigate risks and achieve program goals and objectives. The auditor may determine that it is appropriate to use the work of the internal auditors in the auditor's assessment of the effectiveness of design or operation of internal controls that are significant within the context of the audit objectives.[135]

Information Systems Controls

6.23 Understanding information systems controls is important when information systems are used extensively throughout the program under audit and the fundamental business processes related to the audit objectives rely on information systems. Information systems controls consist of those internal controls that are dependent on information systems processing and include general controls, application controls, and user controls.

a. Information systems general controls (entitywide, system, and application levels) are the policies and procedures that apply to all or a large segment of an entity's information systems. General controls help ensure the proper operation of information systems by creating the environment for proper operation of application controls. General controls include security management, logical and physical access, configuration management, segregation of duties, and contingency planning.

[135]See paragraphs 6.40 through 6.44 for standards and guidance for using the work of other auditors.

b. Application controls, sometimes referred to as business process controls, are those controls that are incorporated directly into computer applications to help ensure the validity, completeness, accuracy, and confidentiality of transactions and data during application processing. Application controls include controls over input, processing, output, master file, interface, and data management system controls.

c. User controls are portions of controls that are performed by people interacting with information system controls. A user control is an information system control if its effectiveness depends on information systems processing or the reliability (accuracy, completeness, and validity) of information processed by information systems.

6.24 An organization's use of information systems controls may be extensive; however, auditors are primarily interested in those information systems controls that are significant to the audit objectives. Information systems controls are significant to the audit objectives if auditors determine that it is necessary to evaluate the effectiveness of information systems controls in order to obtain sufficient, appropriate evidence. When information systems controls are determined to be significant to the audit objectives or when the effectiveness of significant controls is dependent on the effectiveness of information systems controls, auditors should then evaluate the design and operating effectiveness of such controls. This evaluation would include other information systems controls that impact the effectiveness of the significant controls or the reliability of information used in performing the significant controls. Auditors should obtain a sufficient understanding of information systems

controls necessary to assess audit risk and plan the audit within the context of the audit objectives.[136]

6.25 Audit procedures to evaluate the effectiveness of significant information systems controls include (1) gaining an understanding of the system as it relates to the information and (2) identifying and evaluating the general, application, and user controls that are critical to providing assurance over the reliability of the information required for the audit.

6.26 The evaluation of information systems controls may be done in conjunction with the auditors' consideration of internal control within the context of the audit objectives[137] or as a separate audit objective or audit procedure, depending on the objectives of the audit. Depending on the significance of information systems controls to the audit objectives, the extent of audit procedures to obtain such an understanding may be limited or extensive. In addition, the nature and extent of audit risk related to information systems controls are affected by the nature of the hardware and software used, the configuration of the entity's systems and networks, and the entity's information systems strategy.

6.27 Auditors should determine which audit procedures related to information systems controls are needed to obtain sufficient, appropriate evidence to support the audit findings and conclusions. The following factors may assist auditors in making this determination:

[136]Refer to additional criteria and guidance in *Federal Information System Controls Audit Manual* (FISCAM), GAO-09-232G (Washington, D.C.: February 2009) and *IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals*, published by ISACA.

[137]See paragraphs 6.16 through 6.22 for additional discussion on internal control.

a. The extent to which internal controls that are significant to the audit depend on the reliability of information processed or generated by information systems.

b. The availability of evidence outside the information system to support the findings and conclusions: It may not be possible for auditors to obtain sufficient, appropriate evidence without evaluating the effectiveness of relevant information systems controls. For example, if information supporting the findings and conclusions is generated by information systems or its reliability is dependent on information systems controls, there may not be sufficient supporting or corroborating information or documentary evidence that is available other than that produced by the information systems.

c. The relationship of information systems controls to data reliability: To obtain evidence about the reliability of computer-generated information, auditors may decide to evaluate the effectiveness of information systems controls as part of obtaining evidence about the reliability of the data. If the auditor concludes that information systems controls are effective, the auditor may reduce the extent of direct testing of data.

d. Evaluating the effectiveness of information systems controls as an audit objective: When evaluating the effectiveness of information systems controls is directly a part of an audit objective, auditors should test information systems controls necessary to address the audit objectives. For example, the audit may involve the effectiveness of information systems controls related to certain systems, facilities, or organizations.

Provisions of Laws, Regulations, Contracts, and Grant Agreements, Fraud, and Abuse

Provisions of Laws, Regulations, Contracts, and Grant Agreements

6.28 Auditors should identify any provisions of laws, regulations, contracts or grant agreements that are significant within the context of the audit objectives and assess the risk that noncompliance with provisions of laws, regulations, contracts or grant agreements could occur.[138] Based on that risk assessment, the auditors should design and perform procedures to obtain reasonable assurance of detecting instances of noncompliance with provisions of laws, regulations, contracts, or grant agreements that are significant within the context of the audit objectives.

6.29 The auditors' assessment of audit risk may be affected by such factors as the complexity or newness of the laws, regulations, contracts or grant agreements. The auditors' assessment of audit risk also may be affected by whether the entity has controls that are effective in preventing or detecting noncompliance with provisions of laws, regulations, contracts, or grant agreements. If auditors obtain sufficient, appropriate evidence of the effectiveness of these controls, they can reduce the extent of their tests of compliance.

Fraud

6.30 In planning the audit, auditors should assess risks of fraud occurring that is significant within the context of the audit objectives.[139] Fraud involves obtaining something of value through willful misrepresentation.

[138]See paragraphs A.11 through A.13 for additional discussion on the significance of provisions of laws, regulations, contracts, or grant agreements.

[139]See paragraph A.10 for examples of indicators of fraud risk.

Whether an act is, in fact, fraud is a determination to be made through the judicial or other adjudicative system and is beyond auditors' professional responsibility. Audit team members should discuss among the team fraud risks, including factors such as individuals' incentives or pressures to commit fraud, the opportunity for fraud to occur, and rationalizations or attitudes that could allow individuals to commit fraud. Auditors should gather and assess information to identify risks of fraud that are significant within the scope of the audit objectives or that could affect the findings and conclusions. For example, auditors may obtain information through discussion with officials of the audited entity or through other means to determine the susceptibility of the program to fraud, the status of internal controls the audited entity has established to prevent and detect fraud, or the risk that officials of the audited entity could override internal control. An attitude of professional skepticism in assessing these risks assists auditors in assessing which factors or risks could significantly affect the audit objectives.

6.31 When auditors identify factors or risks related to fraud that has occurred or is likely to have occurred that they believe are significant within the context of the audit objectives, they should design procedures to obtain reasonable assurance of detecting any such fraud. Assessing the risk of fraud is an ongoing process throughout the audit and relates not only to planning the audit but also to evaluating evidence obtained during the audit.

6.32 When information comes to the auditors' attention indicating that fraud, significant within the context of the audit objectives, may have occurred, auditors should extend the audit steps and procedures, as necessary, to (1) determine whether fraud has likely occurred and (2) if so, determine its effect on the audit findings. If the fraud that may have occurred is not significant within the context of the audit objectives, the auditors may

conduct additional audit work as a separate engagement, or refer the matter to other parties with oversight responsibility or jurisdiction.

Abuse

6.33 Abuse involves behavior that is deficient or improper when compared with behavior that a prudent person would consider reasonable and necessary business practice given the facts and circumstances. Abuse also includes misuse of authority or position for personal financial interests or those of an immediate or close family member or business associate.[140] Abuse does not necessarily involve fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements.

6.34 Because the determination of abuse is subjective, auditors are not required to detect abuse in performance audits. However, as part of a GAGAS audit, if auditors become aware of abuse that could be quantitatively or qualitatively significant to the program under audit, auditors should apply audit procedures specifically directed to ascertain the potential effect on the program under audit within the context of the audit objectives. After performing additional work, auditors may discover that the abuse represents potential fraud or noncompliance with provisions of laws, regulations, contracts, or grant agreements.

Ongoing Investigations and Legal Proceedings

6.35 Avoiding interference with investigations or legal proceedings is important in pursuing indications of fraud, noncompliance with provisions of laws, regulations, contracts or grant agreements, or abuse. Laws, regulations, and policies may require auditors to report indications of certain types of fraud, noncompliance with provisions of laws, regulations,

[140]See A.08 for additional examples of abuse.

contracts, or grant agreements, or abuse to law enforcement or investigatory authorities before performing additional audit procedures. When investigations or legal proceedings are initiated or in process, auditors should evaluate the impact on the current audit. In some cases, it may be appropriate for the auditors to work with investigators or legal authorities, or withdraw from or defer further work on the audit or a portion of the audit to avoid interfering with an ongoing investigation or legal proceeding.

Previous Audits and Attestation Engagements

6.36 Auditors should evaluate whether the audited entity has taken appropriate corrective action to address findings and recommendations from previous engagements that are significant within the context of the audit objectives. When planning the audit, auditors should ask management of the audited entity to identify previous audits, attestation engagements, performance audits, or other studies that directly relate to the objectives of the audit, including whether related recommendations have been implemented. Auditors should use this information in assessing risk and determining the nature, timing, and extent of current audit work, including determining the extent to which testing the implementation of the corrective actions is applicable to the current audit objectives.

Identifying Audit Criteria

6.37 Auditors should identify criteria. Criteria represent the laws, regulations, contracts, grant agreements, standards, specific requirements, measures, expected performance, defined business practices, and benchmarks against which performance is compared or evaluated. Criteria identify the required or desired state or expectation with respect to the program or operation. Criteria provide a context for evaluating evidence and understanding the findings, conclusions, and recommendations included in the report. Auditors should use criteria that are relevant to the audit

objectives and permit consistent assessment of the subject matter.[141]

Identifying Sources of Evidence and the Amount and Type of Evidence Required

6.38 Auditors should identify potential sources of information that could be used as evidence. Auditors should determine the amount and type of evidence needed to obtain sufficient, appropriate evidence to address the audit objectives and adequately plan audit work.

6.39 If auditors believe that it is likely that sufficient, appropriate evidence will not be available, they may revise the audit objectives or modify the scope and methodology and determine alternative procedures to obtain additional evidence or other forms of evidence to address the current audit objectives. Auditors should also evaluate whether the lack of sufficient, appropriate evidence is due to internal control deficiencies or other program weaknesses, and whether the lack of sufficient, appropriate evidence could be the basis for audit findings.[142]

Using the Work of Others

6.40 Auditors should determine whether other auditors have conducted, or are conducting, audits of the program that could be relevant to the current audit objectives. The results of other auditors' work may be useful sources of information for planning and performing the audit. If other auditors have identified areas that warrant further audit work or follow-up, their work may influence the auditors' selection of objectives, scope, and methodology.

[141]See paragraph A6.02 for examples of criteria.

[142]See paragraphs 6.56 through 6.72 for standards concerning evidence.

6.41 If other auditors have completed audit work related to the objectives of the current audit, the current auditors may be able to use the work of the other auditors to support findings or conclusions for the current audit and, thereby, avoid duplication of efforts. If auditors use the work of other auditors, they should perform procedures that provide a sufficient basis for using that work. Auditors should obtain evidence concerning the other auditors' qualifications and independence and should determine whether the scope, quality, and timing of the audit work performed by the other auditors is adequate for reliance in the context of the current audit objectives. Procedures that auditors may perform in making this determination include reviewing the other auditors' report, audit plan, or audit documentation, and/or performing tests of the other auditors' work. The nature and extent of evidence needed will depend on the significance of the other auditors' work to the current audit objectives and the extent to which the auditors will use that work.[143]

6.42 Some audits may necessitate the use of specialized techniques or methods that require the skills of a specialist. Specialists to whom this section applies include, but are not limited to, actuaries, appraisers, attorneys, engineers, environmental consultants, medical professionals, statisticians, geologists, and information technology experts. If auditors intend to use the work of specialists, they should assess the professional qualifications and independence of the specialists.

6.43 Auditors' assessment of professional qualifications of the specialist involves the following:

[143]See paragraph 3.107 for additional discussion on using the work of other auditors and peer review reports.

a. the professional certification, license, or other recognition of the competence of the specialist in his or her field, as appropriate;

b. the reputation and standing of the specialist in the views of peers and others familiar with the specialist's capability or performance;

c. the specialist's experience and previous work in the subject matter; and

d. the auditors' prior experience in using the specialist's work.

6.44 Auditors' assessment of the independence of specialists who perform audit work includes identifying threats and applying any necessary safeguards in the same manner as they would for auditors performing work on those audits.[144]

Assigning Staff and Other Resources

6.45 Audit management should assign sufficient staff and specialists with adequate collective professional competence to perform the audit.[145] Staffing an audit includes, among other things:

a. assigning staff and specialists with the collective knowledge, skills, and experience appropriate for the job,

b. assigning a sufficient number of staff and supervisors to the audit,

[144]See paragraphs 3.02 through 3.26 for additional discussion related to independence and applying the conceptual framework approach to independence.

[145]See paragraphs 3.72 and 3.79 through 3.81 for additional discussion of using specialists in a GAGAS audit.

c. providing for on-the-job training of staff, and

d. engaging specialists when necessary.

6.46 If planning to use the work of a specialist, auditors should document the nature and scope of the work to be performed by the specialist, including

a. the objectives and scope of the specialist's work,

b. the intended use of the specialist's work to support the audit objectives,

c. the specialist's procedures and findings so they can be evaluated and related to other planned audit procedures, and

d. the assumptions and methods used by the specialist.

Communicating with Management, Those Charged with Governance, and Others

6.47 Auditors should communicate an overview of the objectives, scope, and methodology and the timing of the performance audit and planned reporting (including any potential restrictions on the report), unless doing so could significantly impair the auditors' ability to obtain sufficient, appropriate evidence to address the audit objectives, such as when the auditors plan to conduct unannounced cash counts or perform procedures related to indications of fraud. Auditors should communicate with the following parties, as applicable:

a. management of the audited entity, including those with sufficient authority and responsibility to implement corrective action in the program or activity being audited;

b. those charged with governance;[146]

c. the individuals contracting for or requesting audit services, such as contracting officials or grantees; and

d. the cognizant legislative committee, when auditors perform the audit pursuant to a law or regulation or they conduct the work for the legislative committee that has oversight of the audited entity.

6.48 In those situations where there is not a single individual or group that both oversees the strategic direction of the audited entity and the fulfillment of its accountability obligations or in other situations where the identity of those charged with governance is not clearly evident, auditors should document the process followed and conclusions reached for identifying the appropriate individuals to receive the required auditor communications.

6.49 Determining the form, content, and frequency of the communication is a matter of professional judgment, although written communication is preferred. Auditors may use an engagement letter to communicate the information. Auditors should document this communication.

6.50 If an audit is terminated before it is completed and an audit report is not issued, auditors should document the results of the work to the date of termination and why the audit was terminated. Determining whether and how to communicate the reason for terminating the audit to those charged with governance, appropriate officials of the audited entity, the entity contracting for or requesting the audit, and other appropriate officials will

[146]See paragraphs A1.05 through A1.07 for a discussion of the role of those charged with governance.

depend on the facts and circumstances and, therefore, is a matter of professional judgment.

Preparing a Written Audit Plan

6.51 Auditors must prepare a written audit plan for each audit. The form and content of the written audit plan may vary among audits and may include an audit strategy, audit program, project plan, audit planning paper, or other appropriate documentation of key decisions about the audit objectives, scope, and methodology and the auditors' basis for those decisions. Auditors should update the plan, as necessary, to reflect any significant changes to the plan made during the audit.

6.52 A written audit plan provides an opportunity for audit organization management to supervise audit planning and to determine whether

a. the proposed audit objectives are likely to result in a useful report;

b. the audit plan adequately addresses relevant risks;

c. the proposed audit scope and methodology are adequate to address the audit objectives;

d. available evidence is likely to be sufficient and appropriate for purposes of the audit; and

e. sufficient staff, supervisors, and specialists with adequate collective professional competence and other resources are available to perform the audit and to meet expected time frames for completing the work.

Supervision

6.53 Audit supervisors or those designated to supervise auditors must properly supervise audit staff.

6.54 Audit supervision involves providing sufficient guidance and direction to staff assigned to the audit to address the audit objectives and follow applicable requirements, while staying informed about significant problems encountered, reviewing the work performed, and providing effective on-the-job training.[147]

6.55 The nature and extent of the supervision of staff and the review of audit work may vary depending on a number of factors, such as the size of the audit organization, the significance of the work, and the experience of the staff.

Obtaining Sufficient, Appropriate Evidence

6.56 Auditors must obtain sufficient, appropriate evidence to provide a reasonable basis for their findings and conclusions.

6.57 The concept of sufficient, appropriate evidence is integral to an audit. Appropriateness is the measure of the quality of evidence that encompasses its relevance, validity, and reliability in providing support for findings and conclusions related to the audit objectives.[148] In assessing the overall appropriateness of evidence, auditors should assess whether the evidence is relevant, valid, and reliable. Sufficiency is a measure of the quantity of evidence used to support the findings and conclusions related to the audit objectives. In assessing the sufficiency of evidence, auditors should determine whether enough evidence has been obtained to persuade a knowledgeable person that the findings are reasonable.

[147]See paragraph 6.83c for the documentation requirement related to supervision.

[148]See paragraph A6.05 for additional discussion of the appropriateness of evidence.

6.58 In assessing evidence, auditors should evaluate whether the evidence taken as a whole is sufficient and appropriate for addressing the audit objectives and supporting findings and conclusions. Audit objectives may vary widely, as may the level of work necessary to assess the sufficiency and appropriateness of evidence to address the objectives. For example, in establishing the appropriateness of evidence, auditors may test its reliability by obtaining supporting evidence, using statistical testing, or obtaining corroborating evidence. The concepts of audit risk and significance assist auditors with evaluating the audit evidence.[149]

6.59 Professional judgment assists auditors in determining the sufficiency and appropriateness of evidence taken as a whole. Interpreting, summarizing, or analyzing evidence is typically used in the process of determining the sufficiency and appropriateness of evidence and in reporting the results of the audit work. When appropriate, auditors may use statistical methods to analyze and interpret evidence to assess its sufficiency.

Appropriateness

6.60 Appropriateness is the measure of the quality of evidence that encompasses the relevance, validity, and reliability of evidence used for addressing the audit objectives and supporting findings and conclusions.[150]

a. Relevance refers to the extent to which evidence has a logical relationship with, and importance to, the issue being addressed.

[149]See paragraphs 6.04 and 6.05 for a discussion of significance and audit risk.

[150]See paragraph A6.05 for additional guidance regarding assessing the appropriateness of evidence in relation to the audit objectives.

b. Validity refers to the extent to which evidence is a meaningful or reasonable basis for measuring what is being evaluated. In other words, validity refers to the extent to which evidence represents what it is purported to represent.

c. Reliability refers to the consistency of results when information is measured or tested and includes the concepts of being verifiable or supported.[151]

6.61 There are different types and sources of evidence that auditors may use, depending on the audit objectives. Evidence may be obtained by observation, inquiry, or inspection. Each type of evidence has its own strengths and weaknesses.[152] The following contrasts are useful in judging the appropriateness of evidence. However, these contrasts are not adequate in themselves to determine appropriateness. The nature and types of evidence to support auditors' findings and conclusions are matters of the auditors' professional judgment based on the audit objectives and audit risk.

a. Evidence obtained when internal control is effective is generally more reliable than evidence obtained when internal control is weak or nonexistent.

b. Evidence obtained through the auditors' direct physical examination, observation, computation, and inspection is generally more reliable than evidence obtained indirectly.

c. Examination of original documents is generally more reliable than examination of copies.

[151]See paragraph 6.66 for a discussion of computer-processed information and guidance on data reliability.

[152]See paragraph A6.04 for additional guidance regarding the types of evidence.

d. Testimonial evidence obtained under conditions in which persons may speak freely is generally more reliable than evidence obtained under circumstances in which the persons may be intimidated.

e. Testimonial evidence obtained from an individual who is not biased and has direct knowledge about the area is generally more reliable than testimonial evidence obtained from an individual who is biased or has indirect or partial knowledge about the area.

f. Evidence obtained from a knowledgeable, credible, and unbiased third party is generally more reliable than evidence obtained from management of the audited entity or others who have a direct interest in the audited entity.

6.62 Testimonial evidence may be useful in interpreting or corroborating documentary or physical information. Auditors should evaluate the objectivity, credibility, and reliability of the testimonial evidence. Documentary evidence may be used to help verify, support, or challenge testimonial evidence.

6.63 Surveys generally provide self-reported information about existing conditions or programs. Evaluation of the survey design and administration assists auditors in evaluating the objectivity, credibility, and reliability of the self-reported information.

6.64 When sampling is used, the method of selection that is appropriate will depend on the audit objectives. When a representative sample is needed, the use of statistical sampling approaches generally results in stronger evidence than that obtained from nonstatistical techniques. When a representative sample is not needed, a targeted selection may be effective if the auditors have isolated risk factors or other criteria to target the selection.

6.65 When auditors use information provided by officials of the audited entity as part of their evidence, they should determine what the officials of the audited entity or other auditors did to obtain assurance over the reliability of the information. The auditor may find it necessary to perform testing of management's procedures to obtain assurance or perform direct testing of the information. The nature and extent of the auditors' procedures will depend on the significance of the information to the audit objectives and the nature of the information being used.

6.66 Auditors should assess the sufficiency and appropriateness of computer-processed information regardless of whether this information is provided to auditors or auditors independently extract it. The nature, timing, and extent of audit procedures to assess sufficiency and appropriateness is affected by the effectiveness of the audited entity's internal controls over the information, including information systems controls, and the significance of the information and the level of detail presented in the auditors' findings and conclusions in light of the audit objectives.[153] The assessment of the sufficiency and appropriateness of computer-processed information includes considerations regarding the completeness and accuracy of the data for the intended purposes.[154]

Sufficiency

6.67 Sufficiency is a measure of the quantity of evidence used for addressing the audit objectives and supporting findings and conclusions. Sufficiency also depends on the appropriateness of the evidence. In

[153]See paragraphs 6.23 through 6.27 for additional discussion on assessing the effectiveness of information systems controls.

[154]Refer to additional guidance in *Assessing the Reliability of Computer-Processed Data*, GAO-09-680G (Washington, D.C.: July 2009).

determining the sufficiency of evidence, auditors should determine whether enough appropriate evidence exists to address the audit objectives and support the findings and conclusions.

6.68 The following presumptions are useful in judging the sufficiency of evidence. The sufficiency of evidence required to support the auditors' findings and conclusions is a matter of the auditors' professional judgment.

a. The greater the audit risk, the greater the quantity and quality of evidence required.

b. Stronger evidence may allow less evidence to be used.

c. Having a large volume of audit evidence does not compensate for a lack of relevance, validity, or reliability.

Overall Assessment of Evidence

6.69 Auditors should determine the overall sufficiency and appropriateness of evidence to provide a reasonable basis for the findings and conclusions, within the context of the audit objectives. Professional judgments about the sufficiency and appropriateness of evidence are closely interrelated, as auditors interpret the results of audit testing and evaluate whether the nature and extent of the evidence obtained is sufficient and appropriate. Auditors should perform and document an overall assessment of the collective evidence used to support findings and conclusions, including the results of any specific assessments conducted to conclude on the validity and reliability of specific evidence.

6.70 Sufficiency and appropriateness of evidence are relative concepts, which may be thought of in terms of a

continuum rather than as absolutes. Sufficiency and appropriateness are evaluated in the context of the related findings and conclusions. For example, even though the auditors may have some limitations or uncertainties about the sufficiency or appropriateness of some of the evidence, they may nonetheless determine that in total there is sufficient, appropriate evidence to support the findings and conclusions.

6.71 When assessing the sufficiency and appropriateness of evidence, auditors should evaluate the expected significance of evidence to the audit objectives, findings, and conclusions, available corroborating evidence, and the level of audit risk. The steps to assess evidence may depend on the nature of the evidence, how the evidence is used in the audit or report, and the audit objectives.

a. Evidence is sufficient and appropriate when it provides a reasonable basis for supporting the findings or conclusions within the context of the audit objectives.

b. Evidence is not sufficient or not appropriate when (1) using the evidence carries an unacceptably high risk that it could lead the auditor to reach an incorrect or improper conclusion, (2) the evidence has significant limitations, given the audit objectives and intended use of the evidence, or (3) the evidence does not provide an adequate basis for addressing the audit objectives or supporting the findings and conclusions. Auditors should not use such evidence as support for findings and conclusions.

6.72 Evidence has limitations or uncertainties when the validity or reliability of the evidence has not been assessed or cannot be assessed, given the audit objectives and the intended use of the evidence. Limitations also include errors identified by the auditors in their testing. When the auditors identify limitations or

uncertainties in evidence that is significant to the audit findings and conclusions, they should apply additional procedures, as appropriate. Such procedures include

a. seeking independent, corroborating evidence from other sources;

b. redefining the audit objectives or limiting the audit scope to eliminate the need to use the evidence;

c. presenting the findings and conclusions so that the supporting evidence is sufficient and appropriate and describing in the report the limitations or uncertainties with the validity or reliability of the evidence, if such disclosure is necessary to avoid misleading the report users about the findings or conclusions;[155] and

d. determining whether to report the limitations or uncertainties as a finding, including any related, significant internal control deficiencies.

Developing Elements of a Finding

6.73 Auditors should plan and perform procedures to develop the elements of a finding necessary to address the audit objectives.[156] In addition, if auditors are able to sufficiently develop the elements of a finding, they should develop recommendations for corrective action if they are significant within the context of the audit objectives. The elements needed for a finding are related to the objectives of the audit. Thus, a finding or set of findings is complete to the extent that the audit objectives are addressed and the report clearly relates those objectives to the elements of a finding. For

[155]See paragraph 7.15 for additional reporting requirements when there are limitations or uncertainties with the validity or reliability of evidence.

[156]See paragraph A6.06 for additional discussion on findings.

example, an audit objective may be to determine the current status or condition of program operations or progress in implementing legislative requirements, and not the related cause or effect. In this situation, developing the condition would address the audit objective and development of the other elements of a finding would not be necessary.

6.74 The element of criteria is discussed in paragraph 6.37, and the other elements of a finding—condition, effect, and cause—are discussed in paragraphs 6.75 through 6.77.

6.75 Condition: Condition is a situation that exists. The condition is determined and documented during the audit.

6.76 Cause: The cause identifies the reason or explanation for the condition or the factor or factors responsible for the difference between the situation that exists (condition) and the required or desired state (criteria), which may also serve as a basis for recommendations for corrective actions. Common factors include poorly designed policies, procedures, or criteria; inconsistent, incomplete, or incorrect implementation; or factors beyond the control of program management. Auditors may assess whether the evidence provides a reasonable and convincing argument for why the stated cause is the key factor or factors contributing to the difference between the condition and the criteria.[157]

6.77 Effect or potential effect: The effect is a clear, logical link to establish the impact or potential impact of the difference between the situation that exists (condition) and the required or desired state (criteria).

[157]See paragraph A6.06 for additional discussion on cause.

The effect or potential effect identifies the outcomes or consequences of the condition. When the audit objectives include identifying the actual or potential consequences of a condition that varies (either positively or negatively) from the criteria identified in the audit, "effect" is a measure of those consequences. Effect or potential effect may be used to demonstrate the need for corrective action in response to identified problems or relevant risks.[158]

Early Communication of Deficiencies

6.78 Auditors report deficiencies in internal control, fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse. For some matters, early communication to those charged with governance or management may be important because of their relative significance and the urgency for corrective follow-up action. Further, when a control deficiency results in noncompliance with provisions of laws, regulations, contracts or grant agreements, or abuse, early communication is important to allow management to take prompt corrective action to prevent further noncompliance. When a deficiency is communicated early, the reporting requirements in paragraphs 7.18 through 7.23 still apply.

Audit Documentation

6.79 Auditors must prepare audit documentation related to planning, conducting, and reporting for each audit. Auditors should prepare audit documentation in sufficient detail to enable an experienced auditor, having no previous connection to the audit, to understand from the audit documentation the nature, timing, extent, and results of audit procedures performed, the audit evidence obtained and its source

[158]See paragraph A6.07 for additional discussion on effect.

and the conclusions reached, including evidence that supports the auditors' significant judgments and conclusions. An experienced auditor means an individual (whether internal or external to the audit organization) who possesses the competencies and skills that would have enabled him or her to conduct the performance audit. These competencies and skills include an understanding of (1) the performance audit processes, (2) GAGAS and applicable legal and regulatory requirements, (3) the subject matter associated with achieving the audit objectives, and (4) issues related to the audited entity's environment.

6.80 Auditors should prepare audit documentation that contains evidence that supports the findings, conclusions, and recommendations before they issue their report.

6.81 Auditors should design the form and content of audit documentation to meet the circumstances of the particular audit. The audit documentation constitutes the principal record of the work that the auditors have performed in accordance with standards and the conclusions that the auditors have reached. The quantity, type, and content of audit documentation are a matter of the auditors' professional judgment.

6.82 Audit documentation is an essential element of audit quality. The process of preparing and reviewing audit documentation contributes to the quality of an audit. Audit documentation serves to (1) provide the principal support for the auditors' report, (2) aid auditors in conducting and supervising the audit, and (3) allow for the review of audit quality.

6.83 Auditors should document[159] the following:

a. the objectives, scope, and methodology of the audit;

b. the work performed and evidence obtained to support significant judgments and conclusions, including descriptions of transactions and records examined (for example, by listing file numbers, case numbers, or other means of identifying specific documents examined, but copies of documents examined or detailed listings of information from those documents are not required); and

c. supervisory review, before the audit report is issued, of the evidence that supports the findings, conclusions, and recommendations contained in the audit report.

6.84 When auditors do not comply with applicable GAGAS requirements due to law, regulation, scope limitations, restrictions on access to records, or other issues impacting the audit, the auditors should document the departure from the GAGAS requirements and the impact on the audit and on the auditors' conclusions. This applies to departures from unconditional requirements and from presumptively mandatory requirements when alternative procedures performed in the circumstances were not sufficient to achieve the objectives of the standard.[160]

6.85 Underlying GAGAS audits is the premise that audit organizations in federal, state, and local governments and public accounting firms engaged to perform audits in accordance with GAGAS cooperate in auditing

[159]See paragraphs 6.06, 6.46, 6.48, 6.49, 6.50, 6.69, 6.84, 7.19, 7.22, and 7.44 for additional documentation requirements regarding performance audits.

[160]See paragraphs 2.24 and 2.25 for additional requirements on citing compliance with GAGAS.

programs of common interest so that auditors may use others' work and avoid duplication of efforts. Subject to applicable laws and regulations, auditors should make appropriate individuals, as well as audit documentation, available upon request and in a timely manner to other auditors or reviewers to satisfy these objectives. The use of auditors' work by other auditors may be facilitated by contractual arrangements for GAGAS audits that provide for full and timely access to appropriate individuals, as well as audit documentation.

Reporting Standards for Performance Audits

Introduction

7.01 This chapter contains reporting requirements and guidance for performance audits conducted in accordance with generally accepted government auditing standards (GAGAS). The purpose of reporting requirements is to establish the overall approach for auditors to apply in communicating the results of the performance audit. The reporting requirements for performance audits relate to the form of the report, the report contents, and report issuance and distribution.[161]

7.02 For performance audits conducted in accordance with GAGAS, the requirements and guidance in chapters 1 through 3, 6, and 7 apply.

Reporting

7.03 Auditors must issue audit reports communicating the results of each completed performance audit.

7.04 Auditors should use a form of the audit report that is appropriate for its intended use and is in writing or in some other retrievable form.[162] For example, auditors may present audit reports using electronic media that are retrievable by report users and the audit organization. The users' needs will influence the form of the audit report. Different forms of audit reports include written reports, letters, briefing slides, or other presentation materials.

[161]See paragraph A7.02 for a description of report quality elements.

[162]See paragraph 7.43 for situations when audit organizations are subject to public records laws.

7.05 The purposes of audit reports are to (1) communicate the results of audits to those charged with governance, the appropriate officials of the audited entity, and the appropriate oversight officials; (2) make the results less susceptible to misunderstanding; (3) make the results available to the public, unless specifically limited;[163] and (4) facilitate follow-up to determine whether appropriate corrective actions have been taken.

7.06 If an audit is terminated before it is completed and an audit report is not issued, auditors should follow the guidance in paragraph 6.50.

7.07 If, after the report is issued, the auditors discover that they did not have sufficient, appropriate evidence to support the reported findings or conclusions, they should communicate in the same manner as that used to originally distribute the report to those charged with governance, the appropriate officials of the audited entity, the appropriate officials of the organizations requiring or arranging for the audits, and other known users, so that they do not continue to rely on the findings or conclusions that were not supported. If the report was previously posted to the auditors' publicly accessible website, the auditors should remove the report and post a public notification that the report was removed. The auditors should then determine whether to conduct additional audit work necessary to reissue the report, including any revised findings or conclusions or repost the original report if the additional audit work does not result in a change in findings or conclusions.

[163]See paragraph 7.40 for additional guidance on classified or limited use reports and paragraph 7.44b for distribution of reports for internal auditors.

Report Contents

7.08 Auditors should prepare audit reports that contain (1) the objectives, scope, and methodology of the audit; (2) the audit results, including findings, conclusions, and recommendations, as appropriate; (3) a statement about the auditors' compliance with GAGAS; (4) a summary of the views of responsible officials; and (5) if applicable, the nature of any confidential or sensitive information omitted.

Objectives, Scope, and Methodology

7.09 Auditors should include in the report a description of the audit objectives and the scope and methodology used for addressing the audit objectives. Report users need this information to understand the purpose of the audit, the nature and extent of the audit work performed, the context and perspective regarding what is reported, and any significant limitations in audit objectives, scope, or methodology.

7.10 Audit objectives for performance audits may vary widely. Auditors should communicate audit objectives in the audit report in a clear, specific, neutral, and unbiased manner that includes relevant assumptions. When audit objectives are limited but broader objectives could be inferred by users, auditors should state in the audit report that certain issues were outside the scope of the audit in order to avoid potential misunderstanding.

7.11 Auditors should describe the scope of the work performed and any limitations, including issues that would be relevant to likely users, so that they could reasonably interpret the findings, conclusions, and recommendations in the report without being misled. Auditors should also report any significant constraints imposed on the audit approach by information limitations or scope impairments, including denials or excessive delays of access to certain records or individuals.

7.12 In describing the work conducted to address the audit objectives and support the reported findings and conclusions, auditors should, as applicable, explain the relationship between the population and the items tested; identify organizations, geographic locations, and the period covered; report the kinds and sources of evidence; and explain any significant limitations or uncertainties based on the auditors' overall assessment of the sufficiency and appropriateness of the evidence in the aggregate.

7.13 In reporting audit methodology, auditors should explain how the completed audit work supports the audit objectives, including the evidence gathering and analysis techniques, in sufficient detail to allow knowledgeable users of their reports to understand how the auditors addressed the audit objectives. Auditors may include a description of the procedures performed as part of their assessment of the sufficiency and appropriateness of information used as audit evidence. Auditors should identify significant assumptions made in conducting the audit; describe comparative techniques applied; describe the criteria used; and, when sampling significantly supports the auditors' findings, conclusions, or recommendations, describe the sample design and state why the design was chosen, including whether the results can be projected to the intended population.

Reporting Findings

7.14 In the audit report, auditors should present sufficient, appropriate evidence to support the findings and conclusions in relation to the audit objectives. Clearly developed findings[164] assist management and oversight officials of the audited entity in understanding the need for taking corrective action. If auditors are able

[164]See paragraphs 6.73 through 6.77 for additional discussion on developing the elements of a finding.

to sufficiently develop the elements of a finding, they should provide recommendations for corrective action if they are significant within the context of the audit objectives. However, the extent to which the elements for a finding are developed depends on the audit objectives. Thus, a finding or set of findings is complete to the extent that the auditors address the audit objectives.

7.15 Auditors should describe in their report limitations or uncertainties with the reliability or validity of evidence if (1) the evidence is significant to the findings and conclusions within the context of the audit objectives and (2) such disclosure is necessary to avoid misleading the report users about the findings and conclusions. As discussed in paragraphs 6.69 through 6.72, even though the auditors may have some uncertainty about the sufficiency or appropriateness of some of the evidence, they may nonetheless determine that in total there is sufficient, appropriate evidence given the findings and conclusions. Auditors should describe the limitations or uncertainties regarding evidence in conjunction with the findings and conclusions, in addition to describing those limitations or uncertainties as part of the objectives, scope, and methodology. Additionally, this description provides report users with a clear understanding regarding how much responsibility the auditors are taking for the information.

7.16 Auditors should place their findings in perspective by describing the nature and extent of the issues being reported and the extent of the work performed that resulted in the finding. To give the reader a basis for judging the prevalence and consequences of these findings, auditors should, as appropriate, relate the instances identified to the population or the number of cases examined and quantify the results in terms of dollar value, or other measures. If the results cannot be

projected, auditors should limit their conclusions appropriately.

7.17 Auditors may provide background information to establish the context for the overall message and to help the reader understand the findings and significance of the issues discussed. Appropriate background information may include information on how programs and operations work; the significance of programs and operations (e.g., dollars, impact, purposes, and past audit work, if relevant); a description of the audited entity's responsibilities; and explanation of terms, organizational structure, and the statutory basis for the program and operations. When reporting on the results of their work, auditors should disclose significant facts relevant to the objectives of their work and known to them which, if not disclosed, could mislead knowledgeable users, misrepresent the results, or conceal significant improper or illegal practices.

7.18 Auditors should also report deficiencies in internal control, instances of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that have occurred or are likely to have occurred and are significant within the context of the audit objectives.

Deficiencies in Internal Control

7.19 Auditors should include in the audit report (1) the scope of their work on internal control and (2) any deficiencies in internal control that are significant within the context of the audit objectives and based upon the audit work performed.[165] When auditors detect deficiencies in internal control that are not significant to the objectives of the audit but warrant the attention of those charged with governance, they should include

[165]See paragraph 6.21 for a discussion of internal control deficiencies in performance audits and paragraph A.06 for examples of deficiencies in internal control.

those deficiencies either in the report or communicate those deficiencies in writing to audited entity officials. Auditors should refer to that written communication in the audit report if the written communication is separate from the audit report. When auditors detect deficiencies that do not warrant the attention of those charged with governance, the determination of whether and how to communicate such deficiencies to audited entity officials is a matter of professional judgment.

7.20 In a performance audit, auditors may conclude that identified deficiencies in internal control that are significant within the context of the audit objectives are the cause of deficient performance of the program or operations being audited. In reporting this type of finding, the internal control deficiency would be described as the cause.

Fraud, Noncompliance with Provisions of Laws, Regulations, Contracts, and Grant Agreements, and Abuse

7.21 When auditors conclude, based on sufficient, appropriate evidence, that fraud,[166] noncompliance with provisions of laws, regulations, contracts or grant agreements, or abuse[167] either has occurred or is likely to have occurred which is significant within the context of the audit objectives, they should report the matter as a finding. Whether a particular act is, in fact, fraud or noncompliance with provisions of laws, regulations, contracts or grant agreements may have to await final determination by a court of law or other adjudicative body.

7.22 When auditors detect instances of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that are not significant within the context of the audit objectives but warrant the attention of those charged with governance,

[166]See paragraph A.10 for examples of indicators of fraud risk.

[167]See paragraph A.08 for examples of abuse.

they should communicate those findings in writing to audited entity officials. When auditors detect any instances of fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that do not warrant the attention of those charged with governance, the auditors' determination of whether and how to communicate such instances to audited entity officials is a matter of professional judgment.

7.23 When fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse either have occurred or are likely to have occurred, auditors may consult with authorities or legal counsel about whether publicly reporting such information would compromise investigative or legal proceedings. Auditors may limit their public reporting to matters that would not compromise those proceedings and, for example, report only on information that is already a part of the public record.

Reporting Findings Directly to Parties Outside the Audited Entity

7.24 Auditors should report known or likely fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse directly to parties outside the audited entity in the following two circumstances.

a. When entity management fails to satisfy legal or regulatory requirements to report such information to external parties specified in law or regulation, auditors should first communicate the failure to report such information to those charged with governance. If the audited entity still does not report this information to the specified external parties as soon as practicable after the auditors' communication with those charged with governance, then the auditors should report the information directly to the specified external parties.

b. When entity management fails to take timely and appropriate steps to respond to known or likely fraud,

noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that (1) is significant to the findings and conclusions and (2) involves funding received directly or indirectly from a government agency, auditors should first report management's failure to take timely and appropriate steps to those charged with governance. If the audited entity still does not take timely and appropriate steps as soon as practicable after the auditors' communication with those charged with governance, then the auditors should report the entity's failure to take timely and appropriate steps directly to the funding agency.

7.25 The reporting in paragraph 7.24 is in addition to any legal requirements for the auditor to report such information directly to parties outside the audited entity. Auditors should comply with these requirements even if they have resigned or been dismissed from the audit prior to its completion. Internal audit organizations do not have a duty to report outside the audited entity unless required by law, rule, regulation, or policy.[168]

7.26 Auditors should obtain sufficient, appropriate evidence, such as confirmation from outside parties, to corroborate assertions by management of the audited entity that it has reported such findings in accordance with laws, regulations, or funding agreements. When auditors are unable to do so, they should report such information directly as discussed in paragraphs 7.24 and 7.25.

Conclusions

7.27 Auditors should report conclusions based on the audit objectives and the audit findings. Report conclusions are logical inferences about the program based on the auditors' findings, not merely a summary

[168]See paragraph 7.44b for reporting standards for internal audit organizations when reporting externally.

of the findings. The strength of the auditors' conclusions depends on the sufficiency and appropriateness of the evidence supporting the findings and the soundness of the logic used to formulate the conclusions. Conclusions are more compelling if they lead to the auditors' recommendations and convince the knowledgeable user of the report that action is necessary.

Recommendations

7.28 Auditors should recommend actions to correct deficiencies and other findings identified during the audit and to improve programs and operations when the potential for improvement in programs, operations, and performance is substantiated by the reported findings and conclusions. Auditors should make recommendations that flow logically from the findings and conclusions, are directed at resolving the cause of identified deficiencies and findings, and clearly state the actions recommended.

7.29 Effective recommendations encourage improvements in the conduct of government programs and operations. Recommendations are effective when they are addressed to parties that have the authority to act and when the recommended actions are specific, practical, cost effective, and measurable.

Reporting Auditors' Compliance with GAGAS

7.30 When auditors comply with all applicable GAGAS requirements, they should use the following language, which represents an unmodified GAGAS compliance statement, in the audit report to indicate that they performed the audit in accordance with GAGAS.[169]

[169]See paragraphs 2.24 and 2.25 for additional standards on citing compliance with GAGAS.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

7.31 When auditors do not comply with all applicable GAGAS requirements, they should include a modified GAGAS compliance statement in the audit report. For performance audits, auditors should use a statement that includes either (1) the language in 7.30, modified to indicate the requirements that were not followed or (2) language that the auditor did not follow GAGAS.[170]

Reporting Views of Responsible Officials

7.32 Auditors should obtain and report the views of responsible officials of the audited entity concerning the findings, conclusions, and recommendations included in the audit report, as well as any planned corrective actions.

7.33 Providing a draft report with findings for review and comment by responsible officials of the audited entity and others helps the auditors develop a report that is fair, complete, and objective. Including the views of responsible officials results in a report that presents not only the auditors' findings, conclusions, and recommendations, but also the perspectives of the responsible officials of the audited entity and the corrective actions they plan to take. Obtaining the comments in writing is preferred, but oral comments are acceptable.

[170]See paragraphs 2.24 and 2.25 for additional standards on citing compliance with GAGAS.

7.34 When auditors receive written comments from the responsible officials, they should include in their report a copy of the officials' written comments, or a summary of the comments received. When the responsible officials provide oral comments only, auditors should prepare a summary of the oral comments and provide a copy of the summary to the responsible officials to verify that the comments are accurately stated.

7.35 Auditors should also include in the report an evaluation of the comments, as appropriate. In cases in which the audited entity provides technical comments in addition to its written or oral comments on the report, auditors may disclose in the report that such comments were received.

7.36 Obtaining oral comments may be appropriate when, for example, there is a reporting date critical to meeting a user's needs; auditors have worked closely with the responsible officials throughout the work and the parties are familiar with the findings and issues addressed in the draft report; or the auditors do not expect major disagreements with the findings, conclusions, and recommendations in the draft, or major controversies with regard to the issues discussed in the draft report.

7.37 When the audited entity's comments are inconsistent or in conflict with the findings, conclusions, or recommendations in the draft report, or when planned corrective actions do not adequately address the auditors' recommendations, the auditors should evaluate the validity of the audited entity's comments. If the auditors disagree with the comments, they should explain in the report their reasons for disagreement. Conversely, the auditors should modify their report as necessary if they find the comments valid and supported with sufficient, appropriate evidence.

7.38 If the audited entity refuses to provide comments or is unable to provide comments within a reasonable period of time, the auditors may issue the report without receiving comments from the audited entity. In such cases, the auditors should indicate in the report that the audited entity did not provide comments.

Reporting Confidential and Sensitive Information

7.39 If certain pertinent information is prohibited from public disclosure or is excluded from a report due to the confidential or sensitive nature of the information, auditors should disclose in the report that certain information has been omitted and the reason or other circumstances that make the omission necessary.

7.40 Certain information may be classified or may be otherwise prohibited from general disclosure by federal, state, or local laws or regulations. In such circumstances, auditors may issue a separate, classified or limited use report containing such information and distribute the report only to persons authorized by law or regulation to receive it.

7.41 Additional circumstances associated with public safety, privacy, or security concerns could also justify the exclusion of certain information from a publicly available or widely distributed report. For example, detailed information related to computer security for a particular program may be excluded from publicly available reports because of the potential damage that could be caused by the misuse of this information. In such circumstances, auditors may issue a limited use report containing such information and distribute the report only to those parties responsible for acting on the auditors' recommendations. In some instances, it may be appropriate to issue both a publicly available report with the sensitive information excluded and a limited use report. The auditors may consult with legal counsel regarding any requirements or other circumstances that may necessitate the omission of certain information.

7.42 Considering the broad public interest in the program or activity under audit assists auditors when deciding whether to exclude certain information from publicly available reports. When circumstances call for omission of certain information, auditors should evaluate whether this omission could distort the audit results or conceal improper or illegal practices.

7.43 When audit organizations are subject to public records laws, auditors should determine whether public records laws could impact the availability of classified or limited use reports and determine whether other means of communicating with management and those charged with governance would be more appropriate. For example, the auditors may communicate general information in a written report and communicate detailed information orally. The auditor may consult with legal counsel regarding applicable public records laws.

Distributing Reports

7.44 Distribution of reports completed in accordance with GAGAS depends on the relationship of the auditors to the audited organization and the nature of the information contained in the report. Auditors should document any limitation on report distribution.[171] The following discussion outlines distribution for reports completed in accordance with GAGAS:

a. Audit organizations in government entities should distribute audit reports to those charged with governance, to the appropriate audited entity officials, and to the appropriate oversight bodies or organizations requiring or arranging for the audits. As appropriate, auditors should also distribute copies of the reports to other officials who have legal oversight authority or who

[171]See paragraphs 7.40 and 7.41 for discussion of limited use reports containing confidential or sensitive information.

may be responsible for acting on audit findings and recommendations, and to others authorized to receive such reports.

b. Internal audit organizations in government entities may also follow the Institute of Internal Auditors' (IIA) *International Standards for the Professional Practice of Internal Auditing*.[172] In accordance with GAGAS and IIA standards, the head of the internal audit organization should communicate results to parties who can ensure that the results are given due consideration. If not otherwise mandated by statutory or regulatory requirements, prior to releasing results to parties outside the organization, the head of the internal audit organization should: (1) assess the potential risk to the organization, (2) consult with senior management or legal counsel as appropriate, and (3) control dissemination by indicating the intended users of the report.

c. Public accounting firms contracted to perform an audit in accordance with GAGAS should clarify report distribution responsibilities with the engaging organization. If the contracting firm is responsible for the distribution, it should reach agreement with the party contracting for the audit about which officials or organizations will receive the report and the steps being taken to make the report available to the public.

[172]See paragraph 2.21 for additional discussion about using the IIA standards in conjunction with GAGAS and paragraph 2.22 for additional discussion about citing compliance with another set of standards.

Supplemental Guidance

Introduction

A.01 The following sections provide supplemental guidance for auditors and the audited entities to assist in the implementation of generally accepted government auditing standards (GAGAS). The guidance does not establish additional requirements but instead is intended to facilitate auditor implementation of GAGAS requirements in chapters 2 through 7. The supplemental guidance in the first section may be of assistance for all types of audits covered by GAGAS. Subsequent sections provide supplemental guidance for specific chapters of GAGAS, as indicated.

Overall Supplemental Guidance

A.02 Chapters 4 through 7 discuss the standards for financial audits, attestation engagements, and performance audits. The identification and communication of significant deficiencies and material weaknesses in internal control, fraud, noncompliance with provisions of laws, regulations, contracts or grant agreements, or abuse are important aspects of government auditing. The following discussion is provided to assist auditors in identifying significant deficiencies in internal control, abuse, and indicators of fraud risk and to assist auditors in determining whether noncompliance with provisions of laws, regulations, contracts or grant agreements are significant within the context of the audit objectives.

Internal Control

A.03 The *Internal Control—Integrated Framework*[173] published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) provides guidance on internal control. As discussed in the COSO framework, internal control consists of five interrelated components, which are (1) control

[173]*Internal Control—Integrated Framework,* Committee of Sponsoring Organizations of the Treadway Commission, 1992.

environment, (2) risk assessment, (3) control activities, (4) information and communication, and (5) monitoring. The objectives of internal control relate to (1) financial reporting, (2) operations, and (3) compliance. Safeguarding of assets is a subset of these objectives. Management designs internal control to provide reasonable assurance that unauthorized acquisition, use, or disposition of assets will be prevented or timely detected and corrected.

A.04 In addition to the COSO framework, the publication, *Standards for Internal Control in the Federal Government*,[174] which incorporates the concepts developed by COSO, provides definitions and fundamental concepts pertaining to internal control at the federal level and may also be useful to auditors at other levels of government. The related *Internal Control Management and Evaluation Tool*,[175] based on the federal internal control standards, provides a systematic, organized, and structured approach to assessing the internal control structure.

Examples of Deficiencies in Internal Control

A.05 GAGAS contains requirements for reporting identified deficiencies in internal control.

a. For financial audits, see paragraphs 4.19 through 4.24.

b. For attestation engagements, see paragraphs 5.20 through 5.23.

[174] *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

[175] *Internal Control Management and Evaluation Tool*, GAO-01-1008G (Washington, D.C.: August 2001).

c. For performance audits, see paragraphs 7.19 through 7.20.

A.06 The following are examples of control deficiencies:

a. Insufficient control consciousness within the organization. For example, the tone at the top and the control environment. Control deficiencies in other components of internal control could lead the auditor to conclude that weaknesses exist in the control environment.

b. Ineffective oversight by those charged with governance of the entity's financial reporting, performance reporting, or internal control, or an ineffective overall governance structure.

c. Control systems that did not prevent, or detect and correct material misstatements so that it was necessary to restate previously issued financial statements or operational results. Control systems that did not prevent or detect material misstatements in performance or operational results so that it was later necessary to make significant corrections to those results.

d. Control systems that did not prevent, or detect and correct material misstatements identified by the auditor. This includes misstatements involving estimation and judgment for which the auditor identifies potential material adjustments and corrections of the recorded amounts.

e. An ineffective internal audit function or risk assessment function at an entity for which such functions are important to the monitoring or risk assessment component of internal control, such as for a large or complex entity.

f. Identification of fraud of any magnitude on the part of senior management.

g. Failure by management or those charged with governance to assess the effect of a significant deficiency previously communicated to them and either to correct it or to conclude that it does not need to be corrected.

h. Inadequate controls for the safeguarding of assets.

i. Evidence of intentional override of internal control by those in authority to the detriment of the overall objectives of the system.

j. Deficiencies in the design or operation of internal control that could fail to prevent, or detect and correct, fraud, noncompliance with provisions of laws, regulations, contracts or grant agreements, or abuse having a material effect on the financial statements or the audit objective.

k. Inadequate design of information systems general, application, and user controls that prevent the information system from providing complete and accurate information consistent with financial, compliance, or performance reporting objectives or other current needs.

l. Failure of an application control caused by a deficiency in the design or operation of an information systems general control.

m. Employees or management who lack the qualifications and training to fulfill their assigned functions.

Examples of Abuse

A.07 GAGAS contains requirements for responding to indications of material abuse and reporting abuse that is material to the audit objectives.

a. For financial audits, see paragraphs 4.07 and 4.08 and 4.25 through 4.27.

b. For attestation engagements, see paragraphs 5.08 through 5.09 and 5.24 through 5.26.

c. For performance audits, see paragraphs 6.33 and 6.34 and 7.21 through 7.23.

A.08 The following are examples of abuse, depending on the facts and circumstances:

a. Creating unneeded overtime.

b. Requesting staff to perform personal errands or work tasks for a supervisor or manager.

c. Misusing the official's position for personal gain (including actions that could be perceived by an objective third party with knowledge of the relevant information as improperly benefiting an official's personal financial interests or those of an immediate or close family member; a general partner; an organization for which the official serves as an officer, director, trustee, or employee; or an organization with which the official is negotiating concerning future employment).

d. Making travel choices that are contrary to existing travel policies or are unnecessarily extravagant or expensive.

e. Making procurement or vendor selections that are contrary to existing policies or are unnecessarily extravagant or expensive.

Examples of Indicators of Fraud Risk

A.09 GAGAS contains requirements relating to evaluating fraud risk.

a. For financial audits, see paragraphs 4.06 and 4.25 through 4.27.

b. For attestation engagements, see paragraphs 5.07, 5.20, and 5.24 through 5.26.

c. For performance audits, see paragraphs 6.30 through 6.32 and 7.21 through 7.23.

A.10 In some circumstances, conditions such as the following might indicate a heightened risk of fraud:

a. economic, programmatic, or entity operating conditions threaten the entity's financial stability, viability, or budget;

b. the nature of the entity's operations provide opportunities to engage in fraud;

c. management's monitoring of compliance with policies, laws, and regulations is inadequate;

d. the organizational structure is unstable or unnecessarily complex;

e. communication and/or support for ethical standards by management is lacking;

f. management is willing to accept unusually high levels of risk in making significant decisions;

g. the entity has a history of impropriety, such as previous issues with fraud, waste, abuse, or questionable practices, or past audits or investigations with findings of questionable or criminal activity;

h. operating policies and procedures have not been developed or are outdated;

i. key documentation is lacking or does not exist;

j. asset accountability or safeguarding procedures is lacking;

k. improper payments;

l. false or misleading information;

m. a pattern of large procurements in any budget line with remaining funds at year end, in order to "use up all of the funds available;" and

n. unusual patterns and trends in contracting, procurement, acquisition, and other activities of the entity or program.

Determining Whether Provisions of Laws, Regulations, Contracts and Grant Agreements Are Significant within the Context of the Audit Objectives

A.11 GAGAS contains requirements for determining whether provisions of laws, regulations, contracts or grant agreements are significant within the context of the audit objectives.

a. For financial audits, see paragraphs 4.19 through 4.22.

b. For attestation engagements, see paragraphs 5.07 and 5.08.

c. For performance audits, see paragraphs 6.28 and 6.29.

A.12 Government programs are subject to many provisions of laws, regulations, contracts or grant agreements. At the same time, their significance within the context of the audit objectives varies widely,

depending on the objectives of the audit. Auditors may find the following approach helpful in assessing whether provisions of laws, regulations, contracts or grant agreements are significant within the context of the audit objectives:

a. Express each audit objective in terms of questions about specific aspects of the program being audited (that is, purpose and goals, internal control, inputs, program operations, outputs, and outcomes).

b. Identify provisions of laws, regulations, contracts or grant agreements that directly relate to specific aspects of the program within the context of the audit objectives.

c. Determine if the audit objectives or the auditors' conclusions could be significantly affected if noncompliance with those provisions of laws, regulations, contracts or grant agreements occurred. If the audit objectives or audit conclusions could be significantly affected, then those provisions of laws, regulations, contracts or grant agreements are likely to be significant to the audit objectives.

A.13 Auditors may consult with their own legal counsel to (1) determine those laws and regulations that are significant to the audit objectives, (2) design tests of compliance with laws and regulations, or (3) evaluate the results of those tests. Auditors also may consult with their own legal counsel when audit objectives require testing compliance with provisions of contracts or grant agreements. Depending on the circumstances of the audit, auditors may consult with others, such as investigative staff, other audit organizations or government entities that provided professional services to the audited entity, or applicable law enforcement authorities, to obtain information on compliance matters.

Information to Accompany Chapter 1

A1.01 Chapter 1 discusses the use and application of GAGAS and the role of auditing in government accountability. Those charged with governance and management of audited organizations also have roles in government accountability. The discussion that follows is provided to assist auditors in understanding the roles of others in accountability. The following section also contains background information on the laws, regulations, or other authoritative sources that require the use of GAGAS. This information is provided to place GAGAS within the context of overall government accountability.

Laws, Regulations, and Other Authoritative Sources That Require Use of GAGAS

A1.02 Laws, regulations, contracts, grant agreements, or policies frequently require the use of GAGAS.[176] The following are some of the laws, regulations, and or other authoritative sources that require the use of GAGAS:

a. The Inspector General Act of 1978, as amended, 5 U.S.C. App. requires that the statutorily appointed federal inspectors general comply with GAGAS for audits of federal establishments, organizations, programs, activities, and functions. The act further states that the inspectors general shall take appropriate steps to assure that any work performed by nonfederal auditors complies with GAGAS.

b. The Chief Financial Officers Act of 1990 (Public Law 101-576), as expanded by the Government Management Reform Act of 1994 (Public Law 103-356), requires that GAGAS be followed in audits of executive branch departments' and agencies' financial statements. The Accountability of Tax Dollars Act of 2002 (Public Law 107-289) generally extends this

[176]See paragraph 1.06 for additional discussion on the use of GAGAS.

requirement to most executive agencies not subject to the Chief Financial Officers Act unless they are exempted for a given year by the Office of Management and Budget (OMB).

c. The Single Audit Act Amendments of 1996 (Public Law 104-156) require that GAGAS be followed in audits of state and local governments and nonprofit entities that receive federal awards. OMB Circular No. A-133, *Audits of States, Local Governments, and Non-Profit Organizations*, which provides the governmentwide guidelines and policies on performing audits to comply with the Single Audit Act, also requires the use of GAGAS.

A1.03 Other laws, regulations, or authoritative sources may require the use of GAGAS. For example, auditors at the state and local levels of government may be required by state and local laws and regulations to follow GAGAS. Also, auditors may be required by the terms of an agreement or contract to follow GAGAS. Auditors may also be required to follow GAGAS by federal audit guidelines pertaining to program requirements, such as those issued for Housing and Urban Development programs and Student Financial Aid programs. Being alert to such other laws, regulations, or authoritative sources may assist auditors in performing their work in accordance with the required standards.

A1.04 Even if not required to do so, auditors may find it useful to follow GAGAS in performing audits of federal, state, and local government programs as well as audits of government awards administered by contractors, nonprofit entities, and other nongovernmental entities. Many audit organizations not formally required to do so, both in the United States of America and in other countries, voluntarily follow GAGAS.

The Role of Those Charged with Governance

A1.05 During the course of GAGAS audits, auditors communicate with those charged with governance.[177]

a. For financial audits, see paragraphs 4.03 and 4.04.

b. For attestation engagements, see paragraphs 5.04 and 5.05.

c. For performance audits, see paragraphs 6.47 through 6.50.

A1.06 Those charged with governance are responsible for overseeing the strategic direction of the entity and obligations related to the accountability of the entity. This includes overseeing the financial reporting process, subject matter, or program under audit including related internal controls. In certain entities covered by GAGAS, those charged with governance may also be part of the entity's management. In some audit entities, multiple parties may be charged with governance, including oversight bodies, members or staff of legislative committees, boards of directors, audit committees, or parties contracting for the audit.

A1.07 Because the governance structures of government entities and organizations can vary widely, it may not always be clearly evident who is charged with key governance functions. In these situations, auditors evaluate the organizational structure for directing and controlling operations to achieve the audited entity's objectives. This evaluation also includes how the audited entity delegates authority and establishes accountability for its management personnel.

[177]See paragraph 1.02 for additional discussion of those charged with governance.

Management's Role

A1.08 Managers have fundamental responsibilities for carrying out government functions.[178] Management of the audited entity is responsible for

a. using its financial, physical, and informational resources legally, effectively, efficiently, economically, ethically, and equitably to achieve the purposes for which the resources were furnished or the program was established;

b. complying with applicable laws and regulations (including identifying the requirements with which the entity and the official are responsible for compliance);

c. implementing systems designed to achieve compliance with applicable laws and regulations;

d. establishing and maintaining effective internal control to help ensure that appropriate goals and objectives are met; following laws and regulations; and ensuring that management and financial information is reliable and properly reported;

e. providing appropriate reports to those who oversee their actions and to the public in order to demonstrate accountability for the resources and authority used to carry out government programs and the results of these programs;

f. addressing the findings and recommendations of auditors, and for establishing and maintaining a process to track the status of such findings and recommendations;

[178]See paragraphs 1.01 and 1.02 for additional discussion of management and officials of government programs.

g. following sound procurement practices when contracting for audits, including ensuring procedures are in place for monitoring contract performance; and

h. taking timely and appropriate steps to remedy fraud, noncompliance with provisions of laws, regulations, contracts or grant agreements, or abuse that auditors report.

Information to Accompany Chapter 2

Attestation Engagements

A2.01 Examples of attestation engagements objectives[179] include

a. prospective financial or performance information;

b. management's discussion and analysis (MD&A) presentation;

c. an entity's internal control over financial reporting;

d. the effectiveness of an entity's internal control over compliance with specified requirements, such as those governing the bidding for, accounting for, and reporting on grants and contracts;

e. an entity's compliance with requirements of specified laws, regulations, policies, contracts, or grants;

f. the accuracy and reliability of reported performance measures;

[179]See paragraph 2.09 for additional discussion of attestation engagements.

g. whether incurred final contract costs are supported with required evidence and in compliance with the contract terms;

h. the allowability and reasonableness of proposed contract amounts that are based on detailed costs; and

i. the quantity, condition, or valuation of inventory or assets.

Performance Audit Objectives

A2.02 Examples of program effectiveness and results audit objectives[180] include:

a. assessing the extent to which legislative, regulatory, or organizational goals and objectives are being achieved;

b. assessing the relative ability of alternative approaches to yield better program performance or eliminate factors that inhibit program effectiveness;

c. analyzing the relative cost-effectiveness of a program or activity, focusing on combining cost information or other inputs with information about outputs or the benefit provided or with outcomes or the results achieved;

d. determining whether a program produced intended results or produced results that were not consistent with the program's objectives;

e. determining the current status or condition of program operations or progress in implementing legislative requirements;

[180]See paragraph 2.11a for additional discussion of program effectiveness and results audit objectives.

f. determining whether a program provides equitable access to or distribution of public resources within the context of statutory parameters;

g. assessing the extent to which programs duplicate, overlap, or conflict with other related programs;

h. evaluating whether the entity is following sound procurement practices;

i. assessing the reliability, validity, or relevance of performance measures concerning program effectiveness and results, or economy and efficiency;

j. assessing the reliability, validity, or relevance of financial information related to the performance of a program;

k. determining whether government resources (inputs) are obtained at reasonable costs while meeting timeliness and quality considerations;

l. determining whether appropriate value was obtained based on the cost or amount paid or based on the amount of revenue received;

m. determining whether government services and benefits are accessible to those individuals who have a right to access those services and benefits;

n. determining whether fees assessed cover costs;

o. determining whether and how the program's unit costs can be decreased or its productivity increased; and

p. assessing the reliability, validity, or relevance of budget proposals or budget requests to assist legislatures in the budget process.

A2.03 Examples of audit objectives related to internal control[181] include an assessment of the extent to which internal control provides reasonable assurance about whether

a. organizational missions, goals, and objectives are achieved effectively and efficiently;

b. resources are used in compliance with laws, regulations, or other requirements;

c. resources, including sensitive information accessed or stored outside the organization's physical perimeter, are safeguarded against unauthorized acquisition, use, or disposition;

d. management information, such as performance measures, and public reports are complete, accurate, and consistent to support performance and decision making;

e. the integrity of information from computerized systems is achieved; and

f. contingency planning for information systems provides essential back-up to prevent unwarranted disruption of the activities and functions that the systems support.

A2.04 Compliance objectives[182] include determining whether

[181]See paragraph 2.11b for additional discussion of internal control audit objectives.

[182]See paragraph 2.11c for additional discussion of compliance audit objectives.

a. the purpose of the program, the manner in which it is to be conducted, the services delivered, the outcomes, or the population it serves is in compliance with provisions of laws, regulations, contracts or grant agreements, or other requirements;

b. government services and benefits are distributed or delivered to citizens based on the individual's eligibility to obtain those services and benefits;

c. incurred or proposed costs are in compliance with applicable laws, regulations, contracts, or grant agreements; and

d. revenues received are in compliance with applicable laws, regulations, contracts or grant agreements.

A2.05 Examples of objectives pertaining to prospective analysis[183] include providing conclusions based on

a. current and projected trends and future potential impact on government programs and services;

b. program or policy alternatives, including forecasting program outcomes under various assumptions;

c. policy or legislative proposals, including advantages, disadvantages, and analysis of stakeholder views;

d. prospective information prepared by management;

e. budgets and forecasts that are based on (1) assumptions about expected future events and (2) management's expected reaction to those future events; and

[183]See paragraph 2.11d for additional discussion of prospective analysis audit objectives.

f. management's assumptions on which prospective information is based.

GAGAS Compliance Statements

A2.06 The determination of whether an unmodified or modified GAGAS compliance statement is appropriate is based on the consideration of the individual and aggregate effect of exceptions to GAGAS requirements.[184] Quantitative and qualitative factors that the auditor may consider include:

a. the likelihood that the exception(s) will affect the perceptions of report users about the audit findings, conclusions, and recommendations;

b. the magnitude of the effect of the exception(s) on the perceptions of report users about the audit findings, conclusions, and recommendations;

c. the pervasiveness of the exception(s);

d. the potential effect of the exception(s) on the sufficiency and appropriateness of evidence supporting the audit findings, conclusions, and recommendations; and

e. whether report users could be misled if the GAGAS compliance statement were not modified.

Information to Accompany Chapter 3

A3.01 Chapter 3 discusses the general standards applicable to financial audits, attestation engagements, and performance audits in accordance with GAGAS. The following supplemental guidance is provided to assist auditors and audited entities in avoiding

[184]See paragraphs 2.24 and 2.25 for additional discussion on citing compliance with GAGAS.

impairments to independence, establishing a system of quality control, and identifying peer review risk factors.

Threats to Independence

A3.02 This list is intended to illustrate by example the types of circumstances that create threats to independence that an auditor might identify when applying the conceptual framework.[185] It does not include all circumstances that create threats to independence; these circumstances will be unique to the conditions under which each evaluation takes place.

A3.03 Examples of circumstances that create self-interest threats for an auditor include:

a. A member of the audit team having a direct financial interest in the audited entity. This would not preclude auditors from auditing pension plans that they participate in if (1) the auditor has no control over the investment strategy, benefits, or other management issues associated with the pension plan and (2) the auditor belongs to such pension plan as part of his/her employment with the audit organization, provided that the plan is normally offered to all employees in equivalent employment positions.

b. An audit organization having undue dependence on income from a particular audited entity.

c. A member of the audit team entering into employment negotiations with an audited entity.

d. An auditor discovering a significant error when evaluating the results of a previous professional service performed by a member of the auditor's audit organization.

[185]See paragraphs 3.07 through 3.26.

A3.04 Examples of circumstances that create self-review threats for an auditor include:

a. An audit organization issuing a report on the effectiveness of the operation of financial or performance management systems after designing or implementing the systems.

b. An audit organization having prepared the original data used to generate records that are the subject matter of the audit.

c. An audit organization performing a service for an audited entity that directly affects the subject matter information of the audit.

d. A member of the audit team being, or having recently been, employed by the audited entity in a position to exert significant influence over the subject matter of the audit.

A3.05 Examples of circumstances that create bias threats for an auditor include:

a. An auditor's having preconceptions about the objectives of a program under audit that are sufficiently strong to impact the auditor's objectivity.

b. An auditor's having biases associated with political, ideological, or social convictions that result from membership or employment in, or loyalty to, a particular type of policy, group, organization, or level of government that could impact the auditor's objectivity.

A3.06 Examples of circumstances that create familiarity threats for an auditor include:

a. A member of the audit team having a close or immediate family member who is a principal or senior manager of the audited entity.

b. A member of the audit team having a close or immediate family member who is an employee of the audited entity and is in a position to exert significant influence over the subject matter of the audit.

c. A principal or employee of the audited entity in a position to exert significant influence over the subject matter of the audit having recently served on the audit team.

d. An auditor accepting gifts or preferential treatment from an audited entity, unless the value is trivial or inconsequential.

e. Senior audit personnel having a long association with the audited entity.

A3.07 Examples of circumstances that create undue influence threats for an auditor or audit organization include existence of:

a. External interference or influence that could improperly limit or modify the scope of an audit or threaten to do so, including exerting pressure to inappropriately reduce the extent of work performed in order to reduce costs or fees.

b. External interference with the selection or application of audit procedures or in the selection of transactions to be examined.

c. Unreasonable restrictions on the time allowed to complete an audit or issue the report.

d. External interference over the assignment, appointment, compensation, and promotion of audit personnel.

e. Restrictions on funds or other resources provided to the audit organization that adversely affect the audit organization's ability to carry out its responsibilities.

f. Authority to overrule or to inappropriately influence the auditors' judgment as to the appropriate content of the report.

g. Threat of replacing the auditors over a disagreement with the contents of an auditors' report, the auditors' conclusions, or the application of an accounting principle or other criteria.

h. Influences that jeopardize the auditors' continued employment for reasons other than incompetence, misconduct, or the need for audits or attestation engagements.

A3.08 Examples of circumstances that create management participation threats for an auditor include:

a. A member of the audit team being, or having recently been, a principal or senior manager of the audited entity.

b. An audit organization principal or employee serving as a voting member of an entity's management committee or board of directors, making policy decisions that affect future direction and operation of an entity's programs, supervising entity employees, developing or approving programmatic policy, authorizing an entity's transactions, or maintaining custody of an entity's assets.

c. An audit organization principal or employee recommending a single individual for a specific position that is key to the entity or program under audit, or otherwise ranking or influencing management's selection of the candidate.

d. An auditor preparing management's corrective action plan to deal with deficiencies detected in the audit.

A3.09 Examples of circumstances that create structural threats for an auditor include:

a. For both external and internal audit organizations, structural placement of the audit function within the reporting line of the areas under audit.

b. For internal audit organizations, administrative direction from the audited entity's management.

System of Quality Control

A3.10 Chapter 3 discusses the elements of an audit organization's system of quality control.[186] The following supplemental guidance is provided to assist auditors and audit organizations in establishing policies and procedures in its system of quality control to address the following elements: initiation, acceptance, and continuance of audits; audit performance, documentation, and reporting; and monitoring.

a. Government audit organizations initiate audits as a result of (1) legal mandates, (2) requests from legislative bodies or oversight bodies, and (3) the audit organization's discretion. In the case of legal mandates and requests, a government audit organization may be required to perform the audit and may not be permitted

[186]See paragraphs 3.82 through 3.95 for additional discussion of the system of quality control.

to make decisions about acceptance or continuance and may not be permitted to resign or withdraw from the audit.

b. GAGAS standards for audit performance, documentation, and reporting are in chapter 4 for financial audits, chapter 5 for attestation engagements, and chapters 6 and 7 for performance audits. Chapter 3 specifies that an audit organization's quality control system include policies and procedures designed to provide the audit organization with reasonable assurance that audits are performed and reports are issued in accordance with professional standards and legal and regulatory requirements.[187] Examples of such policies and procedures include the following:

(1) communication provided to team members so that they sufficiently understand the objectives of their work and the applicable professional standards;

(2) audit planning and supervision;

(3) appropriate documentation of the work performed;

(4) review of the work performed, the significant judgments made, and the resulting audit documentation and report;

(5) review of the independence and qualifications of any external specialists or contractors used, as well as a review of the scope and quality of their work;

(6) procedures for resolving difficult or contentious issues or disagreements among team members, including specialists;

[187]See paragraphs 3.82 through 3.95 for additional discussion of quality control policies and procedures.

(7) obtaining and addressing comments from the audited entity on draft reports; and

(8) reporting supported by the evidence obtained, and in accordance with applicable professional standards and legal or regulatory requirements.

c. Monitoring is an ongoing, periodic assessment of audits designed to provide management of the audit organization with reasonable assurance that the policies and procedures related to the system of quality control are suitably designed and operating effectively in practice.[188] The following guidance is provided to assist audit organizations with implementing and continuing its monitoring of quality:

(1) Who: Monitoring is most effective when performed by persons who do not have responsibility for the specific activity being monitored (e.g., for specific audits or specific centralized processes). The staff member or team of staff members assigned with responsibility for the monitoring process collectively need sufficient and appropriate competence and authority in the audit organization to assume that responsibility. Generally the staff member or the team of staff members performing the monitoring are apart from the normal audit supervision associated with individual audits.

(2) How much: The extent of monitoring procedures varies based on the audit organization's circumstances to enable the audit organization to assess compliance with applicable professional standards and the audit organization's quality control policies and procedures. Examples of specific monitoring procedures include

[188]See paragraphs 3.93 through 3.95 for additional discussion of monitoring.

(a) examination of selected administrative and personnel records pertaining to quality control;

(b) review of selected audit documentation and reports;

(c) discussions with the audit organization's personnel (as applicable and appropriate);

(d) periodic summarization of the findings from the monitoring procedures in writing (at least annually), and consideration of the systematic causes of findings that indicate improvements are needed;

(e) determination of any corrective actions to be taken or improvements to be made with respect to the specific audits reviewed or the audit organization's quality control policies and procedures;

(f) communication of the identified findings to appropriate audit organization management with subsequent follow-up; and

(g) consideration of findings by appropriate audit organization management personnel who also determine whether actions necessary, including necessary modifications to the quality control system, are performed on a timely basis.

(3) Review of selected administrative and personnel records: The review of selected administrative and personnel records pertaining to quality control may include tests of

(a) compliance with policies and procedures on independence;

(b) compliance with continuing professional development policies, including training;

(c) procedures related to recruitment and hiring of qualified personnel, including hiring of specialists or consultants when needed;

(d) procedures related to performance evaluation and advancement of personnel;

(e) procedures related to initiation, acceptance, and continuance of audits;

(f) audit organization personnel's understanding of the quality control policies and procedures, and implementation of these policies and procedures; and

(g) audit organization's process for updating its policies and procedures.

(4) Follow-up on previous findings: Monitoring procedures include an evaluation of whether the audit organization has taken appropriate corrective action to address findings and recommendations from previous monitoring and peer reviews. Personnel involved in monitoring use this information as part of the assessment of risk associated with the design and implementation of the audit organization's quality control system and in determining the nature, timing, and extent of monitoring procedures.

(5) Communication: The audit organization communicates internally the results of the monitoring of its quality control systems that allows the audit organization to take prompt and appropriate action where necessary. Information included in this communication includes:

(a) a description of the monitoring procedures performed;

(b) the conclusions drawn from the monitoring procedures; and

(c) where relevant, a description of the systemic, repetitive, or other significant deficiencies and of the actions taken to resolve those deficiencies.

Peer Review

A3.11 Examples of the factors to consider when performing an assessment of peer review risk for selecting audits for peer review[189] include:

a. scope of the audits including size of the audited entity or audits covering multiple locations;

b. functional area or type of government program;

c. types of audits provided, including the extent of nonaudit services provided to audited entities;

d. personnel (including use of new personnel or personnel not routinely assigned the types of audits provided);

e. initial audits;

f. familiarity resulting from a longstanding relationship with the audited entity;

g. political sensitivity of the audits;

h. budget constraints for the audit organization;

i. results of the peer review team's review of the design of system of quality control;

[189]See paragraph 3.99 for additional discussion of the assessment of peer review risk.

j. results of the audit organization's monitoring process; and

k. risk sensitivity of the audit organization.

A3.12 As discussed in paragraph 3.105, an external audit organization should make its most recent peer review report publicly available. Examples of how to achieve this transparency requirement include posting the peer review report on an external Web site or to a publicly available file. To help the public understand the peer review reports, an audit organization may also include a description of the peer review process and how it applies to its organization. The following provides examples of additional information that audit organizations may include to help users understand the meaning of the peer review report.

a. Explanation of the peer review process.

b. Description of the audit organization's system of quality control.

c. Explanation of the relationship of the peer review results to the audited organization's work.

d. If the peer review report that includes deficiencies or significant deficiencies is modified, explanation of the reviewed audit organization's plan for improving quality controls and the status of the improvements.

Information to Accompany Chapter 6

A6.01 Chapter 6 discusses the field work standards for performance audits. An integral concept for performance auditing is the use of sufficient, appropriate evidence based on the audit objectives to support a sound basis for audit findings, conclusions, and recommendations. The following discussion is provided to assist auditors in identifying criteria and the

various types of evidence, including assessing the appropriateness of evidence in relation to the audit objectives.

Types of Criteria

A6.02 The following are some examples of criteria:[190]

a. purpose or goals prescribed by law or regulation or set by officials of the audited entity,

b. policies and procedures established by officials of the audited entity,

c. technically developed standards or norms,

d. expert opinions,

e. prior periods' performance,

f. defined business practices,

g. contract or grant terms, and

h. performance of other entities or sectors used as defined benchmarks.

A6.03 Audit objectives may pertain to describing the current status or condition of a program or process. For this type of audit objective, criteria may also be represented by the assurance added by the auditor's (1) description of the status or condition, (2) evaluation of whether the status or condition meets certain characteristics, or (3) evaluation of whether management's description is verifiable, accurate, or supported.

[190]See paragraph 6.37 for additional discussion on identifying audit criteria.

Types of Evidence

A6.04 In terms of its form and how it is collected, evidence may be categorized as physical, documentary, or testimonial. Physical evidence is obtained by auditors' direct inspection or observation of people, property, or events. Such evidence may be documented in summary memos, photographs, videos, drawings, charts, maps, or physical samples. Documentary evidence is obtained in the form of already existing information such as letters, contracts, accounting records, invoices, spreadsheets, database extracts, electronically stored information, and management information on performance. Testimonial evidence is obtained through inquiries, interviews, focus groups, public forums, or questionnaires. Auditors frequently use analytical processes including computations, comparisons, separation of information into components, and rational arguments to analyze any evidence gathered to determine whether it is sufficient and appropriate.[191] The strength and weakness of each form of evidence depends on the facts and circumstances associated with the evidence and professional judgment in the context of the audit objectives.

Appropriateness of Evidence in Relation to the Audit Objectives

A6.05 One of the primary factors influencing the assurance associated with a performance audit is the appropriateness of the evidence in relation to the audit objectives.[192] For example:

a. The audit objectives might focus on verifying specific quantitative results presented by the audited entity. In these situations, the audit procedures would likely focus

[191]See paragraphs 6.67 and 6.60 for definitions of sufficient and appropriate.

[192]See paragraphs 6.60 through 6.66 for additional discussion on the appropriateness of evidence.

on obtaining evidence about the accuracy of the specific amounts in question. This work may include the use of statistical sampling.

b. The audit objectives might focus on the performance of a specific program or activity in the agency being audited. In these situations, the auditor may be provided with information compiled by the agency being audited in order to answer the audit objectives. The auditor may find it necessary to test the quality of the information, which includes both its validity and reliability.

c. The audit objectives might focus on information that is used for widely accepted purposes and obtained from sources generally recognized as appropriate. For example, economic statistics issued by government agencies for purposes such as adjusting for inflation, or other such information issued by authoritative organizations, may be the best information available. In such cases, it may not be practical or necessary for auditors to conduct procedures to verify the information. These decisions call for professional judgment based on the nature of the information, its common usage or acceptance, and how it is being used in the audit.

d. The audit objectives might focus on comparisons or benchmarking between various government functions or agencies. These types of audits are especially useful for analyzing the outcomes of various public policy decisions. In these cases, auditors may perform analyses, such as comparative statistics of different jurisdictions or changes in performance over time, where it would be impractical to verify the detailed data underlying the statistics. Clear disclosure as to what extent the comparative information or statistics were evaluated or corroborated will likely be necessary to place the evidence in context for report users.

e. The audit objectives might focus on trend information based on data provided by the audited entity. In this situation, auditors may assess the evidence by using overall analytical tests of underlying data, combined with a knowledge and understanding of the systems or processes used for compiling information.

f. The audit objectives might focus on the auditor identifying emerging and cross-cutting issues using information compiled or self-reported by agencies. In such cases, it may be helpful for the auditor to consider the overall appropriateness of the compiled information along with other information available about the program. Other sources of information, such as inspector general reports or other external audits, may provide the auditors with information regarding whether any unverified or self-reported information is consistent with or can be corroborated by these other external sources of information.

Findings

A6.06 When the audit objectives include explaining why a particular type of positive or negative program performance, output, or outcome identified in the audit occurred, they are referred to as "cause."[193] Identifying the cause of problems may assist auditors in making constructive recommendations for correction. Because deficiencies can result from a number of plausible factors or multiple causes, the recommendation can be more persuasive if auditors can clearly demonstrate and explain with evidence and reasoning the link between the deficiencies and the factor or factors they have identified as the cause or causes. Auditors may also identify deficiencies in program design or structure as the cause of deficient performance. Auditors may also identify deficiencies in internal control that are

[193]See paragraph 6.76 for additional discussion of "cause."

significant to the subject matter of the performance audit as the cause of deficient performance. In developing these types of findings, the deficiencies in program design or internal control would be described as the "cause." Often the causes of deficient program performance are complex and involve multiple factors, including fundamental, systemic root causes. Alternatively, when the audit objectives include estimating the program's effect on changes in physical, social, or economic conditions, auditors seek evidence of the extent to which the program itself is the "cause" of those changes.

A6.07 When the audit objectives include estimating the extent to which a program has caused changes in physical, social, or economic conditions, "effect" is a measure of the impact achieved by the program. In this case, "effect" is the extent to which positive or negative changes in actual physical, social, or economic conditions can be identified and attributed to the program.

Information to Accompany Chapter 7

A7.01 Chapter 7 discusses the reporting standards for performance audits. The following discussion is provided to assist auditors in developing and writing their audit report for performance audits.

Report Quality Elements

A7.02 The auditor may use the report quality elements of timely, complete, accurate, objective, convincing, clear, and concise when developing and writing the audit report as the subject permits.[194]

a. Accurate: An accurate report is supported by sufficient, appropriate evidence with key facts, figures,

[194]See paragraph 7.08 for additional discussion of report contents.

and findings being traceable to the audit evidence. Reports that are fact-based, with a clear statement of sources, methods, and assumptions so that report users can judge how much weight to give the evidence reported, assist in achieving accuracy. Disclosing data limitations and other disclosures also contribute to producing more accurate audit reports. Reports also are more accurate when the findings are presented in the broader context of the issue. One way to help audit organizations prepare accurate audit reports is to use a quality control process such as referencing. Referencing is a process in which an experienced auditor who is independent of the audit checks that statements of facts, figures, and dates are correctly reported, that the findings are adequately supported by the evidence in the audit documentation, and that the conclusions and recommendations flow logically from the evidence.

b. Objective: Objective means that the presentation of the report is balanced in content and tone. A report's credibility is significantly enhanced when it presents evidence in an unbiased manner and in the proper context. This means presenting the audit results impartially and fairly. The tone of reports may encourage decision makers to act on the auditors' findings and recommendations. This balanced tone can be achieved when reports present sufficient, appropriate evidence to support conclusions while refraining from using adjectives or adverbs that characterize evidence in a way that implies criticism or unsupported conclusions. The objectivity of audit reports is enhanced when the report explicitly states the source of the evidence and the assumptions used in the analysis. The report may recognize the positive aspects of the program reviewed if applicable to the audit objectives. Inclusion of positive program aspects may lead to improved performance by other government organizations that read the report. Audit reports are more objective when they demonstrate that the work

has been performed by professional, unbiased, independent, and knowledgeable staff.

c. Complete: Being complete means that the report contains sufficient, appropriate evidence needed to satisfy the audit objectives and promote an understanding of the matters reported. It also means the report states evidence and findings without omission of significant relevant information related to the audit objectives. Providing report users with an understanding means providing perspective on the extent and significance of reported findings, such as the frequency of occurrence relative to the number of cases or transactions tested and the relationship of the findings to the entity's operations. Being complete also means clearly stating what was and was not done and explicitly describing data limitations, constraints imposed by restrictions on access to records, or other issues.

d. Convincing: Being convincing means that the audit results are responsive to the audit objectives, that the findings are presented persuasively, and that the conclusions and recommendations flow logically from the facts presented. The validity of the findings, the reasonableness of the conclusions, and the benefit of implementing the recommendations are more convincing when supported by sufficient, appropriate evidence. Reports designed in this way can help focus the attention of responsible officials on the matters that warrant attention and can provide an incentive for taking corrective action.

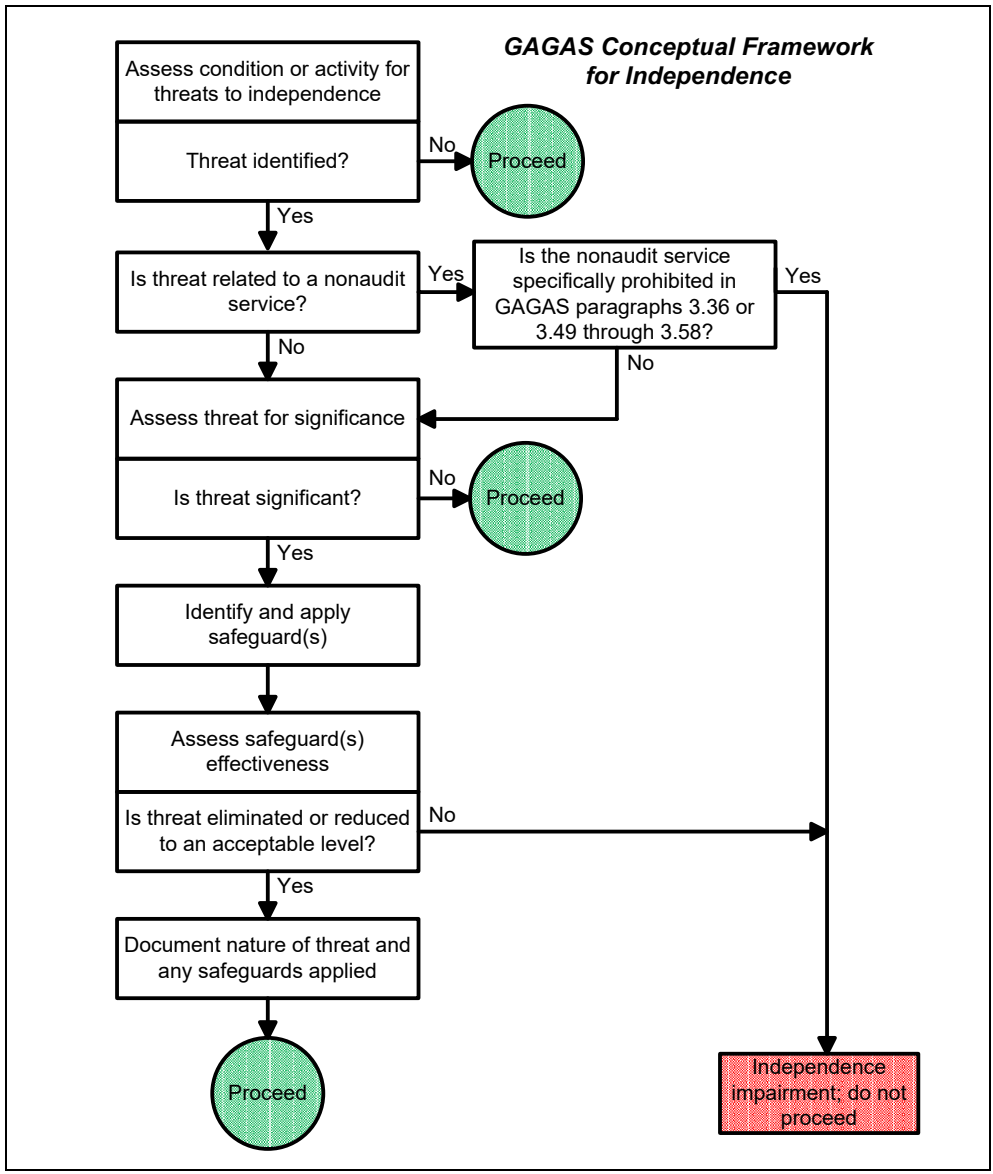
e. Clear: Clarity means the report is easy for the intended user to read and understand. Preparing the report in language as clear and simple as the subject permits assists auditors in achieving this goal. Use of straightforward, nontechnical language is helpful to simplify presentation. Defining technical terms,

abbreviations, and acronyms that are used in the report is also helpful. Auditors may use a highlights page or summary within the report to capture the report user's attention and highlight the overall message. If a summary is used, it is helpful if it focuses on the specific answers to the questions in the audit objectives, summarizes the audit's most significant findings and the report's principal conclusions, and prepares users to anticipate the major recommendations. Logical organization of material, and accuracy and precision in stating facts and in drawing conclusions assist in the report's clarity and understanding. Effective use of titles and captions and topic sentences makes the report easier to read and understand. Visual aids (such as pictures, charts, graphs, and maps) may clarify and summarize complex material.

f. Concise: Being concise means that the report is not longer than necessary to convey and support the message. Extraneous detail detracts from a report, may even conceal the real message, and may confuse or distract the users. Although room exists for considerable judgment in determining the content of reports, those that are fact-based but concise are likely to achieve results.

g. Timely: To be of maximum use, providing relevant evidence in time to respond to officials of the audited entity, legislative officials, and other users' legitimate needs is the auditors' goal. Likewise, the evidence provided in the report is more helpful if it is current. Therefore, the timely issuance of the report is an important reporting goal for auditors. During the audit, the auditors may provide interim reports of significant matters to appropriate entity officials. Such communication alerts officials to matters needing immediate attention and allows them to take corrective action before the final report is completed.

GAGAS Conceptual Framework for Independence



Source: GAO.

Comptroller General's Advisory Council on Government Auditing Standards

Advisory Council Members

Auston Johnson, Chair
State of Utah
(2009-2011)

The Honorable Ernest A. Almonte
State of Rhode Island
(member 2005-2008)

Christine C. Boesz
Consultant
(member 2007-2011)

Kathy A. Buller
Peace Corps
(member 2009-2011)

Dr. Paul A. Copley
James Madison University
(member 2005-2008)

David Cotton
Cotton & Co. LLP
(member 2006-2009)

Beryl H. Davis
Institute of Internal Auditors
(member 2007-2011)

Kristine Devine
Deloitte & Touche, LLP
(member 2005-2011)

Dr. Ehsan Feroz
University of Minnesota Duluth
(member 2002-2009)

Alex Fraser
Standard & Poor's
(member 2006-2008)

Mark Funkhouser
Kansas City, Missouri
(member 2005-2008)

Dr. Michael H. Granof
University of Texas at Austin
(member 2005-2008)

Jerome Heer
County of Milwaukee, Wisconsin
(member 2004-2011)

Michael Hendricks
Consultant
(member 2010-2012)

Marion Higa
State of Hawaii
(member 2006-2009)

The Honorable John P. Higgins, Jr.
U.S. Department of Education
(member 2005-2008)

Julia Higgs
Florida Atlantic University
(member 2009-2011)

Russell Hinton
State of Georgia
(member 2004-2011)

Drummond Kahn
City of Portland, Oregon
(member 2009-2011)

Richard A. Leach
United States Navy
(member 2005-2011)

David W. Martin
State of Florida
(member 2010-2012)

Patrick L. McNamee
PricewaterhouseCoopers, LLP
(member 2005-2008)

John R. Miller
KPMG LLP (Retired)
(chair 2001-2008)

Nancy A. Miller
Miller Foley Group
(member 2010-2012)

Rakesh Mohan
State of Idaho
(member 2004-2011)

The Honorable Samuel Mok
Consultant
(member 2006-2009)

Harold L. Monk, Jr.
Davis, Monk & Company
(member 2002-2012)

Stephen L. Morgan
City of Austin, Texas
(member 2001-2008)

Janice Mueller
State of Wisconsin
(member 2009-2011)

George A. Rippey
U.S. Department of Education
(member 2010-2012)

The Honorable Jon T. Rymer
Federal Deposit Insurance Corporation
(member 2009-2011)

Brian A. Schebler
McGladrey & Pullen, LLP
(member 2005-2011)

Barry R. Snyder
Federal Reserve Board
(member 2001-2008)

Dr. Daniel L. Stufflebeam
Western Michigan University
(member 2002-2009)

F. Michael Taylor
City of Stockton, California
(member 2010-2012)

Roland L. Unger
State of Maryland
(member 2010)

Edward J. Valenzuela
State of Florida
(member 2007-2009)

Thomas E. Vermeer
Alfred Lerner College of Business & Economics
(member 2010-2012)

Sandra H. Vice
State of Texas
(member 2010-2012)

John C. Weber
Crowe Horwath LLP
(member 2010-2012)

George Willie
Bert Smith & Co.
(member 2004-2011)

GAO Project Team

Jeanette M. Franzel, Managing Director
James R. Dalkin, Project Director
Robert F. Dacey, Chief Accountant
Marcia B. Buchanan, Assistant Director
Cheryl E. Clark, Assistant Director
Heather I. Keister, Assistant Director
Kristen A. Kociolek, Assistant Director
Michael C. Hrapsky, Specialist, Auditing Standards
Eric H. Holbrook, Specialist, Auditing Standards
Maria Hasan, Auditor
Laura S. Pacheco, Auditor
Christie A. Pugnetti, Auditor
Margaret A. Mills, Senior Communications Analyst
Jennifer V. Allison, Council Administrator

Index

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order Printed Copies

The printed version of the December 2011 revision of *Government Auditing Standards* can be ordered through the Government Printing Office (GPO) online or by calling 202-512-1800 or 1-866-512-1800 toll free.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

United States Government Accountability Office

GAO

Report to Congressional Requesters

June 2005

HUMAN CAPITAL

Selected Agencies Have Opportunities to Enhance Existing Succession Planning and Management Efforts

GAO-05-585

June 2005

HUMAN CAPITAL

Selected Agencies Have Opportunities to Enhance Existing Succession Planning and Management Efforts

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-05-585, a report to congressional requesters

Why GAO Did This Study

As the federal government confronts an array of challenges in the 21st century, it must employ strategic human capital management, including succession planning, to help meet those challenges. Leading organizations go beyond a succession planning approach that focuses on replacing individuals and engage in broad, integrated succession planning and management efforts that focus on strengthening current and future organizational capacity.

GAO reviewed how the Census Bureau, Department of Labor (DOL), the Environmental Protection Agency (EPA) and the Veterans Health Administration (VHA) are implementing succession planning and management efforts.

What GAO Recommends

GAO made specific recommendations to enhance agencies' succession efforts. The Department of Veterans Affairs agreed with our recommendations. The Census Bureau agreed with two recommendations and in response to a third, stated that its existing monitoring approach is effective. However, without strengthened monitoring, the Bureau is at increased risk that it will not have the skills it needs for the 2010 Census. DOL did not take issue with our findings and will consider our recommendations. EPA did not comment on our recommendations. DOL and EPA provided technical comments.

www.gao.gov/cgi-bin/getrpt?GAO-05-585.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Eileen Larence at (202) 512-6806 or larencee@gao.gov.

What GAO Found

The Census Bureau, DOL, EPA, and VHA have all implemented succession planning and management efforts that collectively are intended to strengthen organizational capacity. However, in light of governmentwide fiscal challenges, the agencies have opportunities to enhance some of their succession efforts.

- While all of the agencies have assigned responsibility for their succession planning and management efforts to councils or boards, VHA has established a subcommittee and high-level positions that are directly responsible for its succession efforts. Also, VHA and the Census Bureau specifically mention succession planning and management as performance expectations in their executives' performance plans.

- The four agencies have begun to link succession efforts to strategic planning. For example, DOL plans to shift from a historical enforcement role to a compliance assistance and consulting role, requiring stronger skills in communication and analysis. To attract and retain employees with such skills, DOL launched the Masters in Business Administration Fellows program in 2002, which it considers one of its major succession training and development programs.

- Monitoring mission-critical workforce needs helps make informed planning decisions. DOL, EPA, and VHA have identified gaps in occupations or competencies, have undertaken strategies to address these gaps, and are planning or are taking steps to monitor their progress in closing these gaps. The Census Bureau could strengthen the monitoring of its mission-critical occupations more closely and at a higher level to ensure it is prepared for the 2010 Decennial Census.

- Effective training and development programs can enhance the federal government's ability to achieve results. All of the agencies' succession efforts include training and development programs at all organizational levels. However, in the current budget environment, there are opportunities to coordinate and share these programs and create synergies through benchmarking with others, achieving economies of scale, limiting duplication of efforts, and enhancing the effectiveness of programs, among other things. Performance measures for these programs can also help agencies evaluate these programs' effects on organizational capacity and justify their value.

- Finally, agencies have recognized the importance of diversity to a successful workforce and use succession planning and management to enhance their workforce diversity.

Contents

Abbreviations

CHCO	Chief Human Capital Officers (Council)
DOC	Department of Commerce
DOL	Department of Labor
EEOC	Equal Employment Opportunity Commission
EPA	Environmental Protection Agency
Fed CDP	Federal Candidate Development Program
MBA	Masters in Business Administration
MSPB	Merit Systems Protection Board
OPM	Office of Personnel Management
SES	Senior Executive Service
VA	Department of Veterans Affairs
VHA	Veterans Health Administration
VISN	Veterans Integrated Service Network

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, D.C. 20548

June 30, 2005

The Honorable George V. Voinovich
Chairman
Subcommittee on Oversight of Government Management,
the Federal Workforce, and the District of Columbia
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Jon Porter
Chairman
Subcommittee on the Federal Workforce and Agency Organization
Committee on Government Reform
House of Representatives

The Honorable Jo Ann Davis
House of Representatives

Large, escalating, and persistent deficits that are unsustainable over the long term are among an array of challenges that the federal government confronts in the 21st century.[1] To help meet government's challenges, we have reported that agencies must employ strategic human capital management. We also continue to designate strategic human capital management as a high-risk area, one that threatens the federal government's ability to serve Americans effectively, because federal human capital strategies are still not appropriately constituted to meet current and emerging challenges or drive the transformations necessary for agencies to meet these challenges.[2] More specifically, agencies need to identify, develop, and select the appropriate leaders, managers, and workforce to meet 21st century challenges, and one critical step is through effective succession planning and management. Leading organizations go beyond a succession planning approach that focuses on simply replacing individuals and engage in broad, integrated succession planning and management efforts that focus on strengthening both current and future organizational capacity. Particularly in an environment of likely continued budget constraints, federal agencies must implement human capital strategies,

[1] GAO, *21st Century Challenges: Reexamining the Base of the Federal Government*, GAO-05-325SP (Washington, D.C.: February 2005).

[2] GAO, *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: January 2005).

including succession planning and management, to transform their cultures to achieve their long-term goals.

Congress has recognized the important role of succession planning and management in preparing federal workers for the future. The Federal Workforce Flexibility Act of 2004 requires the head of each agency to establish, in consultation with the Office of Personnel Management (OPM), a comprehensive management succession program to provide training for employees and develop future managers for the agency.[3] In addition, the Chief Human Capital Officers Act led to the creation of a governmentwide Chief Human Capital Officers (CHCO) Council, which subsequently established a leadership and succession planning subcommittee.[4] This subcommittee' s intended focus is on reviewing leadership development, moving leaders from technicians to strategic thinkers, and meeting future workforce needs in a planned manner. The act also calls for OPM to design measures to assess, among other issues, the continuity of effective leadership through the implementation of succession plans.

We previously identified how agencies in Australia, Canada, New Zealand, and the United Kingdom are adopting a more strategic approach to managing the succession of senior executives and other employees with critical skills.[5] We found that these agencies' succession planning and management efforts (1) receive active support of top leadership; (2) link to the agencies' strategic planning; (3) identify talent from multiple organizational levels, early in their careers, or with critical skills; (4) emphasize developmental assignments for high-potential employees in addition to formal training; (5) address specific human capital challenges, such as diversity; and (6) facilitate broader transformation efforts.[6] We observed that these experiences may prove valuable to agencies in the United States.

[3] 5 U.S.C. §4121.

[4] 5 U.S.C. §1401.

[5] GAO, *Human Capital: Insights for U.S. Agencies from Other Countries' Succession Planning and Management Initiatives*, GAO-03-914 (Washington, D.C.: Sept. 15, 2003).

[6] For more information on transformation, see GAO, *Forum: High-Performing Organizations: Metrics, Means, and Mechanisms for Achieving High Performance in the 21st Century Public Management Environment*, GAO-04-343SP (Washington, D.C.: Feb. 13, 2004).

As a follow up to that report, we reviewed how selected U.S. agencies are implementing succession planning and management efforts. For purposes of this report, we specifically address the first five practices given the selected agencies' immediate succession challenges. We selected agencies based on the nature of these succession challenges as well as their diverse organizational structures and missions.

Specifically, we reviewed the

- Census Bureau, which has a unique, event-driven requirement, namely the 2010 Decennial Census, and projected that 45 percent of its workforce will be eligible to retire by 2010;

- Department of Labor (DOL), which has reported a Senior Executive Service (SES) retirement eligibility rate of more than 60 percent by the beginning of fiscal year (FY) 2010;

- Environmental Protection Agency (EPA), which has reported that almost 60 percent of its SES will be eligible to retire by 2008 and projected a loss of at least 20 percent of its supervisors in 10 of 18 priority occupations; and

- Veterans Health Administration (VHA), which reported a 38 percent SES retirement eligibility rate through 2008 and projects that 24 percent of its Nurse Executives will be eligible for regular retirement in 2005.

To meet this objective, we analyzed strategic, human capital, workforce, succession, and training and development plans; guidance for managers' performance agreements; human capital team charters; and diversity information from the selected agencies. In addition, we reviewed policies and guidance on succession-related issues from OPM, as well as the Equal Employment Opportunity Commission (EEOC) and the Merit Systems Protection Board (MSPB) because of their responsibilities for ensuring the fair application of personnel decisions, such as selection for training and development programs. We also interviewed agency, OPM, EEOC, and MSPB officials involved with strategic, human capital, and succession planning and management. To get the varied perspectives of agencies' staff located in headquarters and regional offices, we interviewed agency officials in Washington, D.C.; Charlotte, North Carolina; and Los Angeles and San Francisco, California. Appendix I provides additional information on our scope and methodology. We conducted our study from June 2004

through April 2005 in accordance with generally accepted government auditing standards.

Results in Brief

The Census Bureau, DOL, EPA, and VHA have all implemented selected succession planning and management efforts that collectively are intended to strengthen both current and future organizational capacity. Generally, these efforts receive top leadership support and commitment, link with strategic planning, identify critical gaps in occupations or competencies, offer training and development programs, and enhance diversity. However, each of the agencies should enhance some succession efforts to better position themselves for the future.

All four agencies have the support and commitment of their organizations' top leadership. For example, they have established councils or boards with responsibility for human capital that involve top agency leadership. Specifically, VHA has a dedicated subcommittee as well as high-level positions that are directly accountable for succession planning and management, while the other three agencies have councils or boards that are responsible for human capital more broadly, including succession. Furthermore, all four agencies include a performance expectation that in general holds executives accountable for human capital management in their performance plans. However, VHA and the Census Bureau include an expectation that specifically holds executives accountable for succession planning and management.

All four agencies have also begun to link their succession efforts to their strategic goals. DOL states that to meet its strategic goal of ensuring a competitive 21st century workforce, it plans to identify skill gaps, assess training needs, and recruit new employees. For example, DOL plans to shift from a historical enforcement role to compliance assistance and consultation, requiring stronger skills in communication and analysis. DOL seeks to develop more skills in technology and project management as well as in strategic planning, quantitative analysis, and analytical thinking for a more "business-like" management approach. To attract and retain employees with such skills, DOL launched the Masters in Business Administration (MBA) Fellows program in 2002, which it considers one of its major succession development programs.

These agencies have identified the talent, and specifically the mission-critical occupations or competencies required to achieve their goals. For example, VHA projects the number of employees needed to fill the gaps in

mission-critical occupations and monitors changes in its mission-critical workforce. EPA has projected gaps by mission-critical occupations, identified technical and cross-occupational competencies, and plans to monitor its progress in closing these gaps. DOL assesses its mission-critical requirements through skills inventories and monitors the turnover of its workforce. The Census Bureau, on the other hand, has also identified its mission-critical occupations, but does not monitor its progress in closing gaps because decisions to fill vacancies are delegated to line managers. However, without monitoring the readiness of its mission-critical workers more closely and at a higher level than line managers, the Bureau may not know overall if it is acquiring the skills it needs to be prepared to conduct the 2010 Decennial Census.

Effective training and development programs can enhance the federal government's ability to prepare its workforce and thereby achieve results. Further, effective succession planning and management efforts identify talent from multiple organizational levels and early in their careers as well as provide both formal and developmental training to strengthen high-potential employees' skills and to broaden their experience. All four agencies have core succession training and development programs for entry-level employees, middle-level management, and senior executives. However, in the current budget environment, there are opportunities for agencies to coordinate and share these programs and create synergies through benchmarking with others, achieving economies of scale, limiting duplication of efforts, and enhancing the effectiveness of programs, among other things. Examples of such coordinated and shared training include a partnership across three agencies to share best practices among their acquisition workforces and OPM's program to help agencies meet their senior executive succession goals and create a leadership corps. The selected agencies generally had not sought out such opportunities for their core succession programs.

Given this environment, agencies also need credible information to evaluate how training and development programs affect organizational capacity. All four agencies are able to report on measures such as participant number and program cost. However, the Census Bureau, VHA, and EPA could better demonstrate their programs' value in providing future talent by identifying outcome-oriented measures and evaluating the extent to which these programs enhance their organizations' capacity. For example, DOL has identified measures that are intended to provide the department with an understanding of the programs' impact on organizational capacity, such as its SES "bench strength," a ratio of senior

executives who are in training or have completed training to those projected to leave.

Finally, all four agencies report using their succession planning and management efforts to enhance diversity. For example, VHA has integrated diversity planning into its succession and workforce planning process. Initially, each regional office that has primary responsibility for health care—or Veterans Integrated Service Network (VISN)—submits a regional succession plan that includes diversity information. VHA then analyzes these data, highlights underrepresentation of certain demographic groups in specific mission-critical occupations, and provides guidance to focus recruiting efforts to enhance diversity.

To improve and refine their succession planning and management efforts, we are recommending that all four agencies actively seek opportunities to coordinate and share their core succession training and development programs with other outside agencies. By doing so, agencies can enhance efficiency and increase the effectiveness of their programs, among other things. We are also making other recommendations to individual agencies to enhance their succession planning and management efforts.

We provided a draft of this report to the Acting Director of OPM and the CHCO Council's Leadership and Succession Planning Subcommittee for their information. We also provided a draft of this report to the Secretaries of Commerce, Labor, and Veterans Affairs (VA) and the Administrator of EPA for their review and comment. VA agreed with our findings and recommendations, and we present their written comments in appendix II. The Department of Commerce (DOC) and the Census Bureau agreed with our findings and our recommendations to seek opportunities to coordinate core succession training and development programs and to evaluate the extent to which these programs enhance organizational capacity. In response to our recommendation to strengthen the monitoring of its mission-critical workforce, the Census Bureau stated that its existing approach is effective. However, without strengthened monitoring of its mission-critical workforce, the Census Bureau is at increased risk that it will not have the skills it needs to be prepared to conduct the 2010 Census as efficiently or effectively as possible. For example, a lesson from the 2000 Census was that while contracts for various projects supported decennial census operations, they did so in many instances at a higher cost than necessary because the Census Bureau did not have sufficient contracting and program staff with the training and experience to manage them. We present DOC's and the Census Bureau's written comments in appendix III.

DOL did not take issue with our findings, stated that it will consider our recommendations, and provided technical comments, which we incorporated as appropriate. EPA did not comment on our recommendations, but provided a technical comment, which we incorporated.

Background

We have found that other countries are experiencing challenges in managing their human capital, and their experiences may prove valuable to federal agencies in the United States. For example, they are using their performance management systems to connect employee performance with organizational success to help foster a results-oriented culture.[7] They are also implementing succession planning and management initiatives that are designed to protect and enhance organizational capacity.[8] Collectively, these agencies' initiatives demonstrated the following practices.

- *Receive active support of top leadership*. Top leadership actively participates in, regularly uses, and ensures the needed financial and staff resources for key succession planning and management initiatives. New Zealand's State Services Commissioner, whose wide-ranging duties include the appointment and review of public service chief executives, formulated a new governmentwide senior leadership and management development strategy.

- *Link to strategic planning*. To focus on both current and future needs and to provide leaders with a broader perspective, the Royal Canadian Mounted Police's succession planning and management initiative figures prominently in the agency's multiyear human capital plan and provides top leaders with an agencywide perspective when making decisions.

- *Identify talent from multiple organizational levels, early in their careers, or with critical skills*. For example, the United Kingdom's Fast Stream program targets high-potential individuals as well as recent college graduates, and aims to provide individuals with experiences and training linked to strengthening specific competencies required for admission to the Senior Civil Service.

[7] GAO, *Results-Oriented Cultures: Insights for U.S. Agencies from Other Countries' Performance Management Initiatives*, GAO-02-862 (Washington, D.C.: Aug. 2, 2002).

[8] GAO-03-914.

- *Emphasize developmental assignments in addition to formal training*. Initiatives emphasize developmental assignments in addition to formal training to strengthen high-potential employees' skills and broaden their experiences. For example, Canada's Accelerated Executive Development Program temporarily assigns executives to work in unfamiliar roles or subject areas, and in different agencies.

- *Address specific human capital challenges, such as diversity, leadership capacity, and retention*. For example, the United Kingdom created a centralized development program that targets minorities with the potential to join the Senior Civil Service.

- *Facilitating broader transformation efforts*. The United Kingdom launched a wide-ranging reform program know as Modernising Government, which focused on improving the quality, coordination, and accessibility of the services government offered to its citizens and restructured the content of its leadership and management development programs to reflect this new emphasis on service delivery. In Australia, to find individuals to champion recent changes in how it delivers services and interacts with stakeholders, the Family Court of Australia identifies and prepares future leaders who will have the skills and experiences to help the organization successfully adapt to agency transformation.

We at GAO have also undertaken a variety of succession planning and management initiatives consistent with these leading practices to strengthen our own internal efforts. For example, we have constructed a detailed workforce planning model and analyzed it to ensure that it hired, retained, and contracted for the appropriate number of staff with the needed competencies. In addition, we have developed certain "people measures" to assess its performance in human capital management, including measures for the attraction and retention of staff, staff utilization and development, and organizational leadership.

Agencies Reinforce Top Leadership Support by Assigning Responsibility for Succession Efforts

Effective succession planning and management programs have the support and commitment of their organizations' top leadership. Our past work has shown that demonstrated commitment of top leaders is perhaps the single most important element of successful management reform.[9] We have reported that to demonstrate its support of succession planning and management efforts, top leadership actively participates in and regularly uses these initiatives to develop and promote individuals, and ensures that these programs receive sufficient resources.[10] As a next step, federal agencies are to hold their senior executives accountable to address human capital issues, such as succession.[11] We found that VHA has assigned responsibility for succession planning and management initiatives to a dedicated subcommittee, while DOL, the Census Bureau, and EPA have councils or boards that are responsible for human capital more broadly, including succession efforts.

VHA has established a subcommittee and high-level positions that are directly responsible for succession planning and management. The Succession and Workforce Development Management Subcommittee reports to the Human Resources Committee of the National Leadership Board, as illustrated in figure 1. VHA's Chief Executive Officer—the Department of Veterans Affairs' Undersecretary for Health—chairs the board, which consists of VISN directors, chief officers, and heads of offices.

[9] GAO, *Management Reform: Elements of Successful Improvement Initiatives*, GAO/T-GGD-00-26 (Washington, D.C.: Oct. 15, 1999).

[10] GAO-03-914.

[11] GAO, *Results-Oriented Cultures: Using Balanced Expectations to Manage Senior Executive Performance*, GAO-02-966 (Washington, D.C.: Sept. 27, 2002).

Figure 1: VHA's Assigned Responsibility for Succession

Source: GAO.

In addition, VHA has established (1) a workforce planner position to help coordinate and manage VHA workforce planning activities, and (2) a nurse workforce planner position to help respond to its nursing shortage and consult with the workforce planner on certain issues, such as regional-specific recruiting challenges and training. Also, this year, VHA seeks to establish a director of succession management, a senior executive-level position. According to a VHA human capital official, the new director's duties will include overseeing national coordination of VHA's succession activities.

At DOL, the Management Review Board, chaired by the Assistant Secretary for Administration and Management, is responsible for a variety of business issues, including human capital. The board is composed of top senior leaders from each of the agencies within DOL. According to DOL, the board's senior leaders helped garner support for departmentwide succession planning and management efforts. For example, the board recommended funding the development of departmentwide competencies required for mission-critical occupations.

The Census Bureau's Human Capital Management Council, consisting of representatives from each of the Census Bureau's directorates, reports to the Deputy Director of Census. According to Census Bureau human resource officials, the Council plays a key role in involving and advising top leadership on human capital issues. For example, the Council developed

and presented a succession management plan that recommended, among other things, piloting job rotations and assignments to address mission-critical priorities and resources. In addition, according to a Census Bureau human resource official, the Council assesses various succession-related issues, such as recruiting and competency development for the Bureau's senior management. In turn, senior management recently tasked a Council representative to provide monthly updates on succession-related issues.

EPA's Human Resources Council, composed of senior leaders who are to advise the EPA Administrator on human capital issues, released EPA's "Strategy for Human Capital," a planning document outlining EPA's long-term human capital goals. The strategy names the offices responsible for leading each of its goals. For example, the Office of Human Resources, the Executive Resources Board, and human resources officers are to implement a strategy to "Ensure the Continuity of Leadership, Critical Expertise, and Agency Values through Succession Planning and Management/Executive Development." According to agency human capital officials, EPA's assistant and regional administrators and their senior managers are responsible for executing succession planning initiatives.

As a next step, federal agencies are to hold their senior executives accountable for human capital issues, thus explicitly aligning individual performance expectations with organizational goals. VHA and the Census Bureau specifically mention succession planning and management in their executives' performance plans. DOL and EPA senior executive performance expectations also include aspects of succession planning and management as part of more general human capital management responsibilities.

- At VHA, in their FY 2005 performance plans, chief officers and program officials are to assure that the regional strategic plans address workforce development, including a succession plan that projects workforce needs. A VHA official also stated that VHA is considering including specific succession-related performance measures, such as turnover rates for selected priority occupations, in applicable executive performance plans.

- The Census Bureau's FY 2005 executive performance plans state that each senior executive "effectively develops and executes plans to accomplish strategic goals and organizational objectives, setting clear priorities and acquiring, organizing, and leveraging available resources (human, financial, budget, etc.,) and succession planning to ensure

timely delivery of high quality services and products in compliance with applicable laws, regulations and policies." Senior executives are also to demonstrate a planned approach to workforce development for managers and staff.

- At DOL, executives are to ensure that "staff are appropriately selected, utilized, appraised, and developed…" Executives are also to develop the talents of the staff and qualified candidates for positions in the organization, according to DOL's latest senior executive performance management plan, revised in 2004.

- EPA' s FY 2004 performance plan for senior executives states that executives should identify current and projected skill gaps and develop strategies for addressing these gaps. According to an EPA executive resource policy official, the FY 2005 senior executive performance plan is under revision, but the expectations concerning skill gaps will not change.

We have also reported that to demonstrate its support of succession planning and management, top leadership ensures that these programs receive sufficient financial and staff resources and are maintained over time.[12] DOL uses a centrally managed "crosscut fund" to supplement its succession planning and management initiatives. Component agencies within DOL submit project proposals, which DOL evaluates against established criteria, such as supporting initiatives in the department's Human Capital Strategic Plan. According to DOL, from FY 2003-2004, the agency allocated about $6.1 million for 18 human capital projects, such as competency assessments for mission-critical occupations, and the Management Development Program, one of DOL's major succession development programs. The Census Bureau, EPA, and VHA allocate money to various programs, including succession efforts, intended to contribute to human capital goals, but detailed funding information was not readily available from the agencies.

[12] GAO-03-914.

Agencies Have Begun to Link Succession Efforts to Their Strategic Goals

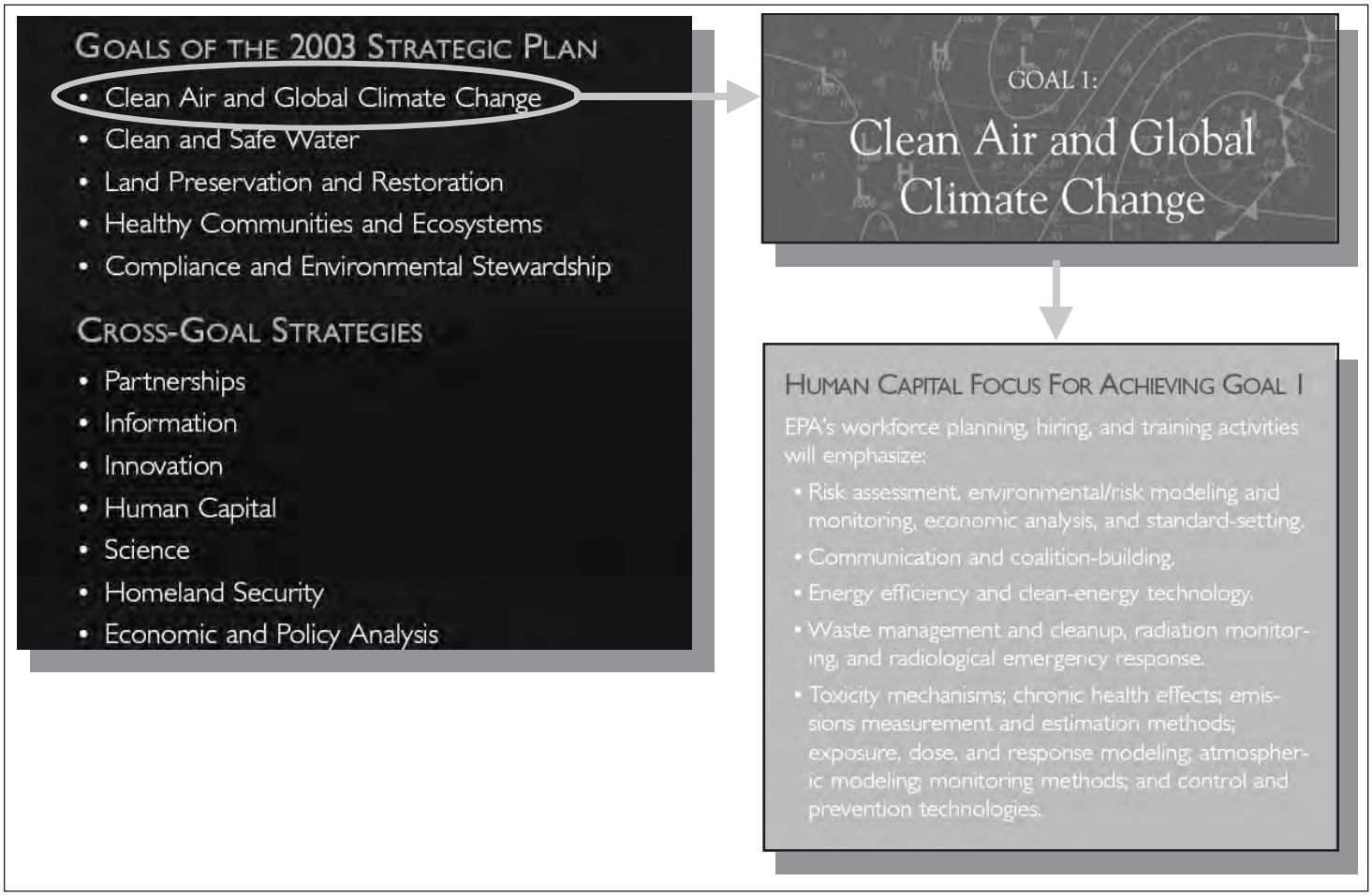
Leading organizations use succession planning and management as a strategic planning tool that focuses on current and future needs and develops pools of high-potential staff in order to meet the organization's mission over the long term. That is, succession planning and management is used to help the organization become what it needs to be, rather than simply to recreate the existing organization. We have previously reported on the importance of linking succession planning and management with the forward-looking process of strategic planning.[13] Specifically, discussing how workforce knowledge, skills, and abilities will contribute to the achievement of strategic and annual performance goals, how significant gaps are identified, and what mitigating strategies are proposed (such as hiring and training) can show the connection between succession planning and strategic planning. All four agencies have begun to link their succession planning to their strategic goals.

We previously reported that EPA's human capital strategy lacked some key elements, including the linking of human capital objectives to strategic goals.[14] Since then, EPA's current strategic plan recognizes that human capital management spans its 5 strategic goals and identifies specific workforce knowledge, skills, and abilities to achieve each goal. For example, as illustrated in figure 2, to achieve its goal for "Clean Air and Global Climate Change," EPA states that its workforce planning, hiring, and training activities will emphasize risk assessment, including environmental-risk modeling and monitoring, economic analysis, and standard setting, among other factors.

[13] GAO, *Human Capital: A Self-Assessment Checklist for Agency Leaders*, GAO/OCG-00-14G (Washington, D.C.: September 2000).

[14] GAO, *Human Capital: Implementing an Effective Workforce Strategy Would Help EPA to Achieve Its Strategic Goals*, GAO-01-812 (Washington, D.C.: July 31, 2001).

Figure 2: EPA's Strategic Goals and Associated Human Capital Focus



Source: EPA.

Separately, the succession plan states that the agency faces a number of future challenges, such as global pollution, and identifies key drivers shaping the agency's future work, such as science and technology advancements, budget constraints, administration priorities, agricultural practices, public expectations, and the media's influences. To respond to these drivers, EPA states that its employees must have the capacity to build stronger working partnerships, increase on-site problem solving, and enhance internal and external communication practices.

As a component of VA, VHA recognizes VA's strategic objective to "recruit, develop and retain a competent, committed and diverse workforce that provides high quality service to veterans and their families" in its *Workforce Succession Strategic Planning Guide*. To achieve this objective, VHA identifies a number of strategic assumptions about the future of veterans' health care. For example, it states that health care delivery will become more patient centered, that patients will be seen based on need instead of a predetermined schedule, and the use of in-home and interactive technology will increase, along with noninstitutional long-term care. Although VHA states that technological advances will improve access and quality of care for veterans, it does not anticipate significant impacts on the need for health care professionals over the next 5 years, and expects to continue to compete for scarce health care professionals in certain occupations.

DOL states that to meet its strategic goal of ensuring a competitive 21st century workforce, it plans to identify skill gaps, assess training needs, and recruit new employees. For example, DOL plans to shift from a historical enforcement role to compliance assistance and consultation, requiring stronger skills in communication and analysis. DOL seeks to develop more skills in technology and project management as well as in strategic planning, quantitative analysis, and analytical thinking for a more "business-like" management approach. To attract and retain employees with such skills, DOL launched the MBA Fellows program in 2002, which it considers one of its major succession development programs. The 2-year developmental program includes rotational assignments, mentoring, and promotional opportunities for successful graduates. In FY 2004, DOL reported retaining 89 percent of its MBA Fellows after 2 years.

Among the Census Bureau's strategic goals is its unique requirement to conduct the Decennial Census. According to the agency strategic plan, the Bureau plans to reengineer the 2010 Census so that it "is cost-effective, provides more timely data, improves coverage accuracy, and reduces operational risk." The agency will accomplish this by collecting

information on a yearly basis, enhancing address databases, using local geographic information, and undertaking operational tests of these new sources and methods. In its human capital plan, the Bureau acknowledges that reengineering the 2010 Census requires new skills in project, contract, and financial management; advanced programming and technology; and statistics, mathematics, economics, quantitative analysis, marketing, demography, and geography. To help obtain these skills, the Bureau has established training programs and developed competency guides. For example, it has instituted a Project Management Master's Certificate Program and an Information Technology Master's Certificate Program. All program managers now are to receive project management training.

Monitoring Mission-Critical Workforce Needs Helps Make Informed Succession Planning Decisions

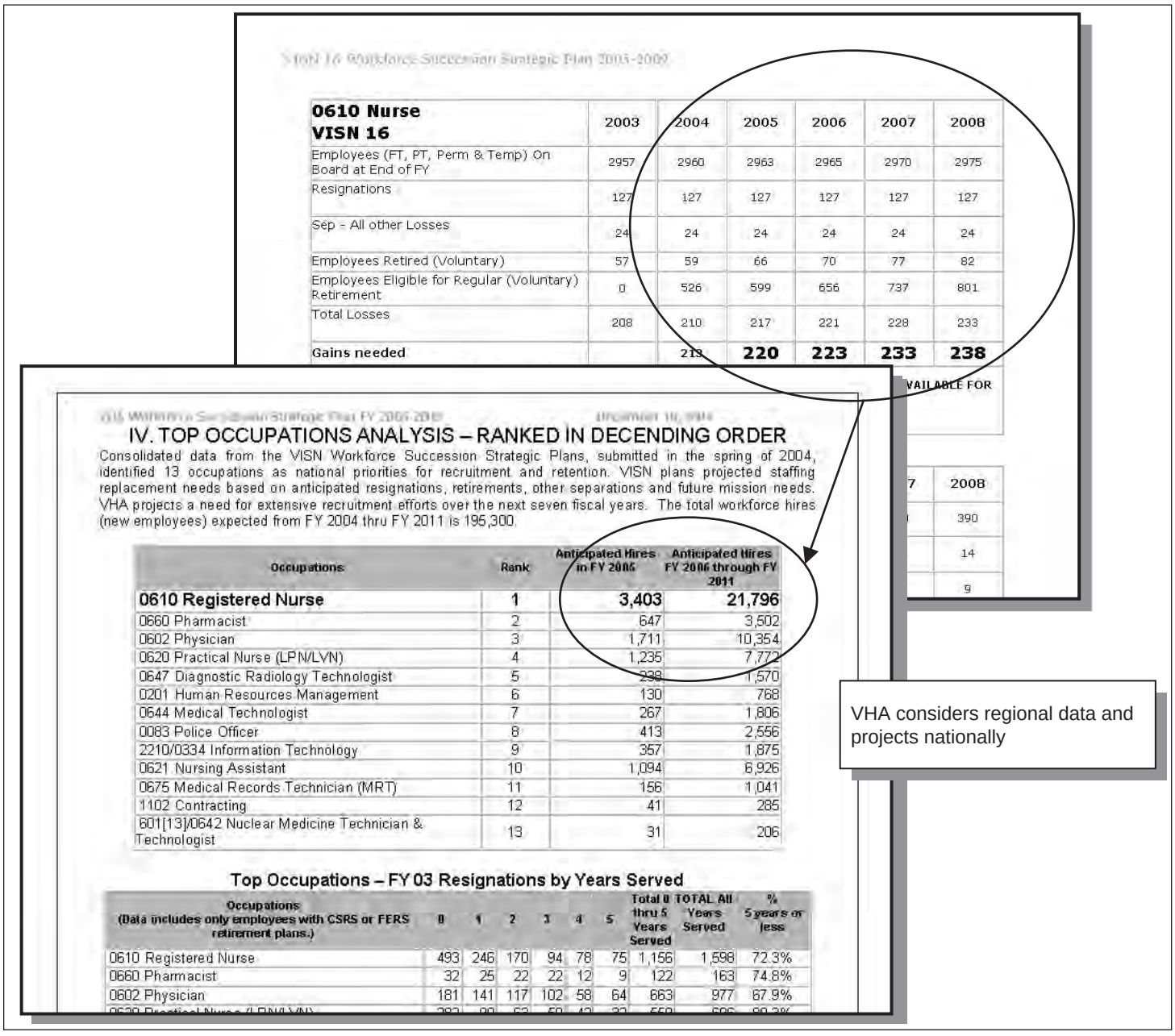
Leading organizations use succession planning and management to identify the talent required to achieve their goals. We have also identified key principles for effective workforce planning including determining the critical skills and competencies that will be needed to achieve current and future programmatic results; developing strategies that are tailored to address gaps in number, deployment, and alignment of human capital approaches for enabling and sustaining the contributions of all critical skills and competencies; and monitoring and evaluating the agency's progress toward its human capital goals and the contribution that human capital results have made toward achieving programmatic results.[15]

VHA, EPA, and DOL have identified gaps in occupations or competencies in their mission-critical workforce to achieve their goals, have undertaken strategies to address these gaps, and plan to or are taking steps to monitor their progress. By doing so, they can make more informed planning decisions and help appropriately focus succession efforts. While the Census Bureau has identified and is recruiting for its mission-critical occupations, it could achieve similar benefits if it more closely monitors its mission-critical workforce as it plans for the 2010 Decennial Census.

[15] GAO, *Human Capital: Key Principles for Effective Strategic Workforce Planning*, GAO-04-39 (Washington, D.C.: Dec. 11, 2003).

VHA has identified 13 occupations it deems as national priorities for recruitment and retention, including registered nurses, physicians, and nuclear medicine technicians, among others. VHA uses a Web-based tool with a workforce strategic planning template to help project its needs in these mission-critical occupations. Each VISN completes a comprehensive and detailed regional workforce assessment that projects staffing needs for priority occupations for at least the next 5 years. These projections are based on anticipated resignations, retirements, other separations, and future mission needs. VHA's workforce planner considers these data when projecting national staffing needs. For example, as illustrated in figure 2, VHA anticipates hiring 3,403 nurses in FY 2005 and 21,796 nurses from FY 2006 through FY 2011. This national projection includes, for example, the VISN 16 assessment that it will need from 220 to 238 nurses from FY 2005 to FY 2008.

Figure 3: VISN 16 Workforce Assessment and VHA's National Succession Plan



Source: VHA.

VHA also monitors and reports changes in its mission-critical workforce based on these data. For example, VHA reports that it increased the total nurses it had on-board by 6.2 percent or 2,184 from FY 1999 to FY 2004. VHA states that the succession programs implemented since 1999 have helped it to meet these mission-critical needs and, therefore, it does not plan to implement additional programs.

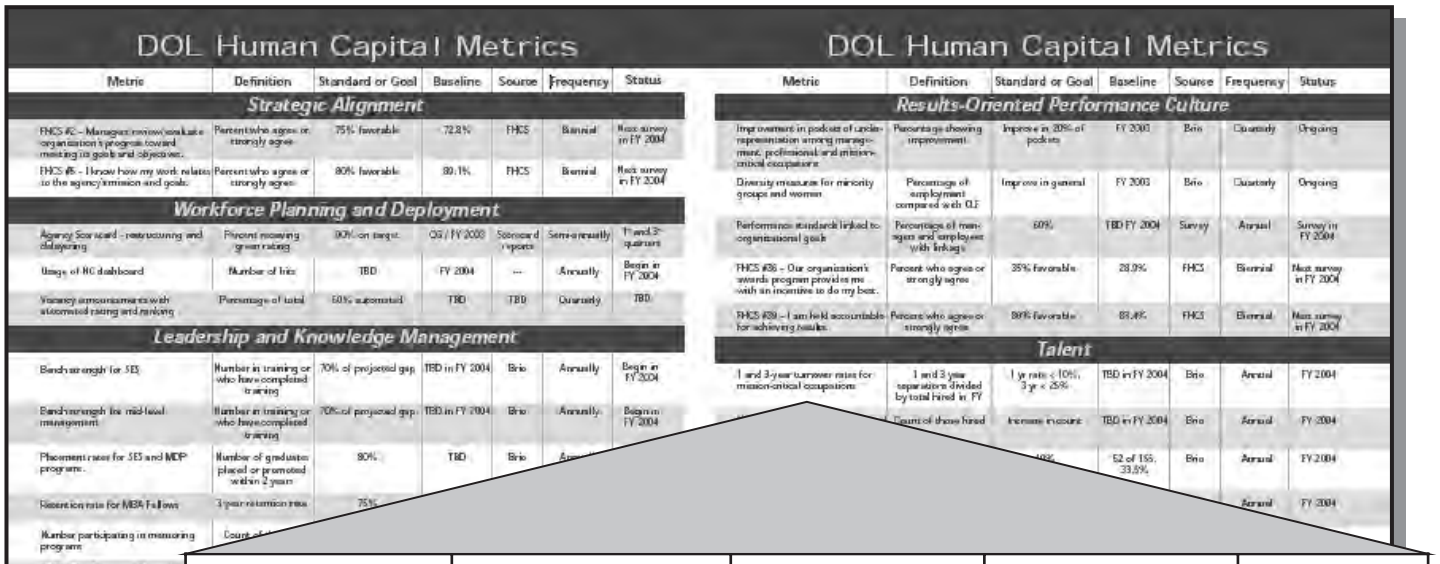
We previously recommended that EPA comprehensively assess its workforce needs.[16] Subsequently, EPA identified 18 priority occupations, including physical scientists, biologists, chemists, and attorneys. EPA projects each occupation's retirement, attrition, and accession rates based on historical averages. For example, EPA estimates that approximately 20 percent of the managers and supervisors in 10 of the 18 priority occupations will leave by 2008, mostly due to retirements. In addition, human capital officials stated that the agency's strategy has been on strengthening mission-critical competencies among their priority occupations. For example, EPA has identified 12 technical competencies, such as information management and sciences and biological sciences, and 12 cross-occupational competencies, such as teamwork and oral communication, that are essential for the agency to acquire, retain, or develop to accomplish its future mission. EPA plans to address emerging mission-critical competencies and gaps in priority occupations through recruitment and development. EPA also plans to update its 2004 strategic workforce planning effort on a cyclical basis to monitor progress in closing any gaps, but the agency did not indicate specific time frames for these updates.

DOL has identified 27 mission-critical occupations, such as investigators, workforce development specialists, and mining engineers as well as the skills needed for each occupation, which it specifies in competency models. For example, for criminal investigators, DOL identified skills such as external awareness and interpersonal communication in addition to the knowledge and conduct of investigations. DOL has also inventoried the skills of its on-board mission-critical workers through the department's mission-critical Skills Assessment Initiative. DOL reports that its component agencies are developing action plans to reduce or close skill gaps which DOL is incorporating into its human capital planning and reporting process.

[16] GAO-01-812.

In addition, DOL has developed performance measures that are designed to help it gauge its organizational capacity, as illustrated in figure 4. For example, for FY 2004 DOL reported a 5 percent turnover rate of its mission-critical employees during their first year, meeting its goal of less than 10 percent. Likewise, DOL reported a 19.5 percent turnover rate during their first 3 years, meeting its goal of less than 25 percent. In addition, DOL reported a 95.4 percent FTE utilization rate, the percentage of filled and authorized, full-time equivalent positions, for FY 2004, compared with a 98 percent goal.

Figure 4: Selected DOL Performance Measures Designed to Gauge Organizational Capacity



Metric	Definition	Standard/ Goal	FY 2004 (actual)	Frequency Measured
1 and 3-Year Turnover for Mission-Critical Occupations	1 and 3-Year separations divided by total hired in FY	1-year rate<10% 3-year rate<25%	1-year rate = 5% 3-year = 19.5%	Annually
FTE Utilization	FTE Utilized/FTE authorized	98%	95.4%	Annually

Source: DOL.

The Census Bureau has identified its mission-critical occupations and is recruiting for statisticians, mathematical statisticians, information technology specialists, cartographers, and geographers on its employment Web site. According to an agency human capital official, the Census Bureau does not monitor or assess gaps in numbers by mission-critical occupation, but focuses on "building infrastructure" by recruiting and developing competencies. The same official stated that the Bureau delegates decisions to line managers to fill vacancies, and thus there is no need to assess workers by mission-critical categories. To assist these managers, the Bureau reports that an electronic hiring system allows them to identify competencies for each vacancy, and that line managers engage in a continuing dialogue with senior managers, the Hiring Coordinators Group, and the Human Capital Management Council to address hiring needs. Nevertheless, while line managers are appropriately concerned with filling vacancies, as noted earlier, the Bureau has also acknowledged that reengineering the 2010 Decennial Census requires new competencies. By not monitoring its mission-critical occupations more closely and at a higher level, Census may not know overall if it is acquiring the skills it needs to be prepared to conduct the 2010 Decennial Census as efficiently or effectively as possible.

Enhanced Coordination and Evaluation of Training and Development Programs Could Help Leverage Scarce Resources

Effective training and development programs can enhance the federal government's ability to achieve results. Further, effective succession planning and management efforts identify talent from multiple organizational levels, early in their careers, or with critical skills as well as provide both formal training and opportunities for rotational, developmental, or "stretch" assignments, to strengthen high-potential employees' skills and to broaden their experience and perspective.[17] While all four agencies offer core succession training and development programs, they each can seek opportunities to achieve efficiencies through more coordination and sharing of these programs. In addition, establishing valid measures to better evaluate how these programs affect organizational capacity can give agency decision makers credible information to justify training and development programs' value.

[17] GAO-03-914.

Agency Succession Efforts Include Training and Development for Employees across Organizational Levels

All four agencies offer programs to train and develop their entry-, middle-, and senior-level employees. These programs provide opportunities for formal training, and all but one program offers rotational or developmental assignments.[18] Table 1 provides a summary of core succession training and development programs by agency.

Table 1: Agencies' Core Succession Training and Development Programs

	Level of training		
Program	**Entry**	**Middle**	**Senior**
Census Bureau (DOC Programs)			
Aspiring Leaders Development Program	x	x	
Executive Leadership Development Program	x	x	
SES Candidate Development Program			x
DOL			
MBA Fellows Program	x	x	
Management Development Program		x	
SES Candidate Development Program			x
EPA			
EPA Intern Program	x		
EPA Rotational Program	x		
Mid-level Development Programs	x	x	
SES Candidate Development Program			x
VHA			
Facility LEAD Program	x		
VISN LEAD Program		x	
Executive Career Field Candidate Development Program			x

Source: Census Bureau, DOC, DOL, EPA, and VHA.

Note: Agency human capital officials identified these as their core succession training and development programs.

[18] EPA's Mid-level Development Programs do not offer formal rotational assignments but rotations are available to all employees.

At the senior level, all four agencies have succession training and development programs intended to enhance leadership skills, primarily through SES candidate development programs. For example, EPA's SES Candidate Development Program—designed to prepare a cadre of leaders to fill future vacant executive positions in the agency and to maintain valuable institutional knowledge—requires candidates to complete an executive development plan and work with an SES mentor and executive coach to help define career goals and provide guidance. The program also requires participants to complete at least 80 hours of formal leadership development training, as well as complete a 4-month developmental assignment. DOL and VHA have similar programs in place. The Census Bureau, as a component of DOC, participates in DOC's SES Candidate Development Program.

The four agencies also have programs intended to develop the leadership and supervisory skills for middle-level managers. For example, VHA's program named "VISN LEAD" provides an opportunity for high-potential employees in field locations to receive coaching and mentoring, create a personal development plan, and join with special VISN-wide project task teams, while retaining their current responsibilities. EPA's Mid-level Development Programs, DOL's Management Development Program, and DOC's Executive Leadership Development Program—in which the Census Bureau participates—all offer similar opportunities.

At the entry level, all agencies have programs intended to develop employees and provide them with the foundation for future leadership. For example, DOL's MBA Fellows program requires participants to take a minimum of four rotational assignments and core training classes, complete a personal development plan, and work with a senior-level mentor, among other activities. Targeting recent MBA graduates, DOL established its program not only to address increased departmentwide needs for business and project-management skills, but also to create a cadre of future department leaders. EPA's Intern Program and Rotational Program, VHA's Facility LEAD Program, and DOC's Aspiring Leaders Development Program, in which the Census Bureau participates, are similar in nature.

According to agency human capital officials, other programs also contribute to their succession efforts. For example, the Census Bureau has established certificate programs in project management and leadership for all employees to develop and enhance these specific skills. The Bureau also has a mathematical statisticians program, which, according to the Deputy

Director, provides career enhancement opportunities designed to help develop and retain employees in this critical occupation. Similarly, DOL has a Career Assistance Program that provides employees at all levels with career planning advice and other development assistance. In addition, the agencies use formal mentoring or coaching programs to help guide employees throughout their career.

Coordination and Sharing of Training and Development Programs Can Achieve Efficiencies

As agencies implement their core succession training and development programs, they must plan and prepare for the possibility of significant and recurring constraints on their resources, in light of fiscal and budgetary constraints. Recognizing this, leading agencies look for opportunities to coordinate and share their efforts and create synergies through benchmarking with others, achieving economies of scale, limiting duplication of efforts, and enhancing the effectiveness of programs, among other things.[19] An example of such a coordinated and shared training effort is the recent announcement of a new partnership by the Office of Federal Procurement Policy, Department of Defense, and the General Services Administration. The initiative is geared toward the civilian and defense acquisition workforces, and is intended to provide similar training and development opportunities for acquisition personnel across all three agencies with the goal of sharing best practices, among other things.

OPM has begun to serve as a bridge for agencies to seek opportunities to coordinate their succession training and development programs as it shifts its role from less of a rule maker and enforcer to more of a strategic partner in leading and supporting agencies' human capital management. For example, OPM established a governmentwide Federal Candidate Development Program (Fed CDP). OPM expects the 14-month program to help agencies meet their SES succession planning goals and contribute to the government's efforts to create a high-quality SES leadership corps. Participating agencies may select, without further competition, people who have successfully completed the Fed CDP training program. In addition, we have testified that approaches to interagency collaboration, such as the CHCO Council, have emerged as an important central leadership strategy

[19] GAO, *Human Capital: A Guide for Assessing Strategic Training and Development Efforts in the Federal Government*, GAO-04-546G (Washington, D.C.: March 2004).

and that agency collaboration can serve to institutionalize many management policies governmentwide.[20] The Leadership and Succession Planning Subcommittee of the CHCO Council is charged with reviewing leadership development, among other things, and is a possible mechanism to help agencies coordinate succession training and development programs.

While some agencies' human capital officials acknowledged the potential benefits of coordinating succession training and development programs with other agencies or departments, they all could do more to seek coordination and sharing opportunities. Cognizant human capital and training officials stated that they had not actively sought opportunities to coordinate core succession training and development programs. Although EPA plans to select one senior executive through the Fed CDP, human capital officials stated they had not extensively explored the idea of coordinating with other agencies for their core succession training and development. VHA human capital officials said they did not coordinate further because they have specialized skill needs. DOL and Census Bureau human capital managers also stated that they had not partnered with other outside agencies to coordinate their core succession training and development programs. By not actively seeking to coordinate and share core succession training and development programs, agencies may miss a potentially valuable opportunity to gain efficiency, which may be especially important in the current budget environment.

Performance Measures Can Help Agencies Assess Programs' Effects on Organizational Capacity

Decision makers need credible information to justify training and development programs' value. We have also reported that agencies need credible information to assess how their training and development programs affect organizational performance and enhance organizational capacity.[21] We have observed in our guide for assessing strategic training and development that while not all training and development programs require, or are suitable for, higher levels of evaluation, establishing valid performance measures can ensure that agencies adequately address their development objectives. Moreover, our guide states that such measures

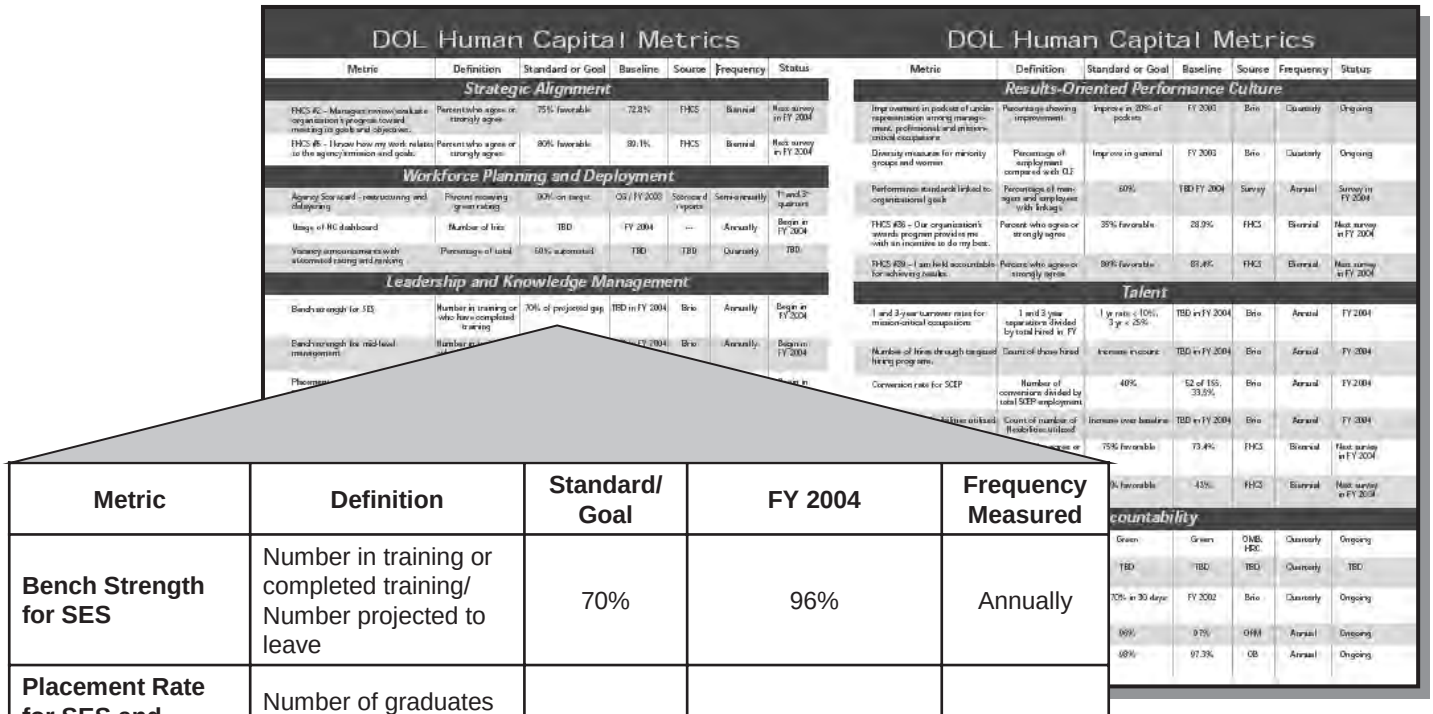
[20] GAO, *Human Capital: Observations on Agencies' Implementation of the Chief Human Capital Officers Act*, GAO-04-800T (Washington, D.C.: May 18, 2004) and *Posthearing Questions Related to Agencies' Implementation of the Chief Human Capital Officers (CHCO) Act*, GAO-04-897R (Washington, D.C.: June 18, 2004).

[21] GAO-04-546G.

should go beyond input and output data, and can include data on quality, costs, and time. We also recognize, however, that agencies need to scale their efforts depending on the program. Factors to consider when deciding on the appropriate level of evaluation include the estimated costs of training efforts, size of training audience, and program visibility, among other things.

All four agencies are able to report on participation and cost related to their succession training and development programs. For example, 12 Census Bureau employees participated in DOC's Aspiring Leaders Development Program in FY 2004, with an average cost of $6,267 per participant, according to the Bureau. In addition, the Census Bureau and DOL have also identified outcome measures related to the performance of some of their succession-related training and development programs. For example, the Census Bureau evaluates, among other things, the extent to which certified project managers are using the skills they have learned in the Project Management Masters Certificate Program. Only DOL has identified measures intended to provide an understanding of core succession training and development programs' effects on organizational capacity. Figure 5 illustrates a selection of these measures.

Figure 5: Selected DOL Human Capital Measures Related to Succession Planning and Management



Metric	Definition	Standard/ Goal	FY 2004	Frequency Measured
Bench Strength for SES	Number in training or completed training/ Number projected to leave	70%	96%	Annually
Placement Rate for SES and Management Development (MDP) Programs	Number of graduates placed or promoted within 2 years/ Number of graduates	80%	SES – 68% placed MDP - 51%[a]	Annually
Retention Rate for MBA Fellows	3-year retention rate	75%	89%[b]	Annually
Number Participating in Mentoring Program	Number in mentoring program	100	119	Annually

Source: DOL.

[a]Promoted to date. Candidates are eligible for promotion through February 2006.
[b]Currently retained after 2 years.

For example, by considering the retention rate for MBA Fellows, DOL can make informed planning decisions about the potential availability of certain skill sets in the department as well as when to initiate a new program and how many students to include in it. DOL reported that in FY 2004, it retained 89 percent of its MBA fellows after 2 years and has a

goal of 75 percent after 3 years. DOL also tracks SES "bench strength," a ratio of senior executives who are in training or have completed training to those projected to leave. DOL reported a 96 percent "bench strength" for its senior executives in FY 2004, exceeding its goal of 70 percent. The Census Bureau, VHA, and EPA could better demonstrate their programs' value in providing future talent by identifying outcome-oriented measures and evaluating the extent to which these programs enhance their organizations' capacity.

Agencies Use Succession Efforts to Enhance Workforce Diversity

Leading organizations recognize that diversity, ways in which people in a workforce are similar and different from one another, is an organizational strength and that succession planning is a leading diversity management practice.[22] Given the retirement projections for the federal government that could create vacancies, agencies can use succession planning and management as a critical tool in their efforts to enhance diversity in their leadership positions. All of the selected agencies have recognized the importance of diversity to a successful workforce and use succession planning and management efforts to enhance their workforce diversity.

VA requires all of its administrative staff offices to produce workforce and succession plans aligned with overall VA strategic planning. VHA states that although its overall workforce is fairly diverse, women and minorities are not well represented in leadership positions nor are they well represented in the pipeline to such positions. We have reported that VHA has integrated diversity planning into its succession efforts.[23] As part of their regional succession plans, VISNs submit diversity information to VHA for national planning. VHA then analyzes the diversity of its top-priority occupations, highlights underrepresentation of certain demographic groups in specific mission-critical occupations, and provides guidance to focus recruiting efforts to enhance diversity. For example, VHA states that White females and American Indian/Alaskan Native females are underrepresented in the nurse occupation and advises that recruitment efforts should focus on them. In addition, VHA tracks applicant diversity for the Executive Career Field Candidate Development Program, one of

[22] GAO, *Diversity Management: Expert-Identified Leading Practices and Agency Examples*, GAO-05-90 (Washington, D.C.: Jan. 14, 2005).

[23] GAO-05-90.

VHA's core succession training and development programs, and reports that applicants to this program are drawn from a diverse pool.

EPA has stated in its human capital plan that a diverse workforce makes the agency a more effective and healthy organization that is better able to relate to the American people and develop more creative and workable solutions. EPA credits its Intern Program, one of its core succession training and development programs, with attracting and retaining a diverse group of employees based on a 2003 assessment of the program. For example, the assessment found that EPA interns were more ethnically diverse than other comparable groups of hires. As part of its diversity action plan, EPA reports that it is expanding targeted recruitment initiatives to identify well-qualified candidates for mission-critical occupations. In addition, regional offices report succession-related efforts intended to enhance diversity initiatives, such as mentoring, leadership, and career development programs, and workforce demographic analyses, among other activities.

DOL identifies a strategic initiative to enhance diversity in management and mission-critical occupations in its human capital plan. To help it achieve this initiative, DOL monitors and evaluates diversity information for its mission-critical occupations annually, and has identified "pockets of low participation" for certain minority groups, such as Hispanics. In addition, DOL has reported a higher percentage of women and Hispanics in its three core succession training and development programs than in its general workforce.

The Census Bureau has established a diversity program office to manage the Bureau's diversity efforts. Bureau officials stated that because of the highly specialized nature of the Bureau's work, such as the use of statistics and mathematics, and the relatively small pool of people trained in these areas, it is difficult to enhance diversity in several critical occupation categories. As part of its combined diversity and recruiting initiative, the Bureau has established a specific recruiting team for mathematical statisticians, one of its highlighted mission-critical occupations. The Bureau also has various targeted recruiting efforts at academic institutions and community organizations with high Hispanic and other minority enrollment, and various Hispanic or Latino Chambers of Commerce.

Conclusions

The Census Bureau, DOL, EPA, and VHA have all implemented succession planning and management efforts that collectively are intended to strengthen organizational capacity. Generally, these efforts receive top leadership support, link with strategic planning, identify critical skills gaps and strategies to fill them, offer training and development programs for high-potential employees, and enhance diversity. Nevertheless, given the nation's large current budget deficit and long-range fiscal imbalance, Congress is likely to place increasing emphasis on agencies to exercise fiscal restraint.

Given this environment, these agencies can look for opportunities to coordinate and share their succession training and development programs to achieve economies of scale, limit duplication of efforts, increase efficiency, and enhance the effectiveness of their programs. For example, all four agencies emphasize rotational or developmental assignments and formal training, and they may have opportunities to coordinate and share these assignments and training with each other or other federal agencies or departments. Agencies can also work with OPM and the CHCO Council to determine how they can better leverage other agencies' succession training and development programs.

Furthermore, it is increasingly important for agencies to evaluate their training and development programs to be able to demonstrate how these efforts enhance organizational capacity. While the Census Bureau, EPA, and VHA have some information on their succession training and development programs, such as participation and cost, they can take additional steps, such as enhanced evaluations, to justify these programs' value. DOL has identified measures intended to provide an understanding of these programs' effects on organizational capacity.

Finally, although the Census Bureau has identified and is recruiting for its mission-critical occupations, it can better monitor its mission-critical workforce. By not monitoring more closely and at a higher level than line managers, the Bureau may not know how to best focus its succession planning efforts, and ultimately how well it is prepared for major tasks, such as the 2010 Decennial Census.

Recommendations for Executive Action

To help agencies reinforce their succession planning and management efforts, and make well informed planning decisions, we recommend a number of actions.

The Secretary of Commerce should ensure that the Director of Census takes the following three actions:

- Strengthen the monitoring of its mission-critical workforce by identifying mission-critical workforce gaps, developing strategies to address gaps, evaluating progress toward closing gaps, and adjusting strategies accordingly.

- Seek appropriate opportunities to coordinate and share core succession training and development programs with other outside agencies to achieve economies of scale, limit duplication of efforts, benchmark with high-performing agencies, keep abreast of current practices, enhance efficiency, and increase the effectiveness of its programs.

- Evaluate core succession training and development programs to assess the extent to which programs contribute to enhancing organizational capacity. When deciding the appropriate analytical approach and level of evaluation, the Bureau should consider factors such as estimated costs of training efforts, size of training audience, and program visibility, among other things.

The Administrator of EPA should take the following two actions:

- Seek appropriate opportunities to coordinate and share core succession training and development programs with other outside agencies to achieve economies of scale, limit duplication of efforts, benchmark with high-performing agencies, keep abreast of current practices, enhance efficiency, and increase the effectiveness of its programs.

- Evaluate core succession training and development programs to assess the extent to which programs contribute to enhancing organizational capacity. When deciding the appropriate analytical approach and level of evaluation, EPA should consider factors such as estimated costs of training efforts, size of training audience, and program visibility, among other things.

The Secretary of Labor should take the following action:

- Seek appropriate opportunities to coordinate and share core succession training and development programs with other outside agencies to achieve economies of scale, limit duplication of efforts, benchmark with high-performing agencies, keep abreast of current practices, enhance efficiency, and increase the effectiveness of its programs.

The Secretary of VA should take the following two actions:

- Seek appropriate opportunities to coordinate and share core succession training and development programs with other outside agencies to achieve economies of scale, limit duplication of efforts, benchmark with high-performing agencies, keep abreast of current practices, enhance efficiency, and increase the effectiveness of its programs.

- Evaluate core succession training and development programs to assess the extent to which programs contribute to enhancing organizational capacity. When deciding the appropriate analytical approach and level of evaluation, VHA should consider factors such as estimated costs of training efforts, size of training audience, and program visibility, among other things.

Agency Comments and Our Evaluation

We provided a draft of this report to the Secretaries of Commerce, Labor, and VA and the Administrator of EPA for their review and comment. In addition, we provided a draft of this report to the Acting Director of OPM and the CHCO Council's Leadership and Succession Planning Subcommittee for their information.

VA agreed with our findings and recommendations. In response to our recommendation to seek opportunities to coordinate and share core succession training and development programs, VA suggested that OPM could act as a "clearinghouse" by gathering and publishing curricula and other relevant training information from agencies, thus enabling agencies to identify existing training programs across the government. We present VA's written comments in appendix II. DOC and the Census Bureau agreed with our findings and our recommendations to seek opportunities to coordinate core succession training and development programs and to evaluate the extent to which these programs enhance organizational capacity. In response to our recommendation to strengthen the monitoring

of its mission-critical workforce, the Census Bureau stated that its existing approach is effective in meeting its needs. However, as we discussed earlier, the Census Bureau acknowledges that reengineering the 2010 Decennial Census requires new competencies. By not strengthening the monitoring of its mission-critical workforce, the Census is at increased risk that it will not have the skills it needs to be prepared to conduct the 2010 Census as efficiently or effectively as possible. For example, a lesson from the 2000 Census was that while contracts for various projects supported decennial census operations, they did so in many instances at a higher cost than necessary because the Census Bureau did not have sufficient contracting and program staff with the training and experience to manage them.[24] We present DOC's and the Census Bureau's written comments in appendix III. DOL did not take issue with our findings, stated that it will consider our recommendations, and provided technical comments, which we incorporated as appropriate. EPA did not comment on our recommendations, but provided a technical comment, which we incorporated.

As agreed with your offices, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days after its date. At that time, we will provide copies of this report to other interested congressional parties; the Secretaries of Commerce, Labor, and VA; the Administrator of EPA; the Director of Census; the Acting Director of OPM; and the CHCO Council's Leadership and Succession Planning Subcommittee. We will also make this report available at no charge on the GAO Web site at http://www.gao.gov.

[24] U.S. Department of Commerce's Office of Inspector General, *What Census 2000 Can Teach Us in Planning for 2010*, Report No. OIG-14431 (Spring 2002).

If you or your staff have any questions about this report, please contact me on (202) 512-6806 or at larencee@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix IV.

Eileen Larence
Director, Strategic Issues

Objectives, Scope, and Methodology

To review how federal agencies are implementing succession planning and management efforts, we selected the Department of Labor (DOL), the Veterans Health Administration (VHA), the Environmental Protection Agency (EPA), and the Census Bureau for our review. We considered the nature of their succession challenges, agency missions, and prior GAO human capital work conducted at these agencies. These agencies represent an array of organizational structures, missions, and succession challenges.

We analyzed strategic, human capital, workforce, succession, and training and development plans, performance contracts, human capital team charters, and diversity information from the selected agencies. In addition, we reviewed policies and guidance on succession-related issues from the Office of Personnel Management (OPM), the Equal Employment Opportunity Commission (EEOC), and the Merit Systems Protection Board (MSPB) because of their responsibilities for ensuring the fair application of personnel decisions, such as selection for training and development programs. We also interviewed agency, OPM, EEOC, and MSPB officials involved with strategic, human capital, and succession planning and management.

The scope of our work did not include independent evaluation or verification of the effectiveness of the succession planning and management initiatives used in the four agencies, including any performance results that agencies attributed to specific practices or aspects of their programs. We assessed the reliability of staffing and projection data provided to us by the Census Bureau, DOL, EPA, VHA, and OPM to ensure the data we used in this report were complete and accurate by (1) interviewing agency officials knowledgeable about the data and (2) performing manual and electronic testing, when applicable. We determined that these data were sufficiently reliable for the purposes of this engagement.

To get the varied perspectives of agencies' staff located in headquarters and regional offices, we interviewed agency officials in Washington, D.C.; Charlotte, North Carolina; and Los Angeles and San Francisco, California. We conducted our study from June 2004 through April 2005.

Comments from the Department of Veterans Affairs

THE DEPUTY SECRETARY OF VETERANS AFFAIRS
WASHINGTON

June 13, 2005

Ms. Eileen Larence
Director
Strategic Issues
U. S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Larence:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office's (GAO) draft report, ***HUMAN CAPITAL: Selected Agencies Have Opportunities to Enhance Existing Succession Planning and Management Efforts,*** (GAO-05-585). The Department agrees with GAO's overall conclusions and concurs with the recommendations. The enclosures provide additional discussion on the recommendations.

VA appreciates the opportunity to comment on your draft report.

Sincerely yours,

Gordon H. Mansfield

Enclosures

Enclosure

THE DEPARTMENT OF VETERANS AFFAIRS (VA) COMMENTS
TO GOVERNMENT ACCOUNTABILITY OFFICE (GAO)
DRAFT REPORT
HUMAN CAPITAL: Selected Agencies Have Opportunities to Enhance Existing Succession Planning and Management Efforts
(GAO-05-585)

- **To help agencies reinforce their succession planning and management efforts, and make well informed planning decisions, we recommend a number of actions. Specifically, the Secretary of VA should take the following actions:**

  Seek appropriate opportunities to coordinate and share core succession training and development programs with other outside agencies to achieve economies of scale, limit duplication of efforts, benchmark with high-performing agencies, keep abreast of current practices, enhance efficiency, and increase the effectiveness of its programs.

Concur – The Department of Veterans Affairs (VA) agrees with GAO's underlying rationale that improved coordination among and between federal agencies would strengthen training programs across the federal sector. As an alternative means of implementation, the Department suggests that the Office of Personnel Management (OPM) serve as a clearinghouse for information sharing. For example, VA could provide information to OPM on the target audience, a description of its training programs, and the curricula. OPM, in turn, would publicize such information, allowing other agencies to pick and choose best practices for adoption into their own organizations. This would maximize each agency's ability to identify existing training programs throughout the government that might provide targeted training content for occupational, professional, technical or supervisory skills, and would achieve the objectives contemplated in the recommendation efficiently and effectively.

Evaluate core succession training and development programs to assess the extent to which programs contribute to enhancing organizational capacity. When deciding the appropriate analytical approach and level of evaluation, VHA should consider factors such as estimated costs of training efforts, size of training audience, and program visibility, among other things.

Concur - In January 2005, the Veterans Health Administration (VHA) established a method for evaluating its succession planning and leadership development programs. A detailed action plan describing this evaluation process, as well as

1

Enclosure

THE DEPARTMENT OF VETERANS AFFAIRS (VA) COMMENTS
TO GOVERNMENT ACCOUNTABILITY OFFICE (GAO)
DRAFT REPORT
HUMAN CAPITAL: Selected Agencies Have Opportunities to Enhance Existing Succession Planning and Management Efforts
(GAO-05-585)

other actions being taken to implement the recommendation, is included as an enclosure to this response.

2

VETERANS HEALTH ADMINISTRATION (VHA)
Action Plan
GAO Draft Report: *HUMAN CAPITAL: Selected Agencies Have Opportunities to Enhance Existing Succession Planning and Management Efforts,*
(GAO-05-585)

Recommended Improvement Action(s): The Secretary of VA should take the following action to evaluate core succession training and development programs to assess the extent to which programs contribute to enhancing organizational capacity. When deciding the appropriate analytical approach and level of evaluation, VHA should consider factors such as estimated costs of training, size of training audience, and program visibility, among other things.

Concur

Goal: To ensure VHA's succession training and development plans enhance the organization's ability to face current and future organization challenges.

Strategy:

Detailed information concerning VHA's workforce planning efforts, including the VHA succession strategic planning guidance and Veterans Integrated Service Network (VISN) plans for 2006-2010, and the VHA 2005-2009 workforce succession strategic plans is available to the Department of Veterans Affairs (VA) entities on the VHA Succession Planning Web Site. Enhancements to this website are continually being made and information is updated on an ongoing basis. VHA's three major succession training and development programs are: the Executive Career Field (ECF) Development program, the VISN Leadership Effectiveness Accountability and Development (LEAD) program, and the facility LEAD program.

In May 2005, VHA's National Leadership Board (NLB) began reviewing the fiscal year (FY) cost proposals and mid-year status of the national programs on a bi-annual basis. These are reported to NLB by the VHA Succession and Workforce Development Management Subcommittee through the VHA Human Resource Committee (HRC). Also in May 2005, VHA initiated bi-annual reviews of the participant size and scope, based on retirement and other losses. The findings are also reported to NLB by the VHA Succession and Workforce Development Management Subcommittee through VHA HRC.

The ECF Candidate Development program uses the eight VHA core High Performance Development Model (HPDM) competencies as a framework for VHA to develop a highly skilled, customer-centered workforce. Research was implemented in January 2005 by the Management Support Office in collaboration with the VHA Center for Organization Leadership and Management Research (COLMR) to establish criteria to evaluate the mentoring and precepting process of

1

the candidate's development program (CDP). The research will be completed in the summer of 2005 and presented to the VHA Succession and Workforce Development Management Subcommittee and forwarded on to HRC and NLB for feedback and approval.

The Management Support Office and COLMR are also researching the ECF CDP rating and selection process (to validate the selection process), the ECF CDP's acceptance to the program with the HPDM 360 degree assessment of their critical core competencies/critical skills set, and the effects of ECF CDP on their manager's evaluation, their career advancement and turnover rates. Results of this research will be completed in summer 2006, although elements of it will be completed sooner. The results will be forwarded to the NLB for feedback and approval prior to implementation. When possible, research findings associated with the VHA leadership Development and Succession Planning program will be published.

The VISN LEAD program is based on six key elements designed to establish criteria for a successful leadership development program that will develop leaders and meet VHA's organizational goals for succession and diversity. The criteria were defined by the VHA LEAD steering committee that consists of all the VISN education coordinators. Annual assessment against these criteria served as a national performance measure for each VISN in FY 2004 and FY 2005 and will continue. Status and progress of the program is reported to the VHA Succession & Workforce Development Subcommittee by the VHA LEAD steering committee and Management Support Office. Attached are the criteria VISNs are measured on for the performance measure (Attachment A). A report summarizing findings of the LEAD assessment goes to the VHA Succession & Workforce Development Subcommittee. The VHA LEAD Steering Committee holds quarterly meetings to coordinate and share training information and programs. Since the establishment of this committee in 2004, VISNs across the system have partnered in the management of leadership development and this is ongoing. Participants in VISN LEAD programs are entered into the VHA Leadership and Workforce Development database for succession planning purposes.

The VHA LEAD Steering Committee also oversees the guidance and monitoring of the facility level LEAD programs. Status and progress is reported by the VHA LEAD Steering committee and Management Support Office to the VHA Succession & Workforce Development Subcommittee. An annual national performance measure for the facility level LEAD will be established for the FY 2006 performance cycle. Similar criteria as those used in the VISN LEAD program are being developed and are expected to be ready for use in the FY 2006 performance cycle. Sharing of information across the system concerning this program is already ongoing. Participants in facility LEAD programs will be entered into the VHA Leadership and Workforce Development Database for succession planning purposes.

2

ATTACHMENT A
LEAD
PROGRAM CERTIFICATION

CRITERIA	MINIMUM ELEMENTS	YES*	NO*
Needs Assessment	1) Outcomes from Workforce Strategic Planning (WF SP) process were driven by and linked to strategic planning. (i.e., curriculum and selection process linked to strategic plan).		
Program Design	2) Course curriculums will include training in all eight (8) HPDM core competencies.		
Program Design	3) Program design includes a variety of learning and instructional methodologies.		
Program Design	4) Formal mentoring and/or coaching is included in the program.		
Program Design	5) Program participants complete a Personal Development Plan (PDP) with the collaboration of both their supervisor and mentor and/or coach		
Program Design	6) At least one individual assessment tool is used.		
Selection Process	7) Programs are widely announced thru a variety of mechanisms.		
Selection Process	8) A formal application process allows employees to self-nominate to the program with the endorsement of their supervisor.		
Evaluation	9) Program has a formal evaluation process in place that assesses the reactions of the participants to the program.		
Evaluation	10) Participants are asked to make recommendations for changes in the program		
Leadership Support	11) Evidence of resources to support program		
Leadership Support	12) Supervisors endorse participant application to the program		
Leadership Support	13) Senior Leaders (ELC members, Triad) are involved in the program		
Reward and Recognition	14) Participants are acknowledged by executive leadership that they were part of the program		

* A statement of "yes" certifies that the minimal criteria of LEAD are in place and relates to a score of one (1) or greater on the self-assessment tool. A statement of "no" equals a score of zero on the self-assessment tool.

SIGNATURE OF FACILITY/VISN DIRECTOR DATE

1

BEST PRACTICE PROGRAM ASSESSMENT GUIDE

CRITERIA CATEGORY	ELEMENTS	EVALUATION	SCORE	SELF ASSESSMENT
NEEDS ASSESSMENT	1) Outcomes from WF SP process were driven by and linked to strategic planning	None	O	
		Present	3	
PROGRAM DESIGN	1) Curriculum shows evidence of training in all eight (8) HPDM core competencies.	None	0 Points	
		Present	3 Point	
	2) Program design includes a variety of learning and instructional methodologies. (stretch assignments – projects)	No specific design identified	0 POINTS	
		The program design follows adult learning principles for classroom or didactic instruction.	1 POINT	
		The program design includes the use of a variety of learning methodologies (i.e., distance learning, independent learning experiences, case studies)	2 POINTS	
		The program design includes opportunities for participants to apply skills outside the classroom. (i.e., assignments, projects, action learning projects)	3 POINTS	

2

CRITERIA CATEGORY	ELEMENTS	EVALUATION	SCORE	SELF ASSESSMENT
		SCORE:		
	3) Formal mentoring and/or coaching is included in the program	No mentoring or coaching component	0 POINTS	
		-An application process is in place to select mentors and coaches. -A matching process is utilized to pair mentors and coaches based on skill, interests and expertise. -Coaches and mentors are trained and/or demonstrate basic skill requirements are met.	1 POINT	
		There is ongoing training offered in the facility and/or VISN for the purposes of continuing to improve and increase the skills of coaches and mentors.	2 POINTS	
		The coaching and mentoring program is evaluated and feedback is utilized to improve the program.	3 POINTS	
		SCORE:		
	4) Program participants complete a Personal Development Plan (PDP) with the collaboration of both their supervisor and mentor and/or coach.	None	0	

3

CRITERIA CATEGORY	ELEMENTS	EVALUATION	SCORE	SELF ASSESSMENT
		Program participants complete a Personal Development Plan (PDP) with the collaboration of both their supervisor and mentor and/or coach	1	
		The PDP incorporates/includes assessment and/or feedback	2	
		Evidence of ongoing collaboration and implementation (review, updates)	3	
		SCORE:		
	5) At least one individual assessment tool is used.	None	0	
		At least one assessment tool.	3	
		SCORE:		
SELECTION PROCESS				
	1) Advertising strategy - How the organization publicizes and attracts candidates to the program	One method of communication (i.e., postmaster) is used to announce the program.	0 POINTS	
		Programs are widely announced thru a variety of mechanisms (i.e., postmaster, intranet, brochures, staff meetings)	1 POINT	

4

CRITERIA CATEGORY	ELEMENTS	EVALUATION	SCORE	SELF ASSESSMENT
		In addition to the announcement to solicit participants, information is available all year to establish continuous awareness of the program.	2 POINTS	
		In addition to multiple posting and announcements, leaders routinely encourage and develop employees to be successful candidates. There is also evidence of efforts to assure a diverse applicant pool (i.e., the special emphasis coordinators are actively involved in the recruitment for the program, career counseling centers are established that serve as feeders for the talent pool, career fairs are regularly held)	3 POINTS	
		SCORE:		
	2) Selection - The process by which applicants are selected	No Formal process	0 POINTS	
		Formal application process allows employees to self-nominate to the program with the endorsement of their supervisor. (see footnote)	1 POINT	
		The formal selection process includes a performance/ competence-based approach for screening applicants. The pool of selected participants represents the diversity and the succession needs of the organization.	2 POINTS	

5

CRITERIA CATEGORY	ELEMENTS	EVALUATION	SCORE	SELF ASSESSMENT
		The formal application and selection process includes the items above and provides individualized feedback to all non-selected protégée. The effectiveness of the selection process is continually assessed to assure that it produces successful program graduates. Uses all elements of the ECF process (vaww.med.gov/succession)	3 POINTS	
		SCORE:		
EVALUATION	1) Program has a formal evaluation process in place.	No evaluation process in place	0 POINTS	
		Level 1 – Reaction How well did the participants like the program? Examples of ways to assess: Evaluation sheets, interviews, or focus groups that measure participant's reactions to content relevancy and use, speaker quality, format, location, etc.	1 POINT	
		Level 2 – Learning What principles, facts and techniques were learned? What attitudes were changed? Examples of ways to assess: End-of-course mastery test, attitudinal assessments, projects, presentations, participant self-report. Level 3 – Behavior What changes in job behavior resulted from the program?	2 POINTS	

6

CRITERIA CATEGORY	ELEMENTS	EVALUATION	SCORE	SELF ASSESSMENT
		Examples of ways to assess: Observation of on-the-job performance, completion of action plans, work samples, interviews.		
		Level 4 – Results/Business Impact What were the tangible results of the program in terms of reduced cost, improved quality, improved quantity, timesaving, etc.? Examples of ways to assess: Control groups, pre-and-post training comparison of data, e.g., number of errors, waiting times, time to fill leadership vacancies. Level 5* - Return on Investment Did the program produce return-on-investment? Examples of ways to assess: Calculate the dollar value of benefits and compare with total cost of training. *Not in original model by Kirkpatrick	3 POINTS	
		SCORE:		
	2) Program has built in feedback loop (i.e., evaluation results fed into continuous - improvement)	No evidence of feedback	0 POINTS	
		Participants are asked to make recommendations for changes in the program	1 POINT	

7

CRITERIA CATEGORY	ELEMENTS	EVALUATION	SCORE	SELF ASSESSMENT
		Developers and faculty review and analyze evaluations data to make program improvements based on that data	2 POINTS	
		There is a comprehensive collaborative analysis of the LEAD program compared with best practices (VHA/Community) resulting in subsequent improvements	3 POINTS	
		SCORE:		
LEADERSHIP SUPPORT	1) Evidence of dedicated resources – staff time and dollars	No dedicated resources – (i.e., no assigned responsibilities, no staff assigned)	0 POINTS	
		Collateral staff provide casual support with no dedicated funding	1 POINT	
		Collateral staff support with dedicated funding	2 POINTS	
		Consistent/dedicated core staff responsible for the LEAD program. Dedicated funding for the program – the dollars spent as they were intended to be at the end of the year.	3 POINTS	
		SCORE:		
	2) Supervisors involved and supportive	No Support –	0 POINTS	
		Supervisors endorse participant application to the program	1 POINT	
		Evidence of supervisory support for their subordinates' participation in the program. (i.e., recommend people consistently and are in	2 POINTS	

8

CRITERIA CATEGORY	ELEMENTS	EVALUATION	SCORE	SELF ASSESSMENT
		involved in planning educational programs.		
		Supervisors demonstrate involvement and or support for the program and its participants. (i.e., reinforces training, PDP, continually suggest learning opportunities).	3 POINTS	
		SCORE:		
	3) Senior Leaders are involved in the program (ELC members - Triad/Quad	No evidence of Senior Leadership involvement	0 POINTS	
		Appropriate leaders serve as coaches and/or mentors for the LEAD programs and ensure there are sufficient mentors for the programs.	1 POINTS	
		Senior Leaders serve as coaches and/or mentors and faculty.	2 POINTS	
		Senior leaders are champions for these programs. They are actively involved in the development, implementation, and evaluation of the program.	3 POINTS	
		SCORE:		
Reward and Recognition	1) There is a defined procedure for recognizing and acknowledging all contributors to the LEAD program	Not present	0 POINTS	
		Participants are acknowledged by executive leadership that they were part of the program	1 POINT	

9

CRITERIA CATEGORY	ELEMENTS	EVALUATION	SCORE	SELF ASSESSMENT
		Participants, faculty, coaches/mentors colleagues, staff and supervisors are publicly acknowledged by leadership	2 POINTS	
		Entire organization celebrates and is recognized for merits, including LEAD outcomes.	3 POINTS	
		SCORE:		
		OVERALL SCORE:		

Footnote:
The ECF application is structured on VHA's HPDM eight core competencies and requires applicants to describe their experience in a performance-based interviewing (PBI) format. It also includes a history of educational and work experience. Applications require management endorsement and are rated and ranked by a diverse panel of VHA senior executives. All applicants receive timely feedback on their application including areas of improvement.

10

Comments from the Department of Commerce

THE DEPUTY SECRETARY OF COMMERCE
Washington, D.C. 20230

June 7, 2005

Ms. Eileen Larence
Director
Strategic Issues
U.S. Government Accountability Office
Washington, DC 20548

Dear Ms. Larence:

The U.S. Department of Commerce appreciates the opportunity to comment on the Government Accountability Office draft report entitled *Human Capital: Selected Agencies Have Opportunities to Enhance Existing Succession Planning and Management Efforts (GAO-05-585).*

I enclose the Department of Commerce's comments on this report.

Sincerely,

David A. Sampson
(Acting)

Enclosure

U.S. Department of Commerce
Comments on
Government Accountability Office Draft Report,
Human Capital: Selected Agencies Have Opportunities to Enhance Existing Succession Planning and Management Efforts (GAO-05-585)

The U.S. Department of Commerce thanks the Government Accountability Office for the opportunity to review the draft report, *Human Capital: Selected Agencies Have Opportunities to Enhance Existing Succession Planning and Management Efforts* (GAO-05-585). This report discusses an important issue of concern to the Census Bureau -- human capital management and in particular succession management.

GENERAL COMMENTS

Since 2000, the U.S. Census Bureau has carefully studied and improved its approaches to succession management. The report highlights some of the critical succession management practices the Census Bureau is employing. These, as well as other key practices, need to be seen within the broader context of the Census Bureau's succession management framework. Understanding this framework is important because it is the diversity and adaptability of approaches as a whole, rather than individual techniques, that have been the key to the Census Bureau's success in planning and meeting succession challenges.

The Census Bureau has created a matrix of broad succession planning practices that is used to structure succession management efforts, disseminate best practices across the organization, and provide a point of reference for gauging progress in succession management practices. The matrix consists of 13 categories: (1) setting strategic goals; (2) collecting and analyzing work force data; (3) assessing employees for management and leadership; (4) orienting new employees at junior, mid- and senior levels; (5) mentoring; (6) continuous career-long learning based on individual development plans; (7) rotational assignments; (8) stretch assignments; (9) formal and informal training (particularly in terms of technical and core competencies); (10) formal management and leadership development programs integrated with on-the-job training; (11) individual development plans and critical performance elements; (12) use of management flexibilities; and (13) knowledge management, including the use of transition positions to allow for overlapping periods of transition for critical retirements.

The Census Bureau refined its recruitment, development, training, and human capital management programs to support a strategic approach to succession management. These refinements included different approaches to meet the varied succession challenges relating to senior management, mathematical statisticians, information technology specialists, and other mission-critical job categories.

Succession management programs are critical for senior executives and other key staff who, as the federal civil service continues to age, are projected to retire in large numbers. The Census Bureau's strategy for succession, particularly for key staff, focuses on building a solid pool of candidates from which to select. This strategy also focuses on building external relationships and outreach to attract diverse and well-qualified

applicants. The Census Bureau recognizes the constraints placed on agencies and bureaus by not knowing when people will actually retire and the inability to preselect successors. The individuals themselves cannot commit to a certain retirement date very far in advance of actual retirement. Personal circumstances change and with them, retirement decisions. Unlike private sector positions, the merit system limits the designation of an "heir apparent" as a tool for making smoother leadership transitions.

For mathematical statisticians, the pool of highly qualified applicants in the marketplace is diminishing. The report mentions one tool used by the Census Bureau to address this issue, which is the mathematical statisticians recruiting team. The recruiting team is part of the Methodology and Standards Council which, in addition to recruiting, leads the management and development of critical technical and leadership talent for mathematical statisticians across the entire organization. The efforts of the Council in building recruiting relationships; attracting candidates; and then selecting, developing, and retaining leading professionals, are critical and could serve as a useful model for other bureaus or agencies facing similar challenges for highly technical professionals.

The field of information technology changes rapidly and affects the competencies and work methods that are needed. To meet this challenge, the Census Bureau uses a strategy of hiring and developing professionals and complementing the capabilities of that work force by acquiring specialized skills and expertise through contracts. Contracting is used in areas where it has been determined, after an assessment of internal resources and capabilities, to be more effective than developing in-house talent. On a much broader scale, the Census Bureau is making the most extensive use of contracting in its history for the 2010 Census. The Census Bureau is contracting for data capture and processing services, geographic systems and support, as well as support for field automation systems. Collectively, these are very large contracts that represent strategic decisions to 'buy' rather than 'build.'

SPECIFIC COMMENTS ON THE REPORT'S TEXT AND RECOMMENDATIONS

P. 15, para. 2 "According to an agency human capital official, …."

The Census Bureau's strategy for ensuring its mission-critical capabilities is an anticipatory one. As the report correctly states, it focuses on building infrastructure by recruiting and developing competencies.

The "delegation of line managers to fill vacancies" refers to the ability of managers to use a proven electronic hiring system that allows them to identify and request a unique blend of competencies for each vacancy. This approach allows the organization to continuously update the competencies it seeks and select staff for competencies that match emerging, as well as established, needs. Front-line managers are engaged in a continuing dialogue with senior managers and interdirectorate councils (e.g., Hiring Coordinators Group and Human Capital Management Council) to identify, plan for, and address skill and competency needs at all organizational levels. The line managers use the flexibility and precision of the hiring system (and the robust pool of applicants who

have been recruited) to address both their specific hiring needs, as well as select for competencies that are of increasing importance to the Census Bureau as a whole.

The report recommends that the Secretary of Commerce should ensure that the Director of the Census take three actions. The Census Bureau's comments on each of these recommendations follow.

Recommendation 1—"Strengthen the monitoring of its mission critical workforce by identifying mission critical workforce gaps, developing strategies to address gaps, evaluating progress toward closing gaps, and adjusting strategies accordingly."

The Census Bureau agrees that monitoring and assuring the necessary competencies of its mission-critical work force is essential and requires close and continuing attention. The Census Bureau has found that its existing approach to succession management is effective in meeting mission-critical requirements. The practices described in the general comments section above are designed to anticipate skill needs and ensure that those needs are met through diverse and flexible approaches. Contracting is also used strategically to meet mission-critical objectives. The Census Bureau has found that its present methods of assessing and ensuring appropriate levels of critical work force capabilities are more efficient and effective than attempting to categorize and quantify 'gaps' within mission-critical occupations.

Recommendation 2—"Seek appropriate opportunities to coordinate and share core succession training and development programs with other outside agencies to achieve economies of scale, limit duplication of efforts, benchmark with high-performing agencies, keep abreast of current practices, enhance efficiency, and increase the effectiveness of its programs."

The Census Bureau agrees with this recommendation. As described in the report, the Census Bureau takes advantage of opportunities to partner and participate in succession development programs with its parent organization, the Department of Commerce. The Census Bureau will continue to explore opportunities to join with other bureaus and agencies in designing and conducting cost-effective training and development programs.

Recommendation 3—"Evaluate core succession training and development programs to assess the extent to which programs contribute to enhancing organizational capacity. When deciding the appropriate analytical approach and level of evaluation, the Bureau should consider factors such as estimated costs of training efforts, size of training audience, and program visibility, among other things."

The Census Bureau agrees with this recommendation. While, as the report notes, the Census Bureau tracks training and development program participation rates, costs, and outcome measures, a more comprehensive approach to evaluations is being planned. The Census Bureau has aligned its Planning and Evaluation Branch, along with its Work Force Development Branch, under the direction of a single Assistant Division Chief in its Human Resources Division. The report's recommendation reinforces the importance of these organizations working closely together to increase the efficiency and effectiveness of the Census Bureau's training and development programs.

GAO Contact and Staff Acknowledgments

GAO Contact

Eileen Larence (202) 512-6806

Acknowledgments

In addition to the contact named above, Lisa Shames, Naved Qureshi, Peter Rumble, Jennifer Cooke, Erin Murello, and Elena Lipson made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

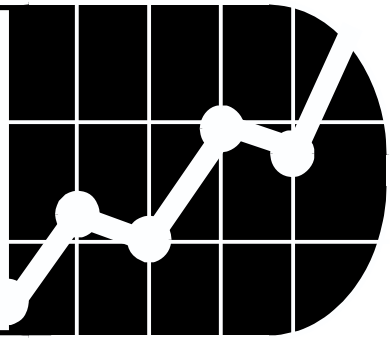
Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

Performance Management
Practitioner Series



Evaluating Performance Appraisal Programs:

An Overview

United States Office of Personnel Management

Workforce Compensation and Performance Service

Theodore Roosevelt Building
1900 E Street, NW.
Washington, DC
20415-8340

PMD-09
January 1999

This page intentionally left blank.

Evaluating Performance Appraisal Programs: An Overview

TABLE OF CONTENTS

CONCEPT

Assessing the value and effectiveness of an appraisal program is necessary for determining how to improve it. This guide suggests procedures and criteria for evaluating the implementation and effect of performance appraisal programs. It provides a brief summary of program evaluation and is a starting point for program evaluators.

Designing Evaluation Into the Program

Agencies are required to evaluate their performance appraisal system and program(s). Ideally, as appraisal program designers plan for the implementation of their program, they should also plan for its ongoing evaluation. The methods and questions used should be similar to the ones used in the design process when an initial assessment of the organization and its current appraisal program was done. (For example, if a survey of employees and managers was used to determine satisfaction levels with the current process, the same survey could be used for the new appraisal process to compare changes in satisfaction levels between the old and the new.) As program designers develop new appraisal programs, they should also develop the criteria they will use to determine whether the program is successful. They should plan to evaluate the program after the first appraisal period is completed. Ongoing program evaluation should be part of the program design and should be planned for, not only because it is required by regulation but to improve program effectiveness.

STRATEGY

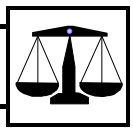
Appraisal programs can be evaluated from two broad perspectives:

- **Are we doing things right?** (i.e., are the process and the rules being followed?) and
- **Are we doing the right things?** (i.e., what effect does the program have?)

Compliance

By asking the first question, evaluators are attempting to determine if the organization is in compliance with regulatory, system, and program requirements. Examples of these types of questions include:

- Were appraisals done on time?
- Did everyone who was supposed to receive an appraisal get one?
- Were employee performance plans issued timely?
- Were progress reviews conducted?
- Does management devote appropriate resources and give priority to the effective maintenance and operation of the performance appraisal program?



As an initial step, compliance information is important to collect. If a program is not being run as it was designed to be run, it will have little chance of accomplishing the reasons for its implementation. But compliance information should not be the only program issue evaluated.

Effect

By asking the second question—Are we doing the right things?—evaluators attempt to determine the effect or the results of the appraisal program. The questions below represent possible criteria for determining the results of an appraisal program:

- **Are the stated objectives of the appraisal program being met?** If there are no stated objectives, do users have unwritten expectations and are those expectations being met? By focusing on program goals and objectives, evaluators can gather information specific to the goals and report results in terms of goal achievement. (Examples of stated program goals could include such things as improving organizational performance, encouraging teamwork, or improving communication about expectations between supervisors and employees.) If there are no stated goals in the program, determine the expectations of the designers, decision makers, and users of the program through surveys, interviews, and focus groups. Then base evaluation questions on those expectations. If there are no stated or unwritten goals for the program, at least the regulatory requirements of performance management (listed below) can be the basis for developing evaluation questions (see 5 CFR 430.102(b)):

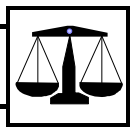
  (1) Communicate and clarify organizational goals to employees.
  Does the program provide for including or addressing organizational goals in employee performance plans?

  (2) Identify individual and, where applicable, team accountability for accomplishing organizational goals.
  Are employees held accountable through elements and standards that relate to organizational goals? Is team accountability addressed, where appropriate?

  (3) Identify and address developmental needs for individuals and, where applicable, teams.
  Are training needs and/or career development discussed?

  (4) Assess and improve individual, team, and organizational performance.
  Is appraisal used for improving individual and group performance — as it's supposed to be — or is it used to threaten and punish employees? Or is it used for some other reason?

  (5) Use appropriate measures of performance as the basis for recognizing and rewarding accomplishments.
  Are measures credible? Are awards based on valid and accepted criteria?



(6) Use the results of performance appraisal as a basis for appropriate personnel actions.

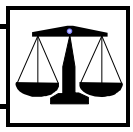
Are appraisal results used appropriately as a factor that is considered when making other personnel decisions (such as within-grade increase determinations, promotion decisions, etc.)?

- **Are employees and managers satisfied with the equity, utility, accuracy, etc., of the program?** The perceptions of managers and employees are important to the success and effectiveness of a program. Employees need to feel they get enough feedback on their performance and that their elements and standards are current and fair. Measures should be perceived as accurate and objective. On paper, the design of an appraisal program may appear to have all the right components. However, the perceptions of the users will be key to whether the program operates successfully.

- **Do the benefits of the program outweigh the costs?** Costs could include the cost of developing the program as well as the cost of using it. Examples of measurable costs are the costs of developing and using an automated appraisal process; the amount of time taken to develop employee performance plans; or the amount of time taken by raters, ratees, reviewers, and other users to appraise performance. But costs must be compared against the benefits. A method that costs little may also produce little, while a method that costs much in terms of development and usage time may provide significant benefits, such as improved performance, clarified expectations, or higher satisfaction rates.

- **Has there been an improvement in employee, unit, or organizational performance?** One of the purposes of performance management is to improve organizational effectiveness in the accomplishment of agency mission and goals. Because of the requirements of the Government Performance and Results Act of 1993, agencies are establishing strategic plans and measuring their performance against the goals they set for themselves in their plans. It may be difficult, however, if not impossible, to attribute the results of organizational performance to an employee appraisal program since an appraisal program is only one of many systems and processes that affect organizational outcomes. It is much easier to relate appraisal program effectiveness to improvements in employee and unit performance, but organizational performance should be considered.

- **Has the attitude or the behavior of employees and/or managers changed as desired?** Appraisal programs can be used as tools to support agency initiatives, such as focusing on results, improving customer service, and developing teamwork. These initiatives often require a change in organizational culture and employee attitudes to be successful. Determining that there have been desired attitude and behavior changes may be an indication that the appraisal program has had some effect. But again, it would be difficult to attribute attitude changes solely to the appraisal program.



- **Are there signs of different treatment in the results of performance appraisal processes?** Statistics on the distribution of performance ratings should be gathered and analyzed. Uneven ratings distributions might raise questions of fairness when compared by race, national origin, sex, and by occupational groups and grade. Performance-based adverse actions taken against certain groups of employees more often than others also should be analyzed. If different treatment is found, designers should attempt to determine if appraisal design features are causing the lack of balance in the ratings or if there is a larger problem in the organization that is surfacing through the appraisal process.

- **Has there been an improvement in the efficiency or the effectiveness of related human resources programs?** The law requires that the results of Federal performance appraisal, i.e., the appraisal of elements and rating of record, be used as a basis for training, rewarding, reassigning, promoting, reducing in grade, retaining, and removing employees. Evaluators may look at the relationships between performance appraisal and other human resource programs. For example, evaluators might want to determine:
  - if summary levels are used as a reference point in promotions or if ratings are so inflated that they are meaningless to the process;
  - if training needs are determined through the appraisal process or if supervisors and employees fail to talk about ways of improving performance during appraisal interviews; and/or
  - if supervisors receive support from the organization when a performance-based action is necessary, or if poor performance is tolerated.

CHECKLIST

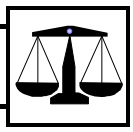
Once a list of possible topics and questions has been developed for evaluating the program, the following checklist can be used to help ensure that the right questions are being asked in the right way:

❑ Is it possible to gather information about the question? Don't bother including it if information can't be gathered.

❑ Is there only one possible answer to the question? The answer should not be predetermined or loaded by the phrasing of the question.

❑ Do decision makers feel they need the information? If no one will use the information, there is no reason to gather it.

❑ Do decision makers want the answer to the question for themselves? The results of evaluations are much more useful when people want the information.



- ❑ Can decision makers indicate how they would use the answer to the question? Knowing ahead of time how evaluation information will be used increases the chances that the evaluation results will not be filed away and never used.

A periodic, well-designed evaluation of the results of performance appraisal programs will provide the information managers and employees need to continually improve their appraisal processes. As program designers or evaluators design the evaluation tool, the underlying questions should be, What difference would it make to have this information? How would the information be used and how would it be useful?

BIBLIOGRAPHY

Part 430 of title 5, Code of Federal Regulations, "Performance Management."

Carroll, Stephen J. and Craig E. Schneier, *Performance Appraisal and Review Systems*. Glenview, IL: Scott, Foresman and Company, 1982.

Halachmi, Arie, "Evaluation Research: Purpose and Perspective," *Public Productivity Handbook*. New York: Marcel Dekker, Inc., 1992. Pages 213-225.

Mohrman, Jr., Allan M., Susan M. Resnick-West, and Edward E. Lawler III, *Designing Performance Appraisal Systems*. San Francisco: Jossey-Bass Publishers, 1989.

Patton, Michael Quinn, *Utilization-Focused Evaluation*. Beverly Hills: SAGE Publications, 1978.

Text Version

Source: OPM
Purpose: (b) (5)

Prepared By: Sean Newman
Reviewed By: Kimberly Perteet

A Handbook for Measuring Employee Performance

A Handbook for Measuring Employee Performance

ALIGNING EMPLOYEE

PERFORMANCE PLANS WITH

ORGANIZATIONAL GOALS

WORKFORCE COMPENSATION
AND PERFORMANCE SERVICE

Executive Resources and Employee Development ■ Performance Management Implementation ■ September 2011

contents

foreword

This handbook is designed for Federal supervisors and employees and presents an eight-step process for developing employee performance plans that are aligned with and support organizational goals. It also provides guidelines for writing performance elements and standards that not only meet regulatory requirements, but also maximize the capability that performance plans have for focusing employee efforts on achieving organizational and group goals.

The methods presented here are designed to develop elements and standards that measure employee and work unit accomplishments rather than to develop other measures that are often used in appraising performance, such as measuring behaviors or competencies. Although this handbook includes a discussion of the importance of balancing measures, the main focus presented here is to measure accomplishments. Consequently, much of the information presented in the first five steps of this eight-step process applies when supervisors and employees want to measure results. However, the material presented in Steps 6 through 8 about developing standards, monitoring performance, and checking the performance plan apply to all measurement approaches.

foreword

The handbook has four chapters and three appendices:

- **CHAPTER 1** gives the background and context of performance management that you will need to understand before beginning the eight-step process.
- **CHAPTER 2** defines **accomplishments,** which is key to using this handbook successfully.
- **CHAPTER 3** includes a detailed description of the **eight-step process** for developing employee performance plans that are aligned with and support organizational goals.
- **CHAPTER 4** provides **study tools**, including a followup **quiz** and a **quick reference** for the eight-step process.
- **THE APPENDICES** contain **example standards** that were written specifically for **appraisal programs** that appraise performance on elements at five, three, and two levels.

After reading the instructional material, studying the examples, and completing the exercises in this book, you should be able to:

- **DEVELOP** a performance plan that aligns individual performance with organizational goals
- **USE** a variety of methods to determine work unit and individual accomplishments
- **DETERMINE** the difference between activities and accomplishments
- **EXPLAIN** regulatory requirements for employee performance plans

chapter 1

chapter 1

PERFORMANCE MANAGEMENT: BACKGROUND AND CONTEXT

Remember the story about the naive student in his first English literature course who was worried because he didn't know what prose was? When he found out that prose was ordinary speech, he exclaimed, "Wow! I've been speaking prose all my life!"

Managing performance well is like speaking prose. Many managers have been "speaking" and practicing effective performance management naturally all their supervisory lives, but don't know it!

Some people mistakenly assume that performance management is concerned only with following regulatory requirements to appraise and rate performance. Actually, assigning ratings of record is only **one part** of the overall process (and perhaps the least important part).

Performance management is the systematic process of:

- **planning** work and setting expectations
- continually **monitoring** performance
- **developing** the capacity to perform
- periodically **rating** performance in a summary fashion
- **rewarding** good performance

The revisions made in 1995 to the governmentwide performance appraisal and awards regulations support "natural" performance management. Great care was taken to ensure that the requirements those regulations establish would complement and not conflict with the kinds of activities and actions effective managers are practicing as a matter of course.

PLANNING In an effective organization, work is planned out in advance. Planning means setting performance expectations and goals for groups and individuals to channel their efforts toward achieving organizational objectives. Getting employees involved in the planning process will help them understand the goals of the organization, what needs to be done, why it needs to be done, and how well it should be done.

The regulatory requirements for planning employees' performance include establishing the elements and standards of their performance appraisal plans. Performance elements and standards should be measurable, understandable, verifiable, equitable, and achievable. Through critical elements, employees are held accountable as individuals for work assignments or responsibilities. Employee performance plans should be flexible so that they can be adjusted for changing program objectives and work requirements. When used effectively, these plans can be beneficial working documents that are discussed often, and not merely paper work that is filed in a drawer and seen only when ratings of record are required.

MONITORING In an effective organization, assignments and projects are monitored continually. Monitoring well means consistently measuring performance and providing ongoing feedback to employees and work groups on their progress toward reaching their goals.

The regulatory requirements for monitoring performance include conducting progress reviews with employees where their performance is compared against their elements and standards. Ongoing monitoring provides the supervisor the opportunity to check how well employees are meeting predetermined standards and to make changes to unrealistic or problematic standards. By monitoring continually, supervisors can identify unacceptable performance at any time during the appraisal period and provide assistance to address such performance rather than wait until the end of the period when summary rating levels are assigned.

PERFORMANCE MANAGEMENT'S FIVE KEY COMPONENTS

DEVELOPING In an effective organization, employee developmental needs are evaluated and addressed. Developing in this instance means increasing the capacity to perform through training, giving assignments that introduce new skills or higher levels of responsibility, improving work processes, or other methods. Providing employees with training and developmental opportunities encourages good performance, strengthens job-related skills and competencies, and helps employees keep up with changes in the workplace, such as the introduction of new technology .

Carrying out the processes of performance management provides an excellent opportunity for supervisors and employees to identify developmental needs. While planning and monitoring work, deficiencies in performance become evident and should be addressed. Areas for improving good performance also stand out, and action can be taken to help successful employees improve even further.

RATING From time to time, organizations find it useful to summarize employee performance. This helps with comparing performance over time or across a set of employees. Organizations need to know who their best performers are.

Within the context of formal performance appraisal requirements, rating means evaluating employee or group performance against the elements and standards in an employee's performance plan and assigning a summary rating of record. The rating of record is assigned according to procedures included in the organization's appraisal program. It is based on work performed during an entire appraisal period. The rating of record has a bearing on various other personnel actions, such as granting within-grade pay increases and determining additional retention service credit in a reduction in force.

REWARDING In an effective organization, rewards are used often and well. Rewarding means recognizing employees, individually and as members of groups, for their performance and acknowledging their contributions to the agency's mission. A basic principle of effective management is that all behavior is controlled by its consequences. Those consequences can and should be both formal and informal and both positive and negative.

Good managers don't wait for their organization to solicit nominations for formal awards before recognizing good performance. Recognition is an ongoing, natural part of day-to-day experience. A lot of the actions that reward good performance, like saying "thank you," don't require a specific regulatory authority. Nonetheless, awards regulations provide a broad range of forms that more formal rewards can take, such as cash, time off, and many recognition items. The regulations also cover a variety of contributions that can be rewarded, from suggestions to group accomplishments.

PERFORMANCE MANAGEMENT AS PROSE

Good managers have been speaking and practicing effective performance management all their lives, executing each key component process well. They not only set goals and plan work routinely, but they also measure progress toward those goals and give feedback to employees. They set high standards, but they also take care to develop the skills needed to reach them. They also use formal and informal rewards to recognize the behavior and results that accomplish their mission. All five components working together and supporting each other achieve natural, effective performance management.

Employee Performance Plans

Employees must know what they need to do to perform their jobs successfully. Expectations for employee performance are established in employee performance plans. Employee performance plans are all of the written, or otherwise recorded, performance elements that set forth expected performance. A plan must include all critical and non-critical elements and their performance standards.

Performance elements tell employees **what** they have to do and standards tell them **how well** they have to do it. Developing elements and standards that are understandable, measurable, attainable, fair, and challenging is vital to the effectiveness of the performance appraisal process and is what this handbook is all about.

Federal regulations define three types of elements: critical elements, non-critical elements, and additional performance elements. Agency appraisal programs are required to use critical elements (although the agency may choose to call them something else), but the other two types can be used at the agency's option. Before continuing further with this handbook, you should contact your human resources office to determine the types of elements your appraisal program allows.

A NOTE ABOUT PERFORMANCE PLANS

This handbook is about developing employee performance plans. However, there is another type of performance plan that you need to be aware of. The Government Performance and Results Act of 1993 requires each agency to prepare an annual performance plan covering each program activity set forth in its budget. These organizational performance plans:

- ***establish program-level performance goals that are objective, quantifiable, and measurable***
- ***describe the operational resources needed to meet those goals***
- ***establish performance indicators to be used in measuring the outcomes of each program***

We will be using organizational performance plans during Step 1 of the eight-step process presented in this handbook. Organizational performance plans are key in the process of aligning employee performance with organizational goals.

A NOTE ABOUT GROUP OR TEAM PERFORMANCE

The term "group or team performance" can be confusing sometimes. When we say that critical elements cannot describe group performance, we are saying that the group's performance as a whole cannot be used as a critical element. This does not preclude describing an individual's contribution to the group as a critical element. The key to distinguishing between group performance and an individual's contribution to the group is that group performance is measured at an aggregate level, not for a single employee. An individual's contribution to the group is measured at the individual employee level.

CRITICAL ELEMENTS A critical element is an assignment or responsibility of such importance that unacceptable performance in that element would result in a determination that the employee's overall performance is unacceptable. Regulations require that each employee have at least one critical element in his or her performance plan. Even though no maximum number is placed on the number of critical elements possible, most experts in the field of performance management agree that between three and seven critical elements are appropriate for most work situations.

Critical elements are the cornerstone of individual accountability in employee performance management. Unacceptable performance is defined in Section 4301(3) of title 5, United States Code, as failure on one or more critical elements, which can result in the employee's reassignment, removal, or reduction in grade. Consequently, critical elements must describe work assignments and responsibilities that are within the employee's control. For most employees this means that critical elements **cannot** describe a group's performance. However, a supervisor or manager can and should be held accountable for seeing that results measured at the group or team level are achieved. Critical elements assessing group performance may be appropriate to include in the performance plan of a supervisor, manager, or team leader who can reasonably be expected to command the production and resources necessary to achieve the results (i.e., be held individually accountable).

NON-CRITICAL ELEMENTS A non-critical element is a dimension or aspect of individual, team, or organizational performance, exclusive of a critical element, that is used in assigning a summary level. Important aspects of non-critical elements include:

- **NO PERFORMANCE-BASED ACTIONS** Failure on a non-critical element **cannot** be used as the basis for a performance-based adverse action, such as a demotion or removal. Only critical elements may be used that way. Moreover, if an employee fails on a non-critical element, the employee's performance cannot be summarized as *Unacceptable* overall based on that failure.

- **GROUP PERFORMANCE** Non-critical elements are the only way an agency can include the group's or the team's performance as an element in the performance plan so that it counts in the summary level. For example, team structured organizations might use a non-critical element to plan, track, and appraise the team on achieving its goals. To do this, each team member's performance plan would include the "team" element (i.e., a non-critical element) and the rating for the team on that element would be counted in the summary level of each team member.

- **WHEN THEY CAN'T BE USED** Non-critical elements cannot be used in appraisal programs that use only two levels to summarize performance in the rating of record. This is because they would have no effect on the summary rating level and, by definition, they must affect the summary level. (That is, in a two-level program, failure on non-critical elements cannot bring the summary level down to *Unacceptable,* and assessments of non-critical elements cannot raise the summary level to *Fully Successful* if a critical element is failed.)

- **CAN GREATLY AFFECT THE SUMMARY LEVEL** Sometimes the word "non-critical" is interpreted to mean "not as important." Prior to 1995, this interpretation was prescribed by regulation. Now, however, depending on how an appraisal program is designed, this need not be the case. Even though consideration of non-critical elements cannot result in assigning an *Unacceptable* summary level, appraisal programs can be designed so that non-critical elements have as much weight or more weight than critical elements in determining summary levels above *Unacceptable*.

BEFORE YOU CAN USE NON-CRITICAL ELEMENTS IN EMPLOYEE PERFORMANCE PLANS, YOU MUST DETERMINE IF YOUR APPRAISAL PROGRAM ALLOWS THEM.

ADDITIONAL PERFORMANCE ELEMENTS

An additional performance element is a dimension or aspect of individual, team, or organizational performance that is not a critical element and is not used in assigning a summary rating level. The essential difference between a non-critical element and an additional performance element is that non-critical elements **do** affect the summary level. Otherwise, the features and limitations of non-critical elements discussed above also apply to additional performance elements. Opportunities for using additional performance elements include:

CHECK THE RULES OF YOUR PROGRAM BEFORE INCLUDING ADDITIONAL PERFORMANCE ELEMENTS IN YOUR PLANS.

- **NEW WORK ASSIGNMENT** Managers and employees may want to establish goals, track and measure performance, and develop skills for an aspect of work that they do not believe should count in the summary level. For example, if an employee volunteered to work on a new project that requires new skills, an additional performance element describing the new assignment provides a non-threatening vehicle for planning, measuring, and giving feedback on the employee's performance without counting it in the summary level.
- **GROUP PERFORMANCE** In a two-level appraisal program, additional performance elements are the only way to include a discussion of group performance in the appraisal process. Even though the element assessment does not count when determining the summary level, managers and employees could use it to manage the group's performance.
- **AWARDS** Additional performance elements can be used to establish criteria for determining awards eligibility, especially in a two-level program that no longer bases awards solely on a summary level.

ELEMENT CHARACTERISTICS

	REQUIRED IN EMPLOYEE PERFORMANCE PLANS	CREDITED IN THE SUMMARY LEVEL	CAN DESCRIBE A GROUP'S PERFORMANCE
CRITICAL ELEMENTS	YES	YES	NO*
NON-CRITICAL ELEMENTS	NO	YES	YES
ADDITIONAL PERFORMANCE ELEMENTS	NO	NO	YES

*Except when written for a supervisor or manager who has individual management control over a group's production and resources.

Additional performance elements were introduced in the September 1995 performance appraisal regulations and have not been used widely yet. We foresee their popularity rising as agencies discover the possibilities they present for managing performance.

KNOW YOUR PROGRAM FEATURES

Again, it is important to stress that before you continue with this handbook, you need to find out the rules established by your appraisal program; specifically , you will need to know:

- which kinds of elements your program allows you to use
- at how many levels your program appraises employee performance on elements
- how many summary levels your program uses
- if your program allows weighting of elements (see Step 4)
- whether the program requires specific elements and/or uses generic standards

example program features

This handbook uses an example agency called the "Federal Benefits Bureau," (FBB) which is an agency that specializes in benefits and retirement services. To be able to understand and work through the examples, you need to know the features of FBB's appraisal program (i.e., the same features listed above).
FBB's appraisal program:

- uses critical, non-critical, and additional performance elements
- appraises employee performance on elements at five levels:

  Unacceptable
  Minimally Successful
  Fully Successful
  Exceeds Fully Successful
  Outstanding
- uses five summary levels, which are the same as the elements' five levels listed above
- allows elements to be weighted according to importance to the organization
- requires **no** specific or generic elements

chapter 2

DISTINGUISHING ACTIVITIES FROM ACCOMPLISHMENTS

CHAPTER 2 DISCUSSES WHAT MAY BE THE MOST IMPORTANT CONCEPT IN THIS HANDBOOK: THE DIFFERENCE BETWEEN MEASURING ACTIVITIES AND MEASURING ACCOMPLISHMENTS. THE FOLLOWING STORY ILLUSTRATES THIS CONCEPT.

The Beekeepers and Their Bees

Once upon a time, there were two beekeepers who each had a beehive. The beekeepers worked for a company called Bees, Inc. The company's customers loved its honey and wanted the business to produce more honey than it had the previous year. As a result, each beekeeper was told to produce more honey at the same quality. With different ideas about how to do this, the beekeepers designed different approaches to improve the performance of their hives.

The first beekeeper established a bee performance management approach that measured how many flowers each bee visited. At considerable cost to the beekeeper, an extensive measurement system was created to count the flowers each bee visited. The beekeeper provided feedback to each bee at midseason on his individual performance, but the bees were never told about the hive's goal to produce more honey so that Bees, Inc., could increase honey sales. The beekeeper created special awards for the bees who visited the most flowers.

The second beekeeper also established a bee performance management approach, but this approach communicated to each bee the goal of the hive—to produce more honey. This beekeeper and his bees measured two aspects of their performance: the amount of nectar each bee brought back to the hive and the amount of honey the hive produced. The performance of each bee and the hive's overall performance were charted and posted on the hive's bulletin board for all bees to see. The beekeeper created a few awards for the bees that gathered the most nectar, but he also established a hive incentive program that rewarded each bee in the hive based on the hive's production of honey—the more honey produced the more recognition each bee would receive.

chapter 2

At the end of the season, the beekeepers evaluated their approaches. The first beekeeper found that his hive had indeed increased the number of flowers visited, but the amount of honey produced by the hive had dropped. The Queen Bee reported that because the bees were so busy trying to visit as many flowers as possible, they limited the amount of nectar they would carry so they could fly faster. Also, because the bees felt they were competing against each other for awards (because only the top performers were recognized), they would not share valuable information with each other (like the location of the flower-filled fields they'd spotted on the way back to the hive) that could have helped improve the performance of all the bees. (After all was said and done, one of the high-performing bees told the beekeeper that if he'd been told that the real goal was to make more honey rather than to visit more flowers, he would have done his work completely differently.) As the beekeeper handed out the awards to individual bees, unhappy buzzing was heard in the background.

The second beekeeper, however, had very different results. Because each bee in his hive was focused on the hive's goal of producing more honey, the bees had concentrated their efforts on gathering more nectar to produce more honey than ever before. The bees worked together to determine the highest nectar-yielding flowers and to create quicker processes for depositing the nectar they'd gathered. They also worked together to help increase the amount of nectar gathered by the poor performers. The Queen Bee of this hive reported that the poor performers either improved their performance or transferred to another hive. Because the hive had reached its goal, the beekeeper awarded each bee his portion of the hive incentive payment. The beekeeper was also surprised to hear a loud, happy buzz and a jubilant flapping of wings as he rewarded the individual high-performing bees with special recognition.

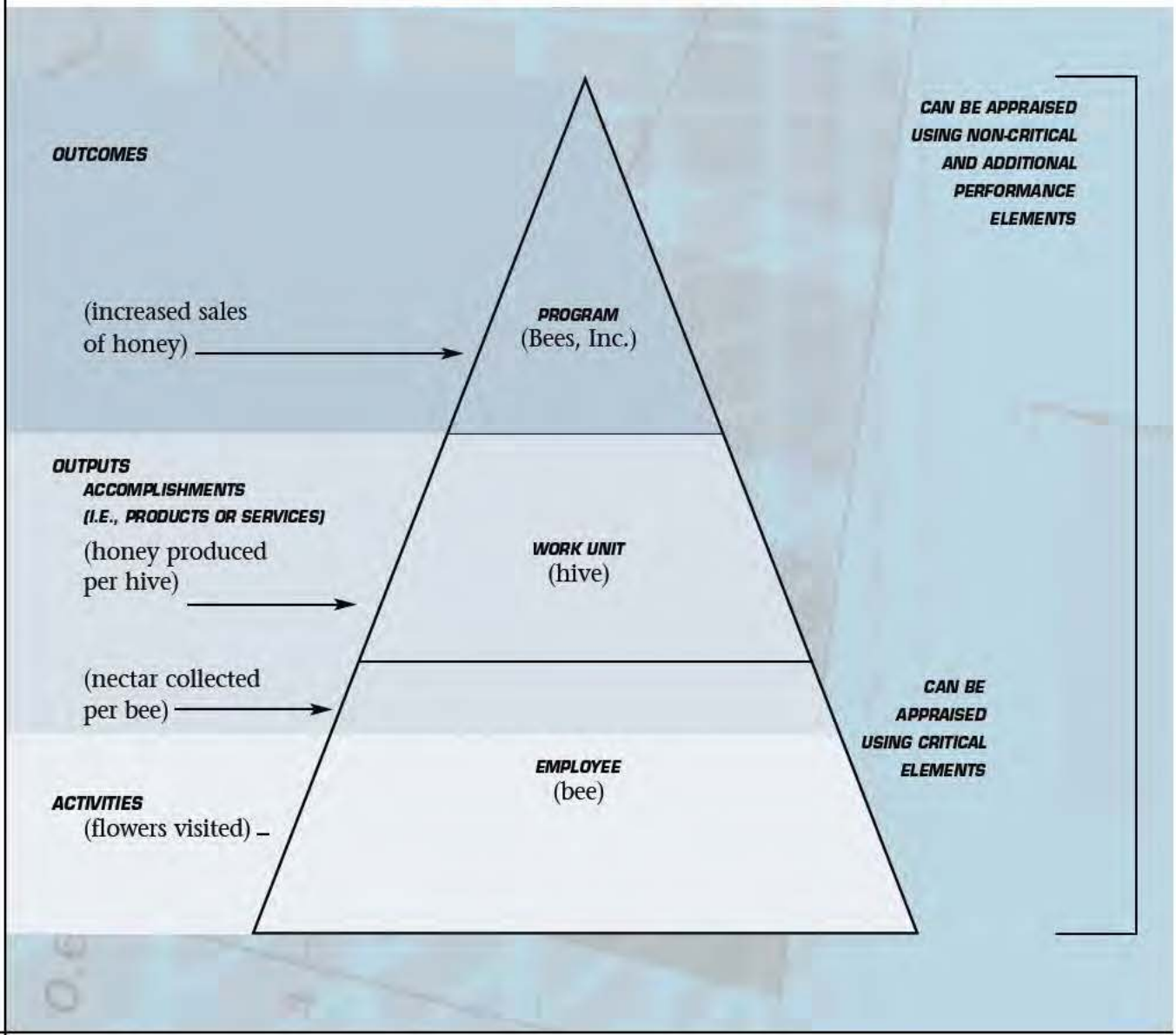
THE MORAL OF THIS STORY IS: MEASURING AND RECOGNIZING ACCOMPLISHMENTS RATHER THAN ACTIVITIES—AND GIVING FEEDBACK TO THE WORKER BEES—OFTEN IMPROVES THE RESULTS OF THE HIVE.

Although it somewhat oversimplifies performance management, the beekeepers' story illustrates the importance of measuring and recognizing accomplishments (the amount of honey production per hive) rather than activities (visiting flowers). This handbook is designed to help you develop elements and standards that center around accomplishments, not activities.

The chart below depicts the type of measurement that should occur at each organizational level of Bees, Inc., and includes measurements used by the beekeepers.

PERFORMANCE PYRAMID

Note that outputs occur at two levels—the work unit and the employee level.



Activities are the actions taken to produce results and are generally described using verbs. In the beekeeper story, the *activity* being measured was *visiting* flowers. Other examples of activities include:

- *filing* documents
- *developing* software programs
- *answering* customer questions
- *writing* reports

Accomplishments (or outputs) are the products or services (the results) of employee and work unit activities and are generally described using nouns. The examples of *outputs* used in the story include the amount of *nectar* each bee collected and the *honey* production for the hive. Other examples include:

- *files* that are orderly and complete
- a software *program* that works
- accurate *guidance* to customers
- a *report* that is complete and accurate

Outcomes are the final results of an agency's products and services (and other outside factors that may affect performance). The example of an outcome used in the beekeeper story was increased sales of honey for Bees, Inc. Other examples of outcomes could include:

- reduced number of transportation-related deaths
- improved fish hatcheries
- a decrease in the rate of teenage alcoholism
- clean air

A NOTE ABOUT FEDERAL EFFORTS TO MEASURE OUTCOMES AND OUTPUTS

Because of the requirements set by the Government Performance and Results Act of 1993 (i.e., the Results Act), Federal agencies are measuring their organizational outcomes and outputs. The Results Act requires agencies to have strategic plans, which include outcome-related goals and objectives for the major functions and operations of the agency. Those outcome goals must be objective, quantifiable, and measurable. The Results Act also requires agencies to develop annual performance plans that cover each one of their programs. Performance plans must include performance goals, which define the annual, often incremental, progress in achieving the outcome goals in the strategic plan. Performance goals are often output-oriented because they address single-year performance. We will talk more about strategic plans with their outcome goals, and performance plans with their output goals, in Chapter 3.

On the performance pyramid illustrated on page 14, notice that accomplishments can be measured at two levels in the organization—the employee level and the work unit level. Employee accomplishments can be included in employee performance plans using all three types of performance elements. Work unit accomplishments also can be included in the appraisal process—through non-critical elements if the agency desires to have work unit performance affect ratings (and only if the appraisal program uses more than two summary levels) or through additional performance elements if work unit performance is not to affect ratings. However they are used in performance appraisal, work unit as well as employee accomplishments can always be recognized through an awards program.

If supervisors, team leaders, and employees want to develop performance plans that support the achievement of organizational outcomes, they might try the second beekeeper's approach of sharing organizational goals with the hive, measuring and rewarding accomplishments rather than activities, and providing feedback on performance.

Using Balanced Measures

THIS HANDBOOK FOCUSES ON MEASURING ACCOMPLISHMENTS AT THE WORK UNIT AND EMPLOYEE LEVELS. THERE MAY BE SITUATIONS, HOWEVER, WHEN ACTIVITIES, BEHAVIORS, OR PROCESSES MAY BE IMPORTANT TO INCLUDE IN AN EMPLOYEE'S PERFORMANCE PLAN. THIS HANDBOOK DOES NOT FOCUS ON HOW TO DEVELOP THOSE KINDS OF MEASURES. HOWEVER, WE WOULD BE REMISS NOT TO INCLUDE A DISCUSSION ABOUT THE IMPORTANCE OF BALANCING MEASURES IN YOUR MEASUREMENT SYSTEM. THEREFORE, A SHORT DESCRIPTION OF BALANCED MEASURES FOLLOWS.

Traditionally, many agencies have measured their organizational performance by focusing on internal or process performance, looking at factors such as the number of full-time equivalents (FTEs) allotted, the number of programs controlled by the agency, or the size of the budget for the fiscal year. In contrast, private sector businesses usually focus on the financial measures of their bottom line: return-on-investment, market share, and earnings-per-share. Alone, neither of these approaches provides the full perspective on an organization's performance that a manager needs to manage effectively. But by balancing customer and employee satisfaction measures with results and financial measures, managers will have a more complete picture and will know where to make improvements.

BALANCING MEASURES Robert S. Kaplan and David P. Norton have developed a set of measures that they refer to as "a balanced scorecard." These measures give top managers a fast but comprehensive view of the organization's performance and include both process and results measures. Kaplan and Norton compare the balanced scorecard to the dials and indicators in an airplane cockpit. For the complex task of flying an airplane, pilots need detailed information about fuel, air speed, altitude, bearing, and other indicators that summarize the current and predicted environment. Reliance on one instrument can be fatal. Similarly, the complexity of managing an organization requires that managers be able to view performance in several areas simultaneously. A balanced scorecard—or a balanced set of measures—provides that valuable information.

MANAGING PERFORMANCE FROM THREE PERSPECTIVES A variety of studies have shown that both the public and private sectors have used balanced measures to help create high-performing organizations. Because balancing the perspectives of business, customers, and employees plays a key role in organizational success, OPM regulations (effective November 13, 2000) now require agencies to evaluate senior executive performance using balanced measures, which should take into account the following factors:

- **The business perspective,** which has a different interpretation in the Government than in the private sector. For many organizations, there are actually two separate sets of measures: the outcomes, or social/political impacts, which define the role of the agency/department within the Government and American society; and the business processes needed for organizational efficiency and effectiveness. Many of the outcome-oriented goals agencies establish in their strategic plans under the Government Performance and Results Act include the business perspective. To gain the business perspective, Federal managers must answer the question: *How do we look to Congress, the President, and other stakeholders?*

- **The customer perspective,** which considers the organization's performance through the eyes of its customers, i.e., American citizens, so that the organization retains a careful focus on customer needs and satisfaction. To achieve the best in business performance, agencies must incorporate customer needs and wants and must respond to them as part of their performance planning. Federal managers must answer the question: *How do customers see us?*
- **The employee perspective,** which focuses attention on the performance of the key internal processes that drive the organization, including employee development and retention. This perspective directs attention to the basis of all future success—the organization's people and infrastructure. Adequate investment in these areas is critical to all long-term success. Federal managers must answer the question: *Do employees view the organization as a good place to work and develop their skills?*

TIE-IN TO EMPLOYEE PERFORMANCE The balanced measures philosophy need not apply only at the organizational or senior executive level. A balanced approach to employee performance appraisal is an effective way of getting a complete look at an employee's work performance. Too often, employee performance plans with their elements and standards measure behaviors, actions, or processes without also measuring the results of employees' work. By measuring only behaviors or actions in employee performance plans, an organization might find that most of its employees are appraised as *Outstanding* when the organization as a whole has failed to meet its objectives.

By using balanced measures at the organizational level, and by sharing the results with supervisors, teams, and employees, managers are providing the information needed to align employee performance plans with organizational goals. By balancing the measures used in employee performance plans, the performance picture becomes complete.

Categories of Work

Sometimes performance plans describe elements using categories of work. Categories are classifications of work types often used to organize performance elements and standards. If, for example, the first beekeeper in our fable had used categories of work for his elements, he might have used the broad category of "making honey" as the element and then included a grouping that described all the activities the bees did to make the honey , such as gather nectar, report to the drones, etc. Other examples of categories of work and the types of activities that are often described under these categories include:

- customer service (greets customers with a smile, answers the phone promptly)
- teamwork (cooperates with others, shares information)
- communication (writes well, gives presentations)
- office duties (files papers, prepares reports)

THIS HANDBOOK DOES NOT EXPLAIN HOW TO DESCRIBE AND MEASURE CATEGORIES OF WORK. HERE YOU ARE ASKED TO CONCENTRATE ON MEASURING ACCOMPLISHMENTS.

EXERCISE ON DISTINGUISHING ACTIVITIES FROM ACCOMPLISHMENTS:

It is time to check your understanding of the differences among activities, accomplishments, and categories. Please check the column that best describes each item.

	ACCOMPLISHMENT	ACTIVITY	CATEGORY
Trains employees			
Supervision			
A completed case			
Public relations			
Recommendations			
Customer service			
HR policy interpretations			
Writes agency policy			
Solutions to problems			
Develops software programs			
Ideas and innovations			
Files paperwork			
Writes memos			
Computer systems that work			
Teamwork			
A completed project			
Satisfied customers			
Answers the phone			
Assists team members			

ANSWERS ON PAGE 88

chapter 3

DEVELOPING EMPLOYEE PERFORMANCE PLANS

You are now going to begin an eight-step process for developing employee performance plans that support organizational goals. Before you begin, however, we want to briefly review a process for developing performance plans that you may have followed in the past but will **NOT** be learning here.

Traditionally in some organizations, performance plans have been developed by copying the activities described in an employee's job description onto the appraisal form. This handbook asks that you **NOT** begin with the position description. Even though a performance plan must reflect the type of work described in the employee's position description, the performance plan does not have to mirror it.

The next two pages illustrate what happens when you develop a performance plan solely from a position description. Page 22 is a simplified position description for a Retirement Benefits Specialist within the Claims Division branch of our example agency — the Federal Benefits Bureau (FBB). Notice how the duties and responsibilities in the position description all begin with a verb. They describe **activities**, not **accomplishments**.

chapter 3

A performance plan for a Retirement Benefits Specialist follows on page 23. It was written by copying the simplified position description from page 22 onto the appraisal form. Note that by copying the activities from the position description onto the appraisal form, FBB has developed a performance plan that only measures **activities,** not accomplishments. Also, by developing a performance plan without using a process that links **accomplishments** to organizational goals, the organization has lost the opportunity to use the appraisal process to communicate its goals to its employees and to align employee efforts with its goals.

REMEMBER THAT FBB'S APPRAISAL PROGRAM APPRAISES EMPLOYEE PERFORMANCE ON ELEMENTS AT FIVE LEVELS. THE FORM ON PAGE 23 SHOWS FIVE POSSIBLE LEVELS OF PERFORMANCE: UNSATISFACTORY (U), MINIMALLY SUCCESSFUL (MS), FULLY SUCCESSFUL (FS), EXCEEDS FULLY SUCCESSFUL (EFS), AND OUTSTANDING (O).

POSITION DESCRIPTION

THE DUTIES AND RESPONSIBILITIES IN THE POSITION DESCRIPTION ALL BEGIN WITH A VERB. THEY DESCRIBE ACTIVITIES.

POSITION DESCRIPTION: #123456
ORGANIZATIONAL TITLE: RETIREMENT BENEFITS SPECIALIST

INTRODUCTION

The incumbent of this position serves in a highly responsible capacity as a Retirement Benefits Specialist in an office responsible for the adjudication of claims for retirement and insurance benefits.
The work requires the services of an experienced, fully-trained Retirement Benefits Specialist. This position is responsible for considering and acting on all aspects of claims and applications for retirement and insurance benefits in an assigned area.

MAJOR DUTIES AND RESPONSIBILITIES

- Determine entitlement to and the amount of retirement annuities and survivor benefits, as well as payments to adult students and the entitlements and payments to certain other parties such as former spouses.
- Develop the record in individual cases, determining what is necessary and the sources of needed information.
- Adjudicate cases.
- Review and approve recommendations and decisions made by other Specialists, and provide training, advice, and assistance.
- Respond to inquiries from various customer sources and provide clear, responsive explanations of actions taken and the bases for them.

APPROVING AUTHORITY SIGNATURE	*DATE*

PERFORMANCE PLAN

☒ ***THIS IS NOT THE TYPE OF PERFORMANCE PLAN THAT YOU WILL DEVELOP IF YOU FOLLOW THE METHOD PRESENTED IN THIS HANDBOOK.***

EMPLOYEE PERFORMANCE PLAN

Name	**Effective Date**

JOB TITLE	*NAME OF OFFICE*
Retirement Benefits Specialist	Office of Retirement Services

ELEMENTS	***TYPE***	***STANDARDS***	***RATING***
TECHNICAL AND POLICY EXPERT ❙ Determine entitlement to and the amount of retirement annuities and survivor benefits, as well as payments to adult students and the entitlements and payments to certain other parties such as former spouses. ❙ Develop the record in individual cases, determining what is necessary and the sources of needed information. ❙ Adjudicate cases of unusual technical difficulty.	Critical	*FULLY SUCCESSFUL:* Amounts of payments are accurate and determine timely. Amounts of paym curate and det ely.	☐ MS ☐ FS ☐ EFS ☐ O
LEADERSHIP ❙ Review and approve recommendations and decisions made by other Specialists, and provide advice and assistance.	Crit	*FULLY SUCCESSFUL* Reviews cases as r Provides high-quality back and advice to othe	☐ U ☐ MS ☐ FS ☐ EFS ☐ O
CUSTOMER SERVICE ❙ Respond to inquiries from various customer sources and provide clear, responsive explanations of actions taken and the bases for them.	Critical	*FULLY SUCCESSFUL:* Customer inquiries are routinely addressed accurately and in a timely fashion.	☐ U ☐ MS ☐ FS ☐ EFS ☐ O

COMMENTS:

APPRAISING OFFICIAL SIGNATURE	*EMPLOYEE SIGNATURE*

HAVING REVIEWED HOW TO DEVELOP A PERFORMANCE PLAN THAT FOCUSES ONLY ON ACTIVITIES, WE WILL NOW DEVELOP A PERFORMANCE PLAN THAT ESTABLISHES ELEMENTS AND STANDARDS, ADDRESSING ACCOMPLISHMENTS THAT LEAD TO ORGANIZATIONAL GOAL ACHIEVEMENT. ***AN EIGHT-STEP PROCESS HAS BEEN DEVELOPED TO PRODUCE SUCH PLANS.*** *EACH STEP IN THE EIGHT-STEP PROCESS WE PRESENT IN THIS HANDBOOK BUILDS ON THE PREVIOUS STEP; YOU CANNOT SKIP A STEP AND END UP WITH GOOD RESULTS.*

step 1: look at the overall picture

DEVELOPING EMPLOYEE PERFORMANCE PLANS

Instead of beginning at the bottom of the organization with the position description to develop employee performance plans, begin the process by looking at your agency' s goals and objectives. Gather the following information:

WHAT ARE YOUR AGENCY'S GENERAL OUTCOME GOALS AS OUTLINED IN ITS STRATEGIC PLAN?

The Government Performance and Results Act of 1993 (i.e., GPRA) requires all agencies to develop a strategic plan that includes objective, quantifiable, and measurable performance goals. Agencies submitted their first strategic plans to Congress in September 1997. You will be referring to your agency's strategic plan while creating employee performance plans.

WHAT ARE THE SPECIFIC PERFORMANCE GOALS ESTABLISHED FOR YOUR PROGRAM AREA AS OUTLINED IN YOUR AGENCY'S ANNUAL PERFORMANCE PLAN?

GPRA also requires each agency to have an annual performance plan that sets out measurable goals that define what will be accomplished during a fiscal year. The goals in the annual performance plan describe the incremental progress toward achieving the general goals and objectives in the strategic plan. Performance plan goals are usually more specific and may be more output-oriented than the general outcome goals found in the strategic plan. Since performance plan goals should be used by managers as they direct and oversee how a program is carried out, these are the goals to which employee performance plans should be linked.

WHAT PERFORMANCE MEASURES ARE ALREADY IN PLACE?

You should be aware of the measurement systems that you can access for information on performance, including measures used for determining progress toward achieving Results Act goals and customer satisfaction surveys.

EXAMPLE OF ORGANIZATIONAL GOALS

Again, this handbook will continually refer to the Retirement Benefits Specialist position located within the Retirement Claims Division (a division of the Office of Retirement Services) of our example agency - the Federal Benefits Bureau (FBB). One of the primary functions of this position is to process retirement claims. FBB's strategic, outcome-oriented goals and two of the Office of Retirement Service's performance goals established in FBB's annual performance plan serve as examples of organizational goals. You will use this information in the next step of our eight-step process.

example organizational goals

)%% V STRATEGIC GOALS

Provide. Offer a wide range of benefits and retirement services that will enhance recipients' quality of life.

Diversity. Create and maintain an inclusive work environment that values diversity and allows every employee the opportunity to reach their highest potential.

Serve. FBB's customer service, benefits, and retirement services meet the evolving needs of Federal employees and their families.

Integrity. Act as model agency within the Federal Government through fiscally responsible business practices and a commitment to excellence.

example organizational goals

FBB'S ANNUAL PERFORMANCE PLAN GOALS FOR THE OFFICE OF RETIREMENT SERVICES (ORS)

ORS GOAL #2

Retirement claims processing times are reduced and more customer services are delivered through self-servicing technology, while customer satisfaction is maintained at last fiscal year's level.

DIRECTLY LINKED TO FBB'S THIRD GOAL: SERVE

MEANS: *(ONLY TWO MEANS ARE PRESENTED HERE.)*

- We will use the ORS Calculator implemented through the automation improvement project to reduce the time needed to process claims.
- We will continue the availability of both Interactive Voice Response and Internet technology to make annuity payment account changes.

CUSTOMER SATISFACTION INDICATORS

- Customers who received their first payment either before or when they expected. (The goal is to reach 80 per cent.)
- Annuitants who indicate overall satisfaction with the handling of their retirement claims. (The goal is to reach 95 per cent.)

BUSINESS PROCESS INDICATORS

- Interim payment processing time. (The goal is 4.5 days.)
- Annuity processing time. (The goal is 90 days.)
- Annuity claims accuracy. (The goal is 92 per cent.)

FINANCIAL INDICATOR

Claims processing unit cost. (The goal is $190 per claim.)

step 2: determine work unit accomplishments

The next step in this eight-step method is to determine the accomplishments (i.e., the products or services) of the work unit. Identifying work unit accomplishments lets you identify appropriate measures in the following steps of this process.

A work unit is a small group of employees that, in a traditional work structure, is supervised by the same first-line supervisor. Work units are generally the smallest organizational group on the organizational chart and usually include between 5 and 20 people. A work unit can also be a team—permanent or temporary—where the team members work interdependently toward a common goal.

Because not all types of work situations and structures are the same, this handbook offers three different ways to determine what to measure at the work unit level:

A. A GOAL CASCADING METHOD

B. A CUSTOMER-FOCUSED METHOD

C. A WORK FLOW CHARTING METHOD

You can use one or all three methods, depending on what fits your situation. Whichever you use, remember to describe accomplishments (using nouns) rather than activities (using verbs).

method A: cascade the agency's goals down to the work unit level

The **goal cascading method** works best for agencies with clear organizational goals and objectives, such as those established in the strategic plans and annual performance plans that agencies have prepared under the Government Performance and Results Act. This method requires answers to each of the following questions:

WHAT ARE THE AGENCY'S SPECIFIC GOALS AND OBJECTIVES?

These can be found in the agency's annual performance plan and customer service standards. (Note that this question repeats Step 1 of the eight-step process.)

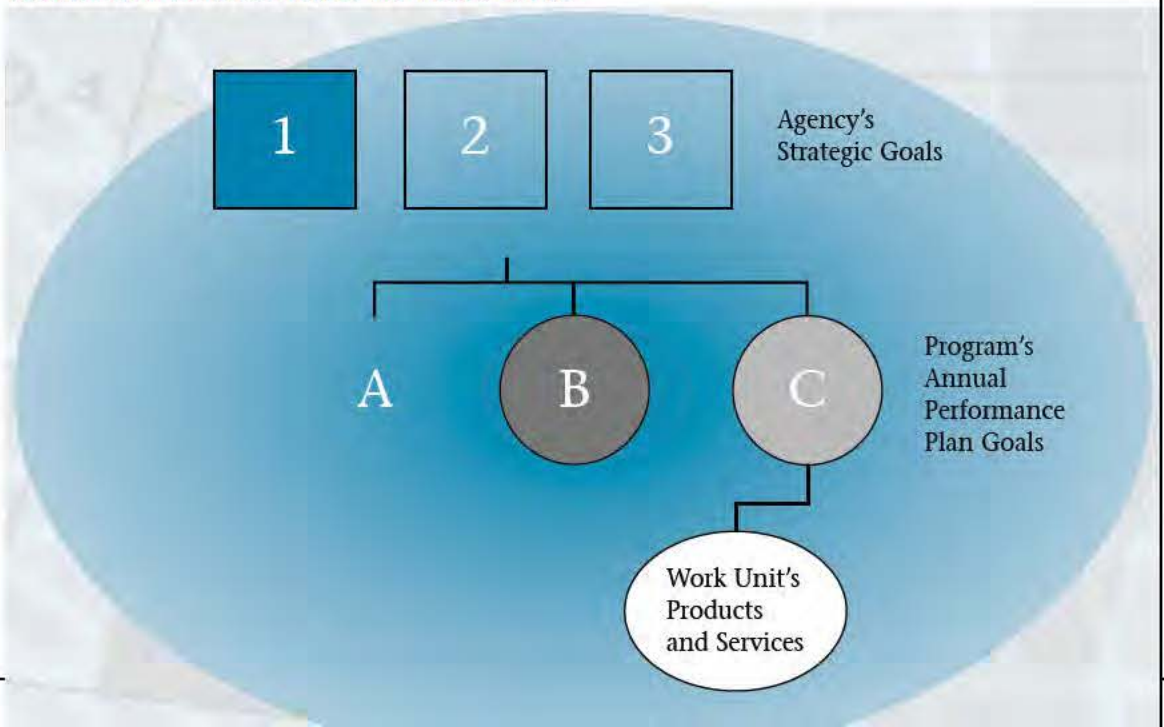
WHICH AGENCY GOAL(S) CAN THE WORK UNIT AFFECT?

Often, work units may affect only one agency goal, but in some situations, agency goals are written so broadly that work units may affect more than one.

WHAT PRODUCT OR SERVICE DOES THE WORK UNIT PRODUCE OR PROVIDE TO HELP THE AGENCY REACH ITS GOALS?

Clearly tying work unit products and services to organizational goals is key to this process. If a work unit finds it generates a product or service that does not affect organizational goals, the work unit needs to analyze the situation. It may decide to eliminate the product or service.

CASCADING AGENCY GOALS TO WORK UNITS



example method A

EXAMPLE OF CASCADING AGENCY GOALS TO A WORK UNIT

FBBStrategic Goal

FBB's THIRD GOAL: SERVE

FBB's customer service, benefits, and retirement services meet the evolving needs of Federal employees and their families.

An Office of Retirement Services (ORS) annual performance plan goal that cascades from FBB's THIRD GOAL: SERVE

ORS GOAL #2

Retirement claims processing times are reduced and more customer services are delivered through self-servicing technology, while customer satisfaction is maintained at last fiscal year's levels.

Some of Office of Retirement Services(ORS) GOALS

A. Reduce overall processing times for annuity claims by processing fully developed annuity claims in an average of 90 days (re ORS Goal #2).

B. Reduce claims processing error rates by providing increased training in workplace competencies (re ORS Goal #2).

Retirement Claims Division GOALS FBB

- Claims processed in less time and with lower error rates.
- Increased number of individuals who can process insurance claims.

EXERCISE ON CASCADING GOALS

In the spaces below, begin mapping your agency's strategic and performance goals and how those goals cascade or "trickle down" through your organization. Try to show how your work unit's products or services link to your agency's goals. Remember to describe work unit accomplishments in terms of products or services (i.e., the end result of all the unit's activities).

YOUR AGENCY'S GOALS

YOUR ORGANIZATION'S GOALS

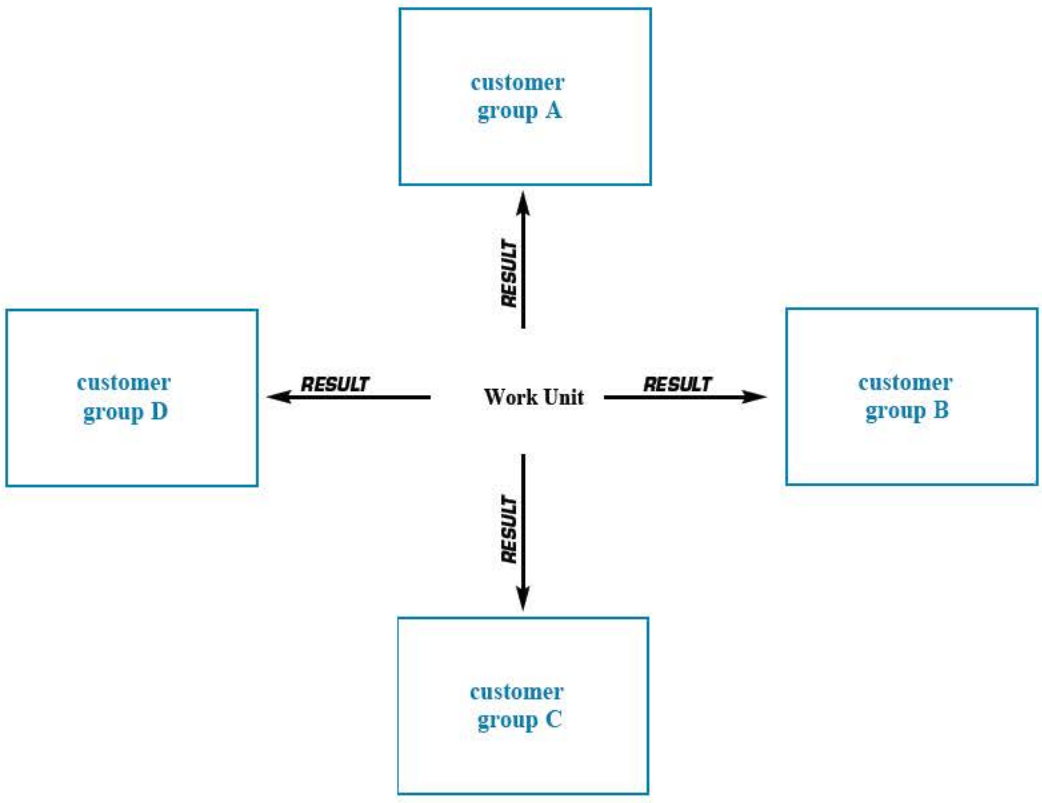
YOUR WORK UNIT'S PRODUCTS OR SERVICES

method B: determine the products and services the work unit provides for its customers

The **customer-focused method** works well when there are no clear agency goals and when the work unit knows who its customers are and what they expect. Often this method is easier to apply to administrative work units that provide support functions, such as a human resources unit, an acquisitions unit, or a facilities maintenance unit. This method focuses on achieving customer satisfaction and requires answers to each of the following questions:

- Who are the customers of the work unit? If the work unit provides a support function, most of its customers may be internal to the agency.
- What products and/or services do the customers expect? Remember to describe accomplishments, not activities.

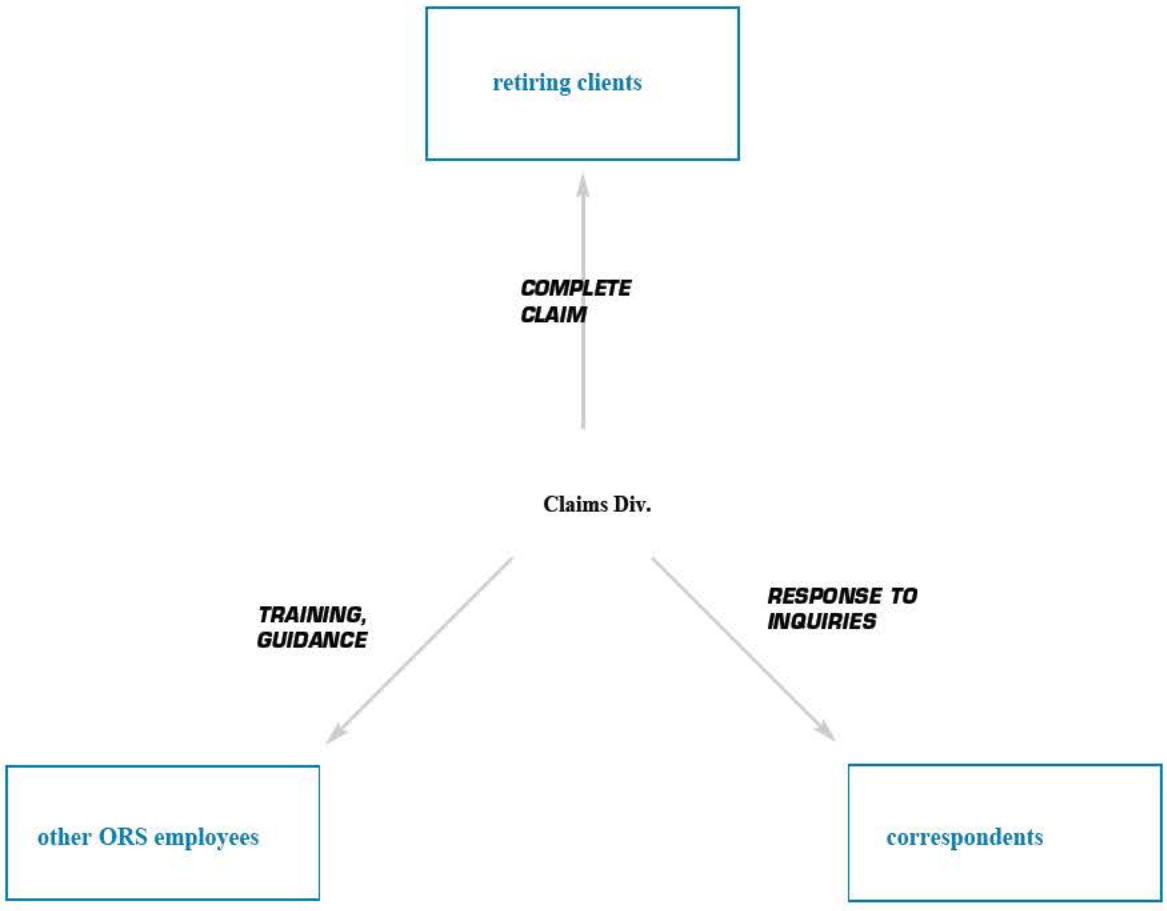
One way to approach this method is to build a map, as shown below. Place an oval representing the work unit in the center of a blank piece of paper. List the customer groups around the oval and describe the products or services the customers expect in the box under the customer groups.



EXAMPLE OF IDENTIFYING CUSTOMERS AND THEIR EXPECTATIONS

The example below diagrams the accomplishments of the Office of Retirement Service's Claims Division from a customer-focused approach. Note that the accomplishments listed are the **results** of the team's work.

example method B



EXERCISE FOR IDENTIFYING CUSTOMERS AND THEIR EXPECTATIONS

Use method B—the customer-focused method—to develop the product(s) or service(s) that your work unit provides.

1) Identify your work unit's customers

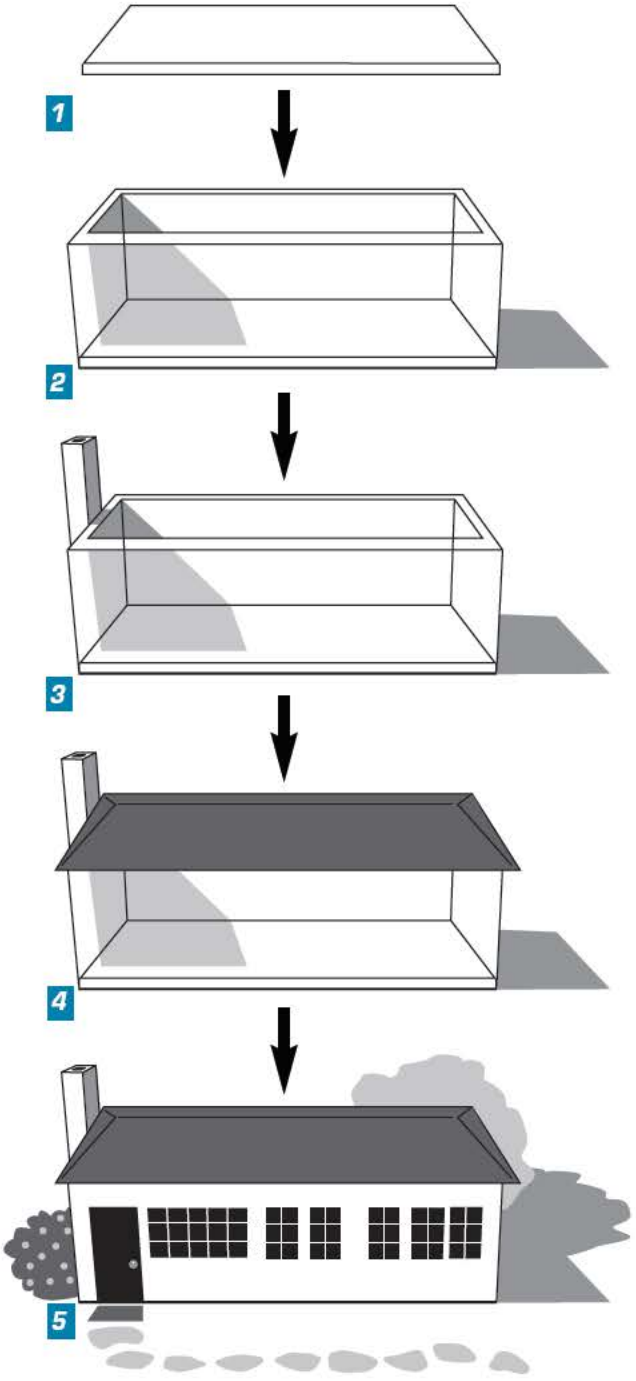
2) Determine what product(s) or service(s) your work unit supplies or provides to its customers

YOUR WORK UNIT

method C: develop a work flow chart for the work unit, establishing key steps in the work process

The **work flow charting method** works well for work units that are responsible for a complete work process, such as the processing of a case, the writing of a report, or the production of a customer information package. This method asks work units to develop work flow charts. A work flow chart is a picture of the major steps in a work process or project. It begins with the first step of the work process, maps out each successive step, and ends with the final product or service. To illustrate, the work flow chart to the right depicts a work process for building a house.

1. Foundation
2. Walls
3. Chimney
4. Roof
5. A complete house



TO HELP YOU BUILD YOUR WORK FLOW CHART, ANSWER THESE QUESTIONS:

- How does the work unit produce its products or services? List the most basic steps in the process. For this purpose, you do not need to list all the activities required. (If you were analyzing the work to find ways of improving the process, you would need to list every activity.)
- Which are the most important steps in the process? By determining these steps, you highlight areas for performance measurement.

As you map out the process, you may find yourself describing activities. Try to group the activities into key steps by describing the results of those activities as one step in the process. As an example, the activities described in the following columns are all the activities that a publication team described when it was trying to create a work flow chart for the process of developing a newsletter. By grouping the related activities into the same columns, it was easier for the team to determine the results of those activities. Those results are written at the top of the column and became the key steps in the work flow chart.

example method C

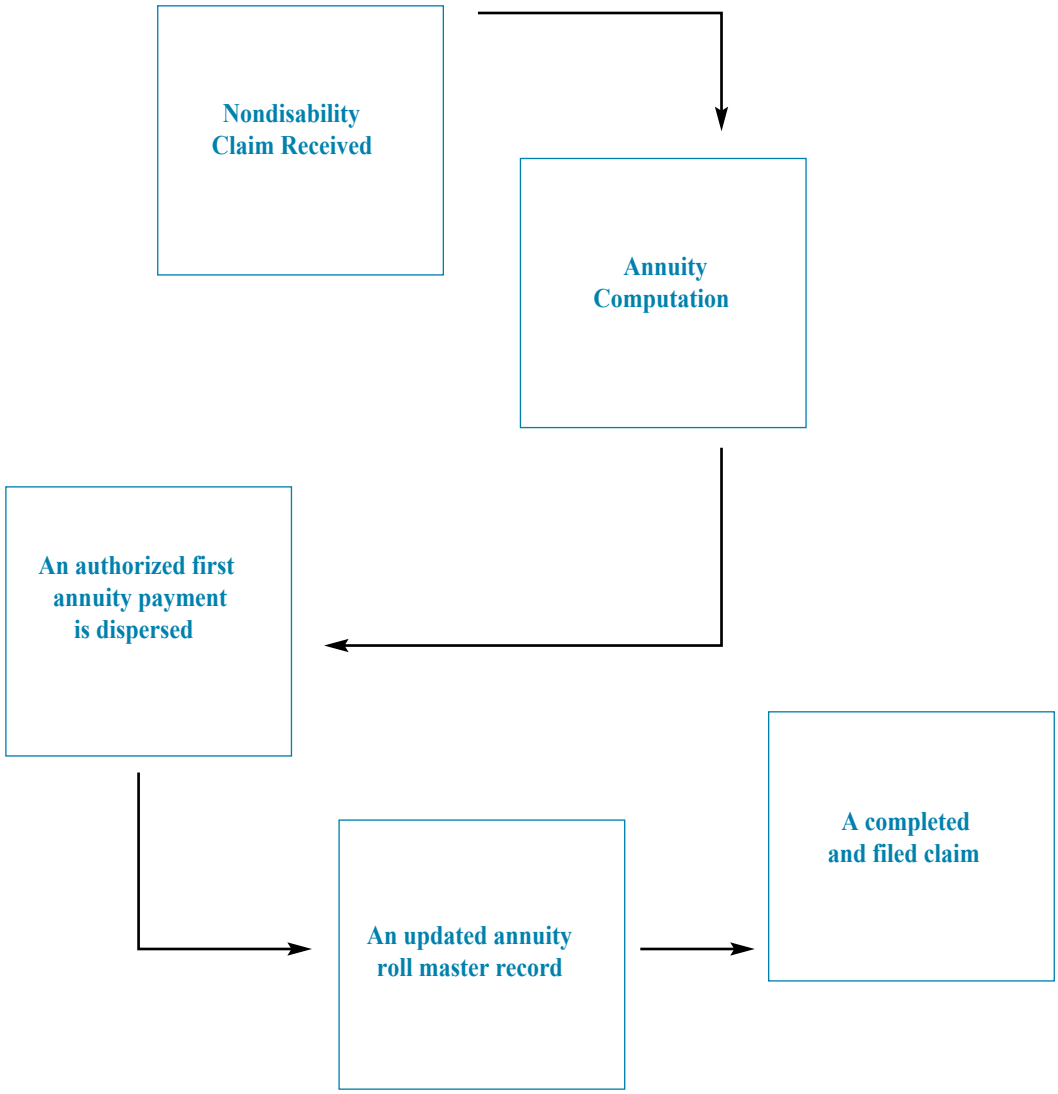
RESULTS	PLAN FOR NEXT ISSUE	THE DRAFT VERSION OF THE ARTICLES	THE EDITED VERSION OF THE ARTICLE	THE CAMERA-READY COPY
ACTIVITIES	brainstorm ideas	interview contacts	review articles for errors	crop pictures
	meet to discuss ideas	get contact review and edits of article	make suggestions for improvements	develop the original graphics
	research various resources for ideas	get pictures or graphics, if used	make necessary changes	create layout boards
	get management approval of proposed plan	write article	consider the overall effect of the entire issue	format issue

WORK FLOW CHART

ANOTHER EXAMPLE OF WORK FLOW CHARTING

This example of the results of method C—which focuses on the work flow and the key steps in the work process—uses a work flow chart that maps the key steps in processing retirement claims. Notice that the steps are described as products. In other words, all the activities to complete the steps are not listed individually but have been grouped and described as products.

example method C



EXERCISE ON WORK FLOW CHARTING

1) Select a product or services that your work unit provides.
2) As best you can, map out the work process your unit uses. Focus on the major categories or steps of the work. You may need to first list the smaller steps of the work and then group them into subproducts. (Remember to describe products and services when you can, not activities.)

step 3:
determine individual accomplishments that support work unit goals

The performance elements that will be measured in the overall employee performance plan can include both individual and group assignments and responsibilities. The most important, results-oriented aspects of a unit's performance (which are its products or services) were identified in Step 2. (Other types of processes that work units may want to measure and include as elements in their plans—but which are not products or services and would not be identified through Step 2—include internal group dynamics processes, such as decision-making or problem-solving processes, or group/team development.)

Elements that address individual accomplishments can be identified using a role-results matrix. A role-results matrix is simply a table that identifies the results each work unit member must produce to support the unit's accomplishments. To build the matrix, list the work unit's products or services across the top row of a table. List each member of the work unit or each job position down the left column of the matrix. For each cell of the table, ask this question: What must this unit member produce or perform (i.e., accomplish) to support this particular work unit product or service? List those employee products or services (i.e., accomplishments) in the appropriate cell. The products or services you list for each unit member are possible performance elements that might be included in the employee's performance plan. All performance elements should be either quantifiable or verifiable and should be described as accomplishments (nouns), not activities (verbs).

A ROLE-RESULTS MATRIX

UNIT EMPLOYEES	UNIT PRODUCT OR SERVICE	UNIT PRODUCT OR SERVICE	UNIT PRODUCT OR SERVICE	UNIT PRODUCT OR SERVICE
EMPLOYEE 1	ACCOMPLISHMENT	ACCOMPLISHMENT	ACCOMPLISHMENT	ACCOMPLISHMENT
EMPLOYEE 2	ACCOMPLISHMENT	ACCOMPLISHMENT	ACCOMPLISHMENT	*N/A
EMPLOYEE 3	ACCOMPLISHMENT	*N/A	ACCOMPLISHMENT	ACCOMPLISHMENT
EMPLOYEE 4	*N/A	ACCOMPLISHMENT	ACCOMPLISHMENT	ACCOMPLISHMENT

*The employee had no part in this work unit product or service.

EXAMPLE OF A ROLE-RESULTS MATRIX

An example of a role-results matrix is shown below. It was built for a work team that produces a bimonthly policy newsletter. The team has five members: the editor, three writers, and a graphic artist. The final product or output is the newsletter. (The expected outcome is better educated employees.) The team created a work flow chart (see page 36), which identified four key steps in the work process. The team then used these key steps to build the matrix and will use it to develop performance elements.

Note that the main steps of the work process are laid out along the top of the matrix. The team members are listed down the left-hand column. Accomplishments are listed for each team member. Also, note that not all members have assignments or responsibilities for every team accomplishment. (This often will occur in cross-functional work units that include a variety of different job series.)

When building a role-results matrix, you may identify certain aspects of performance at either the work unit level or the individual level that you may not be able to measure (e.g., the effect a human resources program has on organizational performance) or over which the unit or the employee has no control (i.e., a portion of the product must be completed by someone outside the work unit). Also, certain aspects of performance may cost too much to measure or the agency may not have the resources to measure them. You should not include these aspects of performance as elements in the performance plan, but they are still legitimate parts of the role-results matrix.

A role-results matrix is a valuable management tool. When supervisors involve employees in the process of completing the matrix, everyone's role in the work unit is very clear, which is important to the successful performance of the group. The whole process of determining work unit products and services, and then completing a role-results matrix, is a beneficial team-building exercise.

example role-results matrix

A ROLE-RESULTS MATRIX FOR A NEWSLETTER TEAM:

TEAM ACCOMPLISHMENTS →

TEAM MEMBERS	THE PLAN FOR THE NEXT ISSUE	THE DRAFT VERSION OF THE ARTICLES	THE EDITED VERSION OF THE ARTICLES	THE CAMERA-READY COPY
EDITOR	*TOPICS TO BE COVERED*		*ARTICLES THAT HAVE BEEN EDITED*	
WRITER A	*RECOMMENDATIONS FOR ARTICLES*	*DRAFT ARTICLE(S)*		
WRITER B	*RECOMMENDATIONS FOR ARTICLES*	*DRAFT ARTICLE(S)*		
WRITER C	*RECOMMENDATIONS FOR ARTICLES*	*DRAFT ARTICLE(S)*		
GRAPHIC ARTIST	*RECOMMENDATIONS FOR LAYOUT*			*A CAMERA-READY COPY*

ANOTHER EXAMPLE OF A ROLE-RESULTS MATRIX

The table below displays example data gathered for FBB's Office of Retirement Service's Claims Division using the cascading method as described on pages 29-30 and the customer-focused method on pages 33-34. Note that the products or services (i.e., the work unit accomplishments) identified through the process of Step 2 are shown along the top of the matrix. Employees are listed down the left side of the matrix. Employee work accomplishments are included in each cell. Notice that the employee work responsibilities are described as accomplishments (i.e., products or services) rather than activities or behaviors.

example role-results matrix

EMPLOYEES	WORK UNIT PRODUCTS OR SERVICES		
DIVISION MGR*	***CLAIMS PROCESSED IN LESS TIME AND WITH LOWER ERROR RATES***	***RESPONSES TO INQUIRIES***	***INCREASED NUMBER OF EMPLOYEES WHO CAN PROCESS CLAIMS***
RETIREMENT BENEFITS SPECIALIST	*A COMPLETED* ***CLAIM*** ***SUGGESTION(S)*** *FOR IMPROVING THE PROCESS*	*N/A*	***GUIDANCE,*** *TRAINING, AND* ***TECHNICAL ASSISTANCE*** *TO OTHER SPECIALISTS*
CUSTOMER SERVICE SPECIALISTS	*CLAIM CONTROL* ***LOG***	***CORRESPONDENCE*** *THAT IS FORMATTED, MAILED, AND FILED* ***ANSWERS*** *TO CUSTOMER TELEPHONE QUESTIONS*	*N/A*

Note that the Division Manager is on the same row as work unit accomplishments. This shows that the Branch Manager is responsible for work unit results.

EXERCISE FOR BUILDING A ROLE-RESULTS MATRIX

Fill in the role-results matrix for your work unit. Place the work unit products or services that you developed in Step 2 (using method A, page 31, method B, page 34, and/or method C, page 38) along the top of the matrix. Fill in the names or the job titles of the work unit's employees in the left-hand column. Then fill in the employees' accomplishments that contribute to each work unit accomplishment.

EMPLOYEES	WORK UNIT PRODUCTS OR SERVICES			
ORGANIZATIONAL CHIEF				

step 4: convert expected accomplishments into performance elements, indicating type and priority

In Steps 2 and 3 of the process presented in this handbook, you developed the expected accomplishments for the work unit and the unit's employees. Now, in Step 4, you will:

- identify which accomplishment(s) should be included as elements in the performance plan
- select which type of element to use
- assign weights or priorities

All employees must have at least one critical element in their performance plan. Critical elements must address individual performance only, except in the case of supervisors who may be held responsible for a work unit's products or services. Work unit performance can be addressed through non-critical or additional performance elements. In appraisal programs with only two summary levels, work unit performance can be addressed only through additional performance elements.

Once you have classified elements as either critical, non-critical, or additional, and if your appraisal program allows, prioritize them so that work units and employees know which elements are most important. One way to do this is to distribute 100 percentage points across the elements based on each one's importance to the organization. (Programs usually allocate weights in five-percent increments.)

HOW CAN YOU DETERMINE WHICH ELEMENTS ARE CRITICAL?

Remember that critical elements are work assignments or responsibilities of such importance that unacceptable performance on the element would result in a determination that an employee's overall performance is unacceptable. Defining critical elements must be done thoughtfully because an employee's unacceptable performance on any critical element could be the basis for an adverse action. To help decide whether an element should be classified as critical or not, answer the following questions:

- Is the element a major component of the work? If you answered "yes," the element might be critical.
- Does the element address individual performance only? Elements measuring group performance cannot be critical elements, except as explained for supervisors and only under certain circumstances.
- If the employee performed unacceptably on the element, would there be serious consequences to completing the work of the organization? If employee error on the element affects the work unit's accomplishments, the element may be critical.
- Does the element require a significant amount of the employee's time? If you answered "yes," the element might be critical.

Unless prescribed by your appraisal program, there is no fixed or uniform number of critical elements to be included in the performance plan; the number varies with the work assignments and may vary from year to year in response to changing program emphases. However, every employee must have at least one critical element.

EXAMPLE OF IDENTIFYING ELEMENTS

The Claims Division within the Office of Retirement Services (ORS) has been used on the following page as an example for identifying elements. The expected accomplishments of the Retirement Benefits Specialist (as outlined in the role-results matrix on page 41) are listed down the left side of the matrix on the next page. The work unit accomplishments for the Division are also listed. The next column shows how the Division Manager and employees designated elements as critical, non-critical, or additional. Finally, priority points are assigned to each element to give them relative weights. (Remember that ORS's appraisal program uses five levels to appraise employee performance on elements and summarizes performance overall at five levels and that non-critical and additional performance elements are allowed.)

example identifying elements

Note the following in the matrix on page 45:

1. The Division decided that "Suggestions for Improving the Process" should not affect the summary level, but the Division wanted to track and measure the value of the suggestions in order to recognize individuals who help improve the process. Therefore, it was included as an additional element and given a weight of 0. The Division plans to use the results of performance on this element as a criterion for awards recognizing innovation by individuals within ORS.

2. The Division decided that claims completed by individuals should be a critical element for Benefits Specialists, but the Division also felt it was important to count in employee performance plans the group's performance as a whole on claims completed. The Division felt that counting group performance on claims processed would encourage specialists to work together as a group and promote collaboration. Since this Division is under a five-level appraisal program and it wants to count this group element in the appraisal process, it will be a non-critical element. (If it were in a two-level appraisal program, the group element would have to be an additional performance element.)

3. For the group goal of increased number of employees who can process insurance claims, the Division decided not to count group performance in the appraisal process. Because of the importance of this group goal, however, management decided to make it an additional element and use it as a basis for recognizing the group if it meets specific goals. (Note that the Division is measuring individual performance to support this group goal and is counting individual performance as a critical element.)

4. The Division determined the priority of each element by distributing 100 points across the critical and non-critical elements. The priority points let employees know which elements are more important to the organization. Priority points also are used in this example to affect how the summary level will be determined. Using this method allows non-critical elements to count significantly in the summary level determination. (Failure on the non-critical element would not cause performance to be *Unacceptable*; it would merely count as 0 priority points and could lower the summary level—but not to *Unacceptable*.)

example identifying elements

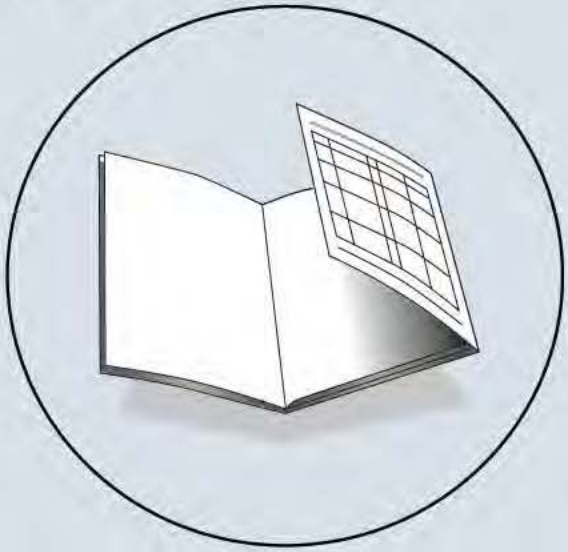
ORS RETIREMENT CLAIMS DIVISION
RETIREMENT BENEFITS SPECIALIST

ELEMENT	*ELEMENT TYPE*	*WEIGHT or POINTS*
Completed claims	Critical (CE)	50
Suggestion(s) for improving the process	Additional (AE)	0
Guidance and technical assistance to other specialists	Critical (CE)	35
WORK PRODUCTS OR SERVICES		
Claims processed in less time and with lower error rates	Non-critical (NC)	15
Increased number of employees who can process claims	Additional (AE)	0

EXERCISE ON IDENTIFYING ELEMENTS

Based on the accomplishments that you identified for your job in the role-results matrix that you made on page 42 and working within the rules established by your appraisal program, identify appropriate elements and categorize them as critical, non-critical, and, if appropriate, additional performance elements. Write those elements and their type under the columns marked "Element" and "Type" on the foldout form on the back cover. (If you have a two-level appraisal program—that is, a pass/fail program—you cannot use non-critical elements.) If applicable, prioritize the elements by distributing 100 points among the elements, giving more points to elements that are more important. Write the priority points you assign under the column labeled "priority" on the foldout form on the back cover .

FOLD OVER INSIDE BACK COVER FLAP AS SHOWN TO FILL OUT CHART



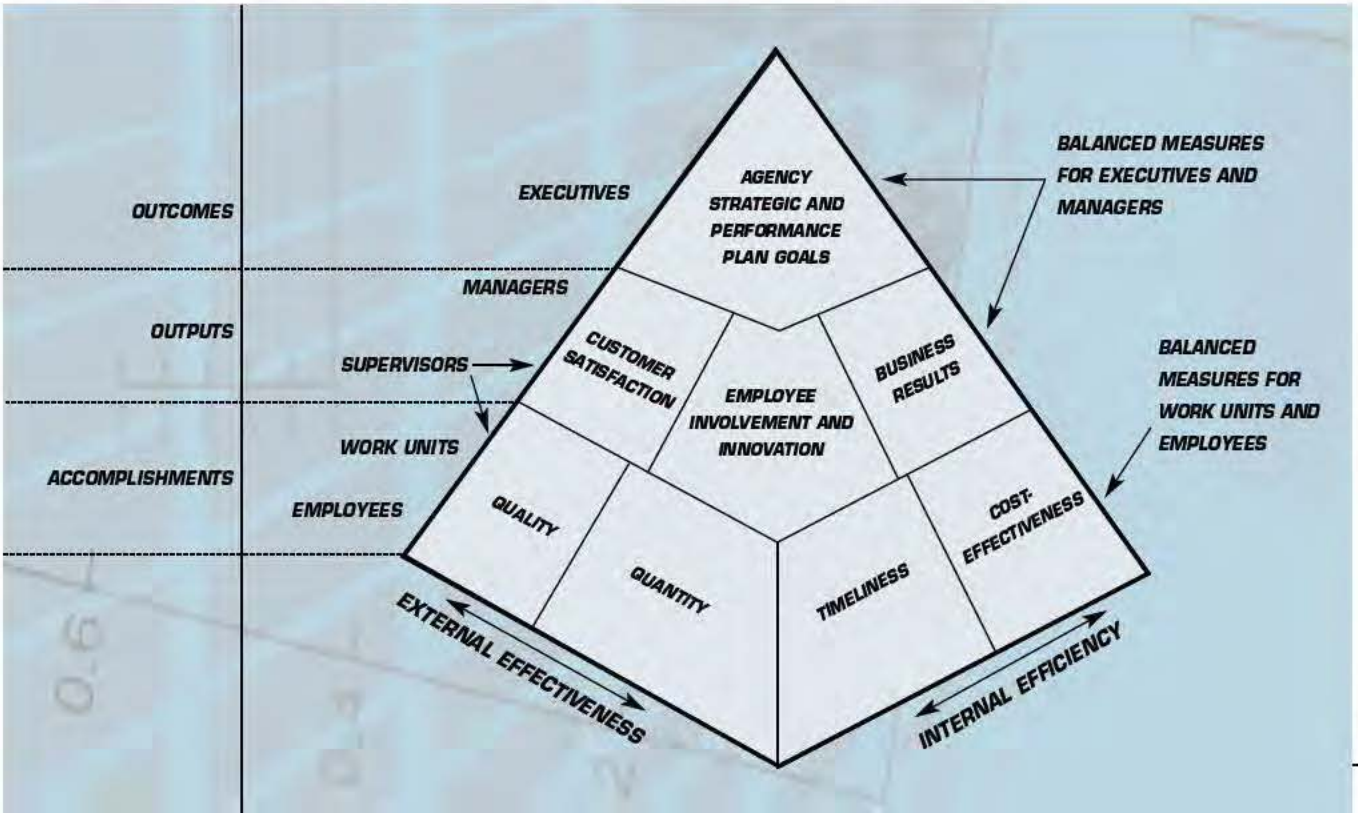
step 5: determine work unit and individual measures

In Step 4 of this process, you designated the critical, non-critical, and additional performance elements you will include in your performance plan. In Step 5, you will determine how to measure performance on those elements.

Measures are the yardsticks used to determine how well work units and employees produced or provided products or services. To develop specific measures of performance for each element in your performance plan, you first must determine the general measures that apply to each. Once you determine the general and specific measures, you will be able to develop the standards for your elements, which you will do in Step 6 of this process. Your standards will be worded in terms of the specific measures developed in this step.

The performance pyramid below shows the types of general measures that are used at different levels in the organization. Note that the balanced measures incorporating the business, customer, and employee perspectives are appropriate for measuring managerial performance and are sometimes appropriate for supervisory or even work unit performance. At the bottom of the pyramid, the four general measures normally used for measuring work unit and employee performance are quality, quantity, timeliness, and cost-effectiveness.

PERFORMANCE PYRAMID FOR IDENTIFYING PERFORMANCE MEASURES



GENERAL MEASURES

QUALITY addresses how well the employee or work unit performed the work and/or the accuracy or effectiveness of the final product. Quality refers to accuracy, appearance, usefulness, or effectiveness. Quality measures can include error rates (such as the number or percentage of errors allowable per unit of work) and customer satisfaction rates (determined through a customer survey).

QUANTITY addresses how much work the employee or work unit produced. Quantity measures are expressed as a number of products produced or services provided, or as a general result to achieve.

TIMELINESS addresses how quickly, when, or by what date the employee or work unit produced the work.

COST-EFFECTIVENESS addresses dollar savings or cost control for the Government. You should develop measures that address cost-effectiveness on specific resource levels (money, personnel, or time) that you can generally document and measure in agency annual fiscal year budgets. Cost-effectiveness measures may include such aspects of performance as maintaining or reducing unit costs, reducing the time it takes to produce or provide a product or service, or reducing waste.

DEVELOPING SPECIFIC MEASURES

To develop specific measures, you first must determine the general measure(s) that are important for each element (i.e., quantity, quality, timeliness, or cost-effectiveness). Then, determine how to measure the quantity, quality, timeliness, and/or cost-effectiveness for the element. If you can measure an accomplishment with numbers, record the form of measurement. If you can only describe performance (i.e., observe and verify), clarify who will appraise the performance and the factors they will appraise.

The kinds of questions you should ask in this process include the following.

FIRST: For each element, decide which general measures apply:

- Is quality important? Does the stakeholder or customer care how well the work is done?
- Is quantity important? Does the stakeholder or customer care how many are produced?
- Is it important to accomplish the element by a certain time or date?
- Is it important to accomplish the element within certain cost limits?
- What measures are already available?

SECOND: For each general measure, ask:

- How could [quality, quantity, timeliness, and/or cost-effectiveness] be measured?
- Is there some number or percent that could be tracked?

If the element does not lend itself to being measured with numbers and can only be described, ask:

- Who could judge that the element was done well?
- What factors would they look for?

FINALLY: Write down or otherwise record the specific measures. If the measure is numeric, list the units that you will track. If the measure is descriptive, identify the judge and list the factors that the judge will look for to observe and verify performance.

example general & specific measures

CLAIMS DIVISION

Note that general and specific measures have been added to the elements for a Retirement Benefits Specialist (see page 45). Also note that only the measures have been identified, not the standard that describes how well the element should be done. (Standards are addressed in the next step in the process.)

RETIREMENT BENEFITS SPECIALIST

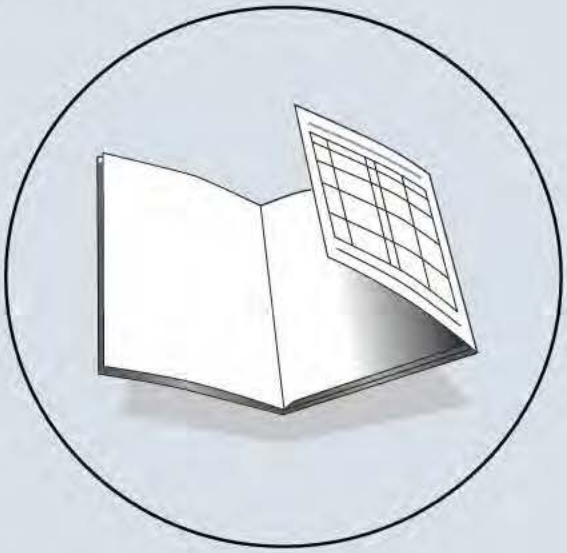
PRIORITY POINTS	ELEMENT	TYPE	GENERAL MEASURES	SPECIFIC MEASURES
50	Completed *claim*	CE	Quality Quantity Timeliness	The accuracy of annuity amounts. The completeness of the paperwork The number of claims processed per week The average number of days it takes to process a claim*
35	*Guidance* and *technical assistance* to other specialists	CE	Quality Timeliness	The accuracy of the information, as determined by supervisor The perceptions of other specialists that the incumbent is willing to assist and that feedback is helpful The number of hours it takes for the incumbent to respond to other specialists' requests for assistance
15	**Division Element:** Division *claims* processed in less time and with lower error rates	NC	Quality Quantity Timeliness	The accuracy rate for annuity amounts from the whole Division The number of claims the Division processes per week The average number of days it takes to process a claim*
0	Suggestion(s) for improving the process (for special individual recognition)	AE	Quality Quantity Cost-Effectiveness	The supervisor's and reviewers' judgment that the suggestion(s) improve(s) efficiency, productivity, and flexibility The number of suggestions made The amount of money saved by adopting the suggestion
0	**Division Element:** Increased number of employees who can process claims	AE	Quantity Quality	The number of employees who can do claims The accuracy rate of annuities processed

**Note: Using the average adjusts for the varying levels of difficulty in claims and ensures that specialists will not focus only on easy claims and ignore the difficult ones. Also, all specialists are assigned equal numbers of easy and difficult claims to ensure fairness of the standard. Finally, the average can be prorated when necessary.*

EXERCISE FOR DETERMINING GENERAL AND SPECIFIC MEASURES

Determine the general measures for your job based on the elements that you created in the previous exercise on page 46. Next, identify some specific measures. Write down those general and specific measures under the columns labeled "General Measure" and "Specific Measure" on the foldout form on the back cover.

FOLD OVER INSIDE BACK COVER FLAP AS SHOWN TO FILL OUT CHART



step 6: develop work unit and individual standards

The next step in the process of developing a performance plan is to establish standards for the elements. To work through this section successfully, you will need to know the number of levels your appraisal program uses to appraise elements. You also will need to know which performance level your program uses as the retention standard. (A definition of retention standard is included in this section.) The discussions below address performance standards and what to avoid when writing standards.

WHAT IS A PERFORMANCE STANDARD?

Performance standards are management-approved expressions of the performance threshold(s), requirement(s), or expectation(s) that employees must meet to be appraised at particular levels of performance.

Each critical element must have a *Fully Successful* or equivalent standard established. Technically, neither non-critical elements nor additional performance elements require a *Fully Successful* or equivalent standard. However, to help employees and work units understand the expectations for performance on these elements, we recommend that they have a clear idea of what is considered fully successful performance.

(NOTE: NON-CRITICAL ELEMENTS MUST BE APPRAISABLE AT LEAST ON TWO LEVELS, BUT THOSE LEVELS CAN BE ESTABLISHED HIGHER THAN THE FULLY SUCCESSFUL LEVEL.)

WHAT SHOULD PERFORMANCE STANDARDS INCLUDE?

Once you have established the specific measures that apply to the elements, you can begin to write the standards. Before writing the *Fully Successful* standard, you must know the number of levels that your appraisal program uses to appraise elements. For example, if you are under an appraisal program that uses two levels to appraise elements, the *Fully Successful* standard would describe a single point of performance. Any performance at or above that point is *Fully Successful,* and anything below it is *Unacceptable.* If, however, your appraisal program uses five levels to appraise performance, you would describe the *Fully Successful* standard as a range. Performance that exceeds the top of that range would be appraised at the level(s) above *Fully Successful,* and performance below the bottom of that range would be *Minimally Successful* (or equivalent) or *Unacceptable.* How you write the *Fully Successful* standard depends on the number of levels your program uses to appraise performance on elements.

If a specific measure for an element is numeric, for example, you would list the units to be tracked and determine the range of numbers (or the single number in a program that appraises elements at two levels) that represents *Fully Successful* performance. If the specific measure is descriptive, you would identify the appraiser(s) who would judge performance, list the factors that the appraiser(s) would look for , and determine what he or she would see or report that verifies that *Fully Successful* performance for that element had been met. (Remember to express performance standards in terms of the specific measure[s] determined in Step 5 of this process.)

Several examples of elements and standards are included below. The specific measures are in italics; the performance (or range of performance) that actually establishes the level of the standard is in boldface type.

ELEMENT: CASES COMPLETED

Fully Successful Standard in an appraisal program that appraises elements at five levels (to meet this standard, all of the bullets listed must be present or occur):

- no more than **3-4** *valid customer complaints per year,* as determined by the supervisor
- no more than **2-3** *errors per quarter,* as spotted by the supervisor
- no more than **4-5** *late cases per year* (processed later than 10 working days from receipt)

(If this standard had been written for an appraisal program that appraised elements at only two levels, the standard would have been "no more than **4** *valid customer complaints per year,*" "no more than **3** *errors per quarter,*" and "no more than **5** *late cases per year.*")

ELEMENT: MEETINGS SCHEDULED

Fully Successful Standard in an appraisal program that appraises elements at five levels (to meet this standard, all of the bullets listed must be present or occur):

The **meeting leader and attendees generally are satisfied** that

- *the room size matched the group size*
- *attendees were notified of the meeting*
- *attendees knew whom to call for information*
- *the meeting was set up by the deadline*

ELEMENT: LEGAL ADVICE

Fully Successful Standard in an appraisal program that appraises elements at five levels (to meet this standard, all of the bullets listed must be present or occur):

- Consistent with attorney's grade, attorney **usually** *carries an adequate workload of projects,* **frequently** *takes on new projects* to meet the needs of the office, and **generally** *shows personal initiative* in handling projects (generally, projects are of average difficulty)
- Consistent with attorney's grade, legal advice rendered is **infrequently** *modified by practice group leaders and supervisors* in a **significant** way
- Advice given to clients is **usually** *timely and thorough* and of **average** *quality,* and **usually** *shows sensitivity* to program and agency needs

ADDITIONAL EXAMPLES OF ELEMENTS AND STANDARDS SPECIFICALLY WRITTEN FOR APPRAISAL PROGRAMS THAT APPRAISE ELEMENTS AT FIVE, THREE, AND TWO LEVELS ARE INCLUDED IN THE APPENDICES.

WHAT SHOULD YOU AVOID WHEN WRITING RETENTION STANDARDS?

By "retention" standard, we mean the standard that describes the level of performance necessary to be retained in a job (i.e., the standard written for performance one level above the *Unacceptable* level). In appraisal programs that do not have a *Minimally Successful* or equivalent level available for appraising elements, the retention-level standard is the *Fully Successful* standard. Otherwise, the retention standard is the *Minimally Successful* or equivalent standard.

The Merit Systems Protection Board (MSPB) and the courts have issued many decisions on the topic of valid performance standards. This section highlights what the Board deems to be two major errors to avoid when writing standards. In order to avoid reversal by the MSPB, agencies must ensure that "retention" standards:

- are not impermissibly absolute (i.e., allow for some error)
- inform the employee of the level of performance needed to retain his or her job

AVOID ABSOLUTE RETENTION STANDARDS

An "absolute" retention standard—one that allows for no errors—is acceptable only in very limited circumstances. When a single failure to perform under a critical element would result in loss of life, injury, breach of national security, or great monetary loss, an agency can legitimately defend its decision to require perfection from its employees. In other circumstances, the MSPB and the courts usually will find that the agency abused its discretion by establishing retention standards that allow for no margin of error.

When writing standards, you should avoid the appearance of requiring perfection at the retention level. In appraisal programs that do not appraise elements at the *Minimally Successful* or equivalent level, you must carefully word the *Fully Successful* or equivalent standards so that they are not absolute. For example here are *Fully Successful* standards used by agencies that the MSPB would consider absolute retention standards if they were used in a two-level appraisal program:

- Work is timely, efficient, and of acceptable quality
- Communicates effectively within and outside of the organization

MSPB considers these standards absolute because they appear to require that work is *always* timely, efficient, and of acceptable quality and that the employee *always* communicates effectively. When writing standards—especially retention standards—avoid simply listing tasks without describing the regularity of the occurrence of the task—but also avoid the requirement to do it *always*.

Also, in appraisal programs that appraise elements at levels above *Fully Successful*, the *Fully Successful* standard itself—as well as the *Exceeds Fully Successful* standard when an *Outstanding* or equivalent level is possible—should not be absolute. If it is supposed to be possible to exceed, make sure it is written that way.

To help determine whether you are writing an absolute standard, ask yourself:

- How many times may the employee fail this requirement and still be acceptable?
- Does the retention standard use words such as "all," "never," and "each"? (These words do not automatically create an absolute standard, but they often alert you to problems.)
- If the retention standard allows for no errors, would it be valid according to the criteria listed above (risk of death, injury, etc.)?

The examples of elements and standards included in the appendices were carefully written to avoid absolute requirements.

AVOID "BACKWARD" STANDARDS

Case law requires that an employee understand the level of performance needed for retention in the position. When using a *Minimally Successful* level of performance, a common tendency is to describe it in terms of work that does not get done instead of what must be done to meet that retention standard. Describing negative performance actually describes *Unacceptable* performance. Standards such as "fails to meet deadlines" or "performs work inaccurately" allow an employee to do virtually no work or to do it poorly and still meet that retention standard. MSPB considers these "backward" retention standards invalid. To help you determine whether you are writing a backward retention standard, ask:

- Does the standard express the level of work the supervisor wants to see or does it describe negative performance? (Example of describing negative performance: Requires assistance more than 50 percent of the time.)
- If the employee did nothing, would he or she meet the standard, as written? (Example: Completes fewer than four products per year.)

MORE EXAMPLE STANDARDS

Example standards for a Retirement Benefits Specialist are shown on the next two pages. These standards were written for elements that are appraised at five levels. The appraisal regulations only require that a *Fully Successful* standard be established for each element. However, to clarify at the outset what employees need to do to exceed the *Fully Successful* level (as well as what they must do to be retained in the position) the Claims Division includes standards for the *Minimally Successful*, *Fully Successful*, and *Exceeds Fully Successful* levels of performance. (Performance below the minimum of the *Minimally Successful* range of performance is considered *Unacceptable*, and performance above the maximum of the *Exceeds Fully Successful* range of performance is *Outstanding*.)

Most of the example standards on the next two pages are quantifiable. The numbers used are based on work flow data. Examples of descriptive standards written at a variety of levels are found in the appendices. In all these examples, distinguishing between *Fully Successful* and levels above or below *Fully Successful* requires careful planning and forethought.

NOTE THAT THE STANDARDS TYPICALLY DESCRIBE A RANGE OF PERFORMANCE. ALSO NOTE THAT THE ELEMENTS HAVE BEEN REARRANGED TO ORDER THE ELEMENTS BY WEIGHT.

example develop standards

RETIREMENT BENEFITS SPECIALIST

ELEMENT	GENERAL MEASURES	SPECIFIC MEASURES	STANDARDS *		
			MINIMALLY SUCCESSFUL	FULLY SUCCESSFUL	EXCEEDS FULLY SUCCESSFUL
Completed *claims* Critical Element 50 priority points	Quality	The accuracy of annuity amounts The completeness of the paperwork	82-87% of annuity amounts are accurate and of claims are complete	88-93% of annuity amounts are accurate and of claims are complete	94-97% of annuity amounts are accurate and of claims are complete
	Quantity	The number of claims processed per week	10-12 claims processed per week	13-16 claims processed per week	17-20 claims processed per week
	Timeliness	The average number of days it takes to process a claim	An average of 101-110 days to complete claim	An average of 90-100 days to complete claim	An average of 75-90 days to complete claim
Guidance and *technical assistance* to other specialists Critical Element 35 priority points	Quality	The accuracy of the information, as determined by supervisor	Usually accurate	Usually accurate	Almost always accurate
		The perceptions of other specialists that the incumbent is willing to assist and that feedback is helpful	50-59% of specialists agree that incumbent is routinely willing to assist and that feedback is helpful	60-80% of specialists agree that incumbent is routinely willing to assist and that feedback is helpful	81-89% of specialists agree that incumbent is routinely willing to assist and that feedback is helpful
	Timeliness	The number of hours it takes for the incumbent to respond to other specialists' requests for assistance	Usually responds within 9-12 working hours from receipt of request	Usually responds within 4-8 working hours from receipt of request	Usually responds within 2-3 working hours from receipt of request
Claims Division: *claims* processed in less time and with lower error rates Non-critical Element 15 priority points	Quality	The accuracy rate for annuity amounts from the whole Division	N/A**	88-93% annuity amounts are accurate	94-97 % annuity amounts are accurate
	Quantity	The number of claims the Division processes per week		220-230 claims processed by the Division per week	231-244 claims processed by the Division per week
	Timeliness	The average number of days it takes to process a claim		An average of 90-100 days to complete claim	An average of 75-90 days to complete claim

example develop standards

RETIREMENT BENEFITS SPECIALIST, CONTINUED

ELEMENT	GENERAL MEASURES	SPECIFIC MEASURES	STANDARDS*		
			MINIMALLY SUCCESSFUL	FULLY SUCCESSFUL	EXCEEDS FULLY SUCCESSFUL
Suggestion(s) for improving the process (for special individual recognition) ▎Additional Performance Element ▎0 priority points	Quality	The supervisor's and reviewers' judgment that the suggestion(s) improve(s) efficiency, productivity, and flexibility	N/A**	Management and Division members determine that the suggestion(s) is/are worth adopting	Management and Division members determine that the suggestion(s) is/are worth adopting
	Quantity	The number of suggestions made		Incumbent provides 1-2 adopted suggestions per year	Incumbent provides 3-5 adopted suggestions per year
	Cost Effectiveness	The amount of money saved by adopting the suggestion		The incumbent's suggestion saved up to 10% of costs	The incumbent's suggestion saved 10-25% of costs
Claims Division: Increased number of employees who can process claims ▎Additional Performance Element ▎0 priority points	Quantity	The number of employees who can do claims	N/A**	35- 50% of Division employees can process claims	51-75% of Division employees can process claims
	Quality	The accuracy rate of annuities processed		88-93% of annuity amounts are accurate	94-97% of annuity amounts are accurate

*To meet the performance level of the standards described for each element, each listed part of the standard must be present or occur.

**The Division decided that there was no benefit to establishing a *Minimally Successful* standard for a non-critical or an additional performance element.

If these standards had been written for an appraisal program that appraises elements at only two levels, only the *Fully Successful* standard would have been included and it would describe a single point, not a range. So, for example, on the first element (i.e., completed case files) instead of establishing an 88-93 percent accuracy rate, etc., as the *Fully Successful* standard, the standard would be:

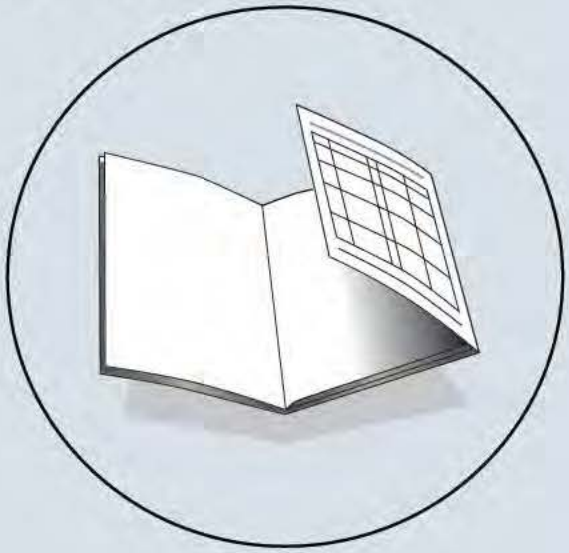
- 88% accuracy or better
- at least 13 cases processed per week;
- takes an average of 100 days to complete case

Another point of interest in the example is that the elements and standards written for the Division were included in each Division employee's performance plan as group elements and standards.

EXERCISE FOR WRITING STANDARDS

Based on the elements and measures you established in the previous exercise on page 51, develop *Fully Successful* standards for your elements. Write those standards under the column labeled "Standards" on the foldout form on the back cover. Remember to write standards that specifically match the measurement levels of your appraisal program (i.e., two-level or more than two-level). This exercise is asking you to develop only the *Fully Successful* standard. However, if your appraisal program appraises elements at more than two levels, you may also want to define the other levels of performance that are possible.

FOLD OVER INSIDE BACK COVER FLAP AS SHOWN TO FILL OUT CHART



step 7: determine how to monitor performance

Monitoring performance means measuring performance and providing feedback to employees. Agency appraisal programs are required to provide ongoing appraisal, which includes, but is not limited to, conducting one or more progress reviews during each appraisal period. In addition to a once– or twice–a–year progress review, which is sometimes a formal part of the appraisal process, supervisors and employees should discuss performance informally and often.

Determining how to monitor performance is an important step in developing performance plans. You may have worked through the previous six steps of the process presented in this handbook, developed what you thought were great elements and standards, and then found that monitoring performance on an element is impossible, or too costly, or too time-consuming. If this happens, think through other specific measures that indicate performance—measures that are as specific as possible.

To complete this step in the process:

- Determine what data to collect for each performance element, the source of the data, and whether to collect all the data or just a sample
- Determine when to collect the data, who will collect it, and who will receive it
- Review existing reports for possible use as feedback reports
- Create feedback tables or graphs where necessary or applicable
- Try to design feedback processes that give feedback automatically

FEEDBACK

Effective and timely feedback addressing employee performance on elements and standards is an essential component of a successful performance management program. People need to know in a timely manner how they are doing, what is working, and what is not working.

Feedback can come from many different sources: managers and supervisors, measurement systems, peers, and customers, just to name a few. Using multiple sources of feedback, which is sometimes called 360-degree assessment or multirater appraisal, is done in a variety of ways, but most methods are computerized and the raters are anonymous. Whether you need or want to use multirater appraisal depends on what you want to measure. For example, if you want to measure customer satisfaction, the best way to get the information is to ask the customer directly. (If customer survey tools are not available, or they are too expensive to develop, you may have to rely on other feedback sources, such as the number of complaints received.)

However feedback occurs, certain factors ensure its effectiveness:

SPECIFICITY Feedback works best when it relates to a specific goal, such as those established in elements and standards. Basing feedback on the employee's performance against his or her elements and standards is key to providing tangible, objective, and powerful feedback. Telling employees that they are doing well because they exceeded their goal by 10 percent is more effective than simply saying "you're doing a good job."

TIMELINESS Employees should receive information about how they are doing in as timely a fashion as possible. If they need to improve their performance, the sooner they find out about it, the sooner they can correct the problem. If employees have reached or exceeded a goal, the sooner they receive positive feedback, the more rewarding it is to them.

MANNER Give feedback in a manner that will best help improve performance. Since people respond better to information presented in a positive way, express feedback in a positive manner. This is not to say that information should be sugar-coated. Present accurate, factual, and complete feedback; it is more effective when it reinforces what the employee did right and then identifies what the employee needs to do in the future. Constant criticism eventually falls on deaf ears.

NATURALLY OCCURRING FEEDBACK Some kinds of feedback occur naturally while other kinds require careful planning and management. Naturally occurring feedback can be classified into two categories. The first type is self-evident feedback—information that employees can see for themselves as they do their work. For instance, a team of materials handlers who are given the assignment of moving ten stacks of supplies from one side of the warehouse to the other by the end of the day will know that if only one of ten stacks is moved by noon, it is not likely to complete the assignment on time. This information is self-evident and is obtained by the employees making their own comparisons against a specific goal.

Another kind of self-evident feedback can be gained by having a broader scope of work. The broader the employee's scope of work, the better the employee can determine the quality of the finished product. For example, a writer/editor assigned to write a portion of an article may feel satisfied with the section he wrote. But the same writer/editor , if assigned responsibility for the entire article, would see that his independently written section had no relation to the rest of the article and needed revision.

The second category of naturally occurring feedback is carefully planned feedback characterized by automatic, frequent delivery through a measurement system. It is possible to design feedback into a work process or a measurement system so that employees receive it automatically. For example, feedback loops designed into many work processes provide performance measures daily, such as a production or printing process (i.e., number of copies printed per day as determined by machine count). Also, total quality and reengineering programs use extensive work process measurement methods. Employees measure for themselves how they and their team are doing.

Designing effective feedback into a performance management program will improve individual and team performance and will make your organization more effective. With effective feedback processes, employees can see their progress and that motivates them to reach their performance goals successfully.

example feedback sources

RETIREMENT BENEFITS SPECIALIST

ELEMENT	GENERAL MEASURES	SPECIFIC MEASURES	STANDARDS*			FEEDBACK SOURCE FOR MONITORING
			MINIMALLY SUCCESSFUL	FULLY SUCCESSFUL	EXCEEDS FULLY SUCCESSFUL	
Completed *claims* Critical Element 50 priority points	Quality	The accuracy of annuity amounts. The completeness of the paperwork	82-87% of annuity amounts are accurate and of claims are complete	88-93% of annuity amounts are accurate and of claims are complete	94-97 % of annuity amounts are accurate and of claims are complete	Data from automated system
	Quantity	The number of claims processed per week	10-12 claims processed per week	13-16 claims processed per week	17-20 claims processed per week	Data from automated system
	Timeliness	The average number of days it takes to process a claim	An average of 101-110 days to complete claim	An average of 90-100 days to complete claim	An average of 75-90 days to complete claim	Data from automated system
Guidance and *technical assistance* to other specialists Critical Element 35 priority points	Quality	The accuracy of the information, as determined by supervisor	Usually accurate	Usually accurate	Almost always accurate	Random supervisor observation and 360-degree tool
		The perceptions of other specialists that the incumbent is willing to assist and that feedback is helpful	50-59% of specialists agree that incumbent is routinely willing to assist and that feedback is helpful	60-80% of specialists agree that incumbent is routinely willing to assist and that feedback is helpful	81-89% of specialists agree that incumbent is routinely willing to assist and that feedback is helpful	
	Timeliness	The number of hours it takes for the incumbent to respond to other specialists' requests for assistance	Usually responds within 9-12 working hours from receipt of request	Usually responds within 4-8 working hours from receipt of request	Usually responds within 2-3 working hours from receipt of request	360-degree tool
Claims Division: Division *claims* processed in less time and with lower error rates Non-Critical Element 15 priority points	Quality	The accuracy rate of annuity amounts for the whole Division	N/A**	88-93% annuity amounts are accurate	94-97 % annuity amounts are accurate	Data from automated system
	Quantity	The number of claims the Division processes per week		220-230 claims processed by Division per week	231-244 claims processed by Division per week	Data from automated system
	Timeliness	The average number of days it takes to process a claim		An average of 90-100 days to complete claim	An average of 75-90 days to complete claim	Data from automated system

example feedback sources

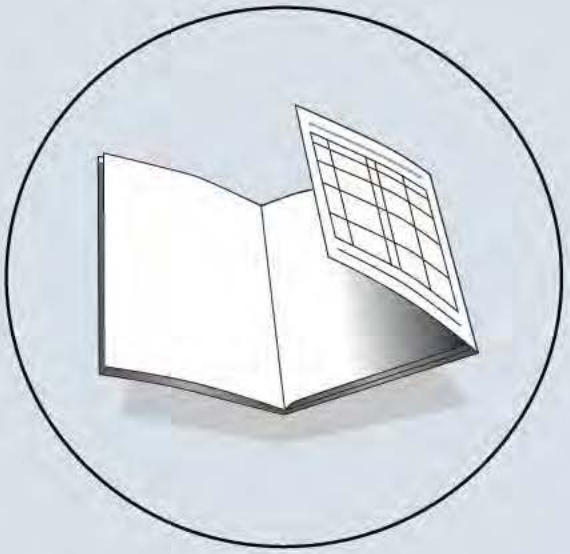
ELEMENT	GENERAL MEASURES	SPECIFIC MEASURES	STANDARDS*			FEEDBACK SOURCE FOR MONITORING
			MINIMALLY SUCCESSFUL	FULLY SUCCESSFUL	EXCEEDS FULLY SUCCESSFUL	
Suggestion(s) for improving the process (for special individual recognition) ▎Additional Performance Element ▎0 priority points	Quality	The supervisor's and reviewers' judgment that the suggestion(s) improve(s) efficiency, productivity, flexibility, and/or usability	N/A**	Management and Division members determine that the suggestion(s) is/are worth adopting	Management and Division members determine that the suggestion(s) is/are worth adopting	Supervisor and Branch members' judgment
	Quantity	The number of suggestions made		Incumbent provides 1-2 adopted suggestions per year	Incumbent provides 3-5 adopted suggestions per year.	Supervisor tracks
	Cost Effectiveness	The amount of money saved by adopting the suggestion.		The incumbent's suggestions saved up to 10% of costs	The incumbent's suggestions saved up to 10-25% of costs	Data from automated system
Claims Division: Increased number of employees who can process claims ▎Additional Performance Element ▎0 priority points	Quantity	The number of employees who can do claims	N/A**	35-50% of Division employees can process claims	51-75% of Division employees can process claims	Supervisor observation
	Quality	The accuracy rate of annuities processed		88-93% of annuity amounts are accurate	94-97% of annuity amounts are accurate	Data from automated system

*To meet the performance level of the standards described for each element, each listed part of the standard must be present or occur.
**The Division decided that there was no benefit to establishing a *Minimally Successful* standard for a non-critical or an additional performance element.

EXERCISE ON DEFINING FEEDBACK SOURCES

Now that you have developed elements, measures, and standards in previous exercises, what are the best sources of feedback for those elements? How often is it feasible to receive feedback? Who needs to see the feedback? Write down those sources of feedback under the column labeled "Feedback Source" on the foldout form on the back cover.

FOLD OVER INSIDE BACK COVER FLAP AS SHOWN TO FILL OUT CHART



step 8: check the performance plan

Once you have developed a performance plan using the previous seven steps, checking your work is always a good idea. Use the checklist below to ensure that the elements and standards you developed to include in the performance plan are effective and meet regulatory requirements:

- Are the critical elements truly critical? Does failure on the critical element mean that the employee's overall performance is unacceptable?
- Is the range of acceptable performance clear? Are the performance expectations quantifiable, observable, and/or verifiable?
- Are the standards attainable? Are expectations reasonable?
- Are the standards challenging? Does the work unit or employee need to exert a reasonable amount of effort to reach the fully successful performance level?
- Are the standards fair? Are they comparable to expectations for other employees in similar positions? Do they allow for some margin of error?
- Are the standards applicable? Can the appraiser(s) use the standards to appraise performance? Can the appraiser(s) manage the data collected through the measurement process?
- Will work units and employees understand what is required?
- Are the elements and standards flexible? Can they be adapted readily to changes in resources or objectives?
- If your program permits appraising elements at levels above the *Fully Successful* or equivalent level, is the *Fully Successful* or equivalent standard surpassable? Is it possible for a work unit's or an employee's performance to exceed it?

Guiding Principles for Performance Measurement

The principles listed below contain some valuable lessons learned about measuring performance.

VIEW PERFORMANCE MEASUREMENT AS A VALUABLE TOOL, NOT AS AN EVIL
People view measurement systems from at least two different perspectives. When used constructively, they see a measurement system as a helpful feedback tool that provides information to managers and employees about how well they are doing in reaching their goals and where they might have room for improvement. It also provides information on which to base awards and recognition. When used poorly, however, people see a measurement system as a punishing club with which to hit people over the head if the numbers or results are bad. Managers and employees must trust that the measurement system is beneficial to them and the organization; otherwise, the temptation to game the numbers to avoid discipline will overwhelm them.

ACCEPTANCE OF THE PERFORMANCE MEASUREMENT PROCESS IS ESSENTIAL TO ITS SUCCESS Involving employees in the development of the elements and standards included in the performance plan is an excellent way to clarify expectations and measurement terminology. Active employee participation in creating valid measures that accurately reflect performance decreases the possibility that employees may feel manipulated through the measurement system.

MEASURE WHAT IS IMPORTANT—NOT WHAT IS EASY TO MEASURE It is easy to count the number of days since a project began, but if that is all that you measure, is that enough information to assess performance? No, probably not. Or if, for example, a customer service team only measures the number of calls that come into the team (the easy measure) and does not attempt to measure customer satisfaction with its service (the more difficult measure), the team does not have complete information about its performance and has no idea how well it is serving its customers. In addition, because what gets measured gets done, the team will probably focus on how it can increase the number of calls it receives and ignore the quality of service it provides.

As a result, organizations need to anticipate the behavioral and unintended consequences of measuring performance. As an example, recently a medical laboratory came under fire because of the errors it made in certain of its cancer tests. A high number of cancer tests that the laboratory had approved as negative turned out to be wrong—cancer had actually been

evident. An investigation found that the laboratory had been measuring and rewarding its employees on the number of slides they reviewed daily, not on the accuracy of the reviews. Knowing that the more slides they reviewed, the more recognition they received, employees were quickly moving from slide to slide to slide without accurately reading them. As a result, the lab's errors in measuring what was important allowed cancer to go untreated and people who could have been saved through early detection and treatment lost their lives.

DEVELOP EMPLOYEE PERFORMANCE PLANS THAT ARE FLEXIBLE ENOUGH TO ALLOW FOR CHANGES IN PROGRAM GOALS TO KEEP THE PROCESS CREDIBLE Do not design performance plans that are set in concrete; build in flexibility so you can adjust them as program goals and work assignments change. Even though employees must work at least a minimum period of time on elements and standards before they receive performance ratings, the agency minimum appraisal period usually provides enough time during the appraisal period for changes in elements and standards. (Minimum appraisal periods usually range from 30-120 days, depending on the agency. Check with your agency to find out the minimum appraisal period that applies to you.)

RELY ON MULTIPLE MEASURES Don't rely on a single measure. Remember the story of the three blind men who went for a walk and came across an elephant? One felt the animal's trunk and claimed that the elephant was like a large snake. Another explored the elephant's leg and claimed that the elephant was like a big tree trunk. The third blind man touched the elephant's side and said that the elephant was like a tall, wide wall. All three of them were right, but all of them were wrong. Each one was relying on only one measure from one perspective. If the measures had been used together, the three men would have had a more accurate picture of the elephant.

EMPLOYEES SHOULD PERCEIVE THAT PERFORMANCE MEASUREMENT IS IMPORTANT In many organizations, employees have been exposed to a variety of management fads that seem to appear and then fade away as the next fad takes its place. Employees need to know that management is serious and committed to measuring and improving performance.

MANAGEMENT SHOULD DEMONSTRATE THAT PERFORMANCE IS CRITICAL TO ORGANIZATIONAL AND INDIVIDUAL SUCCESS Closely related to the previous principle, this principle observes that not only should employees perceive that performance measurement is important, but also management must demonstrate that performance matters. When management tolerated poor performance in the past and employees see that the new measurement system has not changed the situation (in other words, Joe or Mary still comes to work and reads the paper for most of the day), employees know that performance is not important, despite the new system.

chapter 4

LEARNING AIDS

Performance Measurement Quiz

Circle the correct answer(s).

1. Circle the accomplishments listed below:
   a. A completed, accurate report
   b. Types reports and correspondence
   c. Teamwork
   d. Guidance and technical assistance
   e. Satisfied customers
   f. Answers phones

2. Non-critical elements have to be weighted less than critical elements.
   a. True
   b. False

3. Standards should be written in terms of specific measures.
   a. True
   b. False

4. Which of the following is/are NOT regulatory requirements for critical elements?
   a. Each employee must have a minimum of one critical element
   b. Critical elements must measure individual performance
   c. Critical elements generally can be used to measure team-level performance
   d. Critical elements must have an established standard at least at a *Fully Successful* level
   e. Critical elements must be given greater weight than non-critical elements in deriving a summary level rating

5. Which of the following statement(s) is/are true about feedback?
   a. Peers can be included as sources of input for appraisals
   b. Feedback should be specific
   c. Whether to use 360-degree feedback depends on what you're measuring
   d. Feedback should be timely
   e. Feedback should be given in a manner that will best help improve performance
   f. All of the above are true

chapter 4

6. Performance plans must be built from the employee's position description.
   a. True
   b. False

7. You can't measure results at the individual level.
   a. True
   b. False

8. The four general measures for measuring employee and work unit performance are cost-effectiveness, quantity, timeliness, and:
   a. Flexibility
   b. Quality
   c. Agency strategy
   d. Teamwork

9. Absolute standards can never be used.
   a. True
   b. False

10. A *Fully Successful* standard is a retention standard when (circle one or more):
   a. The standard is used in a Pass/Fail program with critical elements appraised at only two levels
   b. When there is no *Minimally Successful* level available in the appraisal program
   c. None of the above.

11. Measurement should be used for performance improvement.
   a. True
   b. False

ANSWERS ON PAGE 88

Quick Reference: The Eight-Step Process

STEP 1 ***LOOK AT THE OVERALL PICTURE***

Review organizational goals and objectives and performance measures already available. Determine which goals and measures the employee's work unit can affect.

STEP 2 ***DETERMINE WORK UNIT ACCOMPLISHMENTS USING ANY OR ALL OF THE FOLLOWING METHODS:***

METHOD A ***A GOAL CASCADING METHOD***

Cascade the agency's goals to the work unit level. Determine the work unit' s accomplishment(s) that directly affect the organization's goals.

METHOD B ***A CUSTOMER-FOCUSED METHOD***

Determine the product(s) or service(s) that the work unit provides to its customers.

METHOD C ***A WORK FLOW CHARTING METHOD***

Develop a work flow chart for the work unit, establishing key steps(s) in the work process.

STEP 3 ***DETERMINE INDIVIDUAL ACCOMPLISHMENTS THAT SUPPORT WORK UNIT GOALS***

Elements that address individual performance can be identified using a role-results matrix. List the work unit accomplishments across the top of the matrix. List each member of the work unit or each job position down the left side of the matrix. In each cell, list the accomplishment (i.e., performance element) that the member must produce or perform to support the work unit accomplishment. All performance elements should be either quantifiable or verifiable.

STEP 4 ***CONVERT EXPECTED ACCOMPLISHMENTS INTO PERFORMANCE ELEMENTS, INDICATING TYPE AND PRIORITY***

All employees must have at least one critical element. Critical elements must address individual performance only. Work unit performance can be addressed through non-critical or additional elements. In appraisal programs with only two summary levels, work unit performance can be addressed only through additional performance elements.

STEP 5 **DETERMINE WORK UNIT AND INDIVIDUAL MEASURES**

For each element, determine which general measure(s) (i.e., quantity, quality, timeliness, or cost-effectiveness) are important. Determine how to measure the quantity, quality, timeliness, and/or cost-effectiveness for the element. If an accomplishment can be measured with numbers, determine the unit of measurement to be used. If performance can only be described (i.e., observed and verified), clarify who would appraise the work and what factors they would look for.

STEP 6 **DEVELOP WORK UNIT AND INDIVIDUAL STANDARDS**

A *Fully Successful* or equivalent standard must be established for each critical element. If the measure for the element is numeric, determine the range of numbers that would represent *Fully Successful* performance. For critical elements appraised at two levels, the *Fully Successful* standard identifies the level of performance below which performance is *Unacceptable*. For critical elements appraised at more than two levels, establish a range of performance above which special recognition may be warranted and below which a performance problem exists.

If the measure for the element is descriptive, determine what the appraiser would see or report that would verify that performance is *Fully Successful*. For critical elements appraised at two levels, describe performance for that element below which is *Unacceptable* performance. For elements appraised at more than two levels, and for elements for which stretch goals are desired, determine what exceeding expectations would look like. Describe what the appraiser would see happening when expectations are exceeded.

STEP 7 **DETERMINE HOW TO MONITOR PERFORMANCE**

Determine what data to collect for each performance element, which source the data should come from, and whether to collect all the data or just a sample. Determine when to collect the data, who should collect it, and who should receive it. Review existing reports for possible use as feedback reports. Create feedback tables or graphs where appropriate or necessary. Try to design feedback processes that give employees feedback automatically.

STEP 8 ***CHECK THE PERFORMANCE PLAN USING THE FOLLOWING GUIDELINES:***

- Are the critical elements truly critical? Does failure on the critical element mean that the employee's overall performance is unacceptable?
- Is the range of acceptable performance clear? Are the performance expectations quantifiable, observable, and/or verifiable?
- Are the standards attainable? Are expectations reasonable?
- Are the standards challenging? Does the work unit or employee need to exert a reasonable amount of effort to reach a fully successful performance level?
- Are the standards fair? Are they comparable to expectations for other employees in similar positions? Do they allow for some margin of error?
- Are the standards applicable? Can the appraiser(s) use the standards to appraise performance? Can the appraiser(s) manage the data collected through the measurement process?
- Will work units and employees understand what is required?
- Are the elements and standards flexible? Can they be adapted readily to changes in resources or objectives?
- If your program permits appraising elements at levels above the *Fully Successful* or equivalent level, is the *Fully Successful* or equivalent standard surpassable? Is it possible for a work unit's or an employee's performance to exceed it?

Five-Level Appraisal–Examples

THE FOLLOWING EXAMPLES OF ELEMENTS AND STANDARDS WERE WRITTEN SPECIFICALLY FOR APPRAISAL PROGRAMS THAT APPRAISE PERFORMANCE ON ELEMENTS AT FIVE LEVELS.

HUMAN RESOURCES ASSISTANT

ELEMENT	STANDARDS*
CUSTOMER SATISFACTION	**FULLY SUCCESSFUL STANDARD** (To meet this standard, the employee must meet all of the following requirements). As determined by the supervisor through direct observation and/or discussions with several customers and/or peers: • Usually communicates clearly, courteously, and effectively with customers • Routinely responds to each customer request with the most accurate and complete information available. If the information to a telephone call can not be provided immediately upon request, usually provides an answer within 3 working days of receipt of call. Email responses are usually answered within 5 working days. Formal written correspondence is produced within agencywide standards (usually 10 working days) • Generally mails requested information within 3 working days of receipt of request • Whenever possible, elicits customer feedback to improve service • If the employee cannot answer a customer's question completely, he/she generally provides name and phone number for the proper contact. If the question requires additional research, keeps the customer apprised of progress • If requested material is temporarily unavailable to mail to customers, usually notifies the customers when they may expect to receive it **OUTSTANDING STANDARD** Exceeds the *Fully Successful* standard plus two of the following occur: • Receives praise and/or written commendations from customers • On own initiative, assumes and accomplishes a significant amount of work beyond the normal load of assigned duties to achieve customer satisfaction • Proactively communicates with customers to establish good working relationship and assess customer needs • Consistently demonstrates in-depth knowledge of customer programs **MINIMALLY SUCCESSFUL STANDARD** The employee meets the first two requirements listed for *Fully Successful* and of the four remaining requirements, meets all but number(s) 4 & 6 .

Note: We have purposely listed the Minimally Successful standard last to emphasize performance that is Fully Successful and higher more than performance that is less than Fully Successful.

*The standards include measures that can be tracked without using a customer survey. *Exceeds Fully Successful* falls between the performance described for *Fully Successful* and that described for *Outstanding*. *Unacceptable* performance falls below the minimum of *Minimally Successful*.

HUMAN RESOURCES SPECIALIST

ELEMENT	STANDARDS*
HR POLICY PRODUCTS (e.g., written guidance, reports, overviews, workshops, formal presentations)	***FULLY SUCCESSFUL* STANDARD** (To meet this standard, the employee must meet all of the following requirements.) ***QUALITY*** ▌ Written products generally follow plain English principles, including logical organization, descriptive section headings, simple terms, and good use of tables, lists, graphics, and white space ▌ Assigned presentations and workshops are generally well-organized with a logical flow, a use of simple terms, and graphics that illustrate concepts to help audience understanding. The overall audience rating of any presentation given is at least acceptable ▌ Products usually reflect sound analytical thinking and present recommendations consistent with sound HR principles and supportive of Administration initiatives ***QUANTITY*** ▌ Produces (or does significant work for) a) at least one major product (e.g., a workshop; a complex paper or report, often over 10 pages long) b) at least three intermediate-in-scope products (e.g., topic papers 3-10 pages long) c) at least five minor products (e.g., articles or 1-2 page papers) d) a combination of these (To meet the definition of "produces," the report or paper at least must be cleared by the Division Chief.) ***TIMELINESS*** ▌ Draft written products are usually completed and submitted for review by the date agreed to at initial assignment. Revisions are usually done and returned within the agreed-upon time frame ***OUTSTANDING* STANDARD** ▌ Produces more than two major products, more than five intermediate-in-scope products, more than eight minor products, OR a combination of these ▌ Exceeds the quality and timeliness criteria ▌ Plus meets at least three of the following: a) On own initiative, proposes the subject of the product b) Completes extensive research to complete the product c) Develops applicable, understandable models and examples d) Synthesizes complex issues and condenses and explains them so that they are understandable to a general audience e) Product content provides leadership in the program, fits the HR policy into the big picture of management, links HR policy to organizational goals, and/or highlights the links of HR policy with other management functions f) Develops original understandable graphics that illustrate the concept being presented ***MINIMALLY SUCCESSFUL* STANDARD** The employee accomplishes the work described at the *Fully Successful* level except that intermediate and minor products of a routine nature are produced with moderate but not excessive rework.

Note: We have purposely listed the Minimally Successful standard last to emphasize performance that is Fully Successful and higher more than performance that is less than Fully Successful.

**Exceeds Fully Successful* falls between the performance described for *Fully Successful* and that described for *Outstanding*. *Unacceptable* falls below *Minimally Successful*.

MEDICAL RECORDS TECHNICIAN

ELEMENT	STANDARDS*
MEDICAL RECORDS that include accurately filed documentation	***FULLY SUCCESSFUL* STANDARD** (To meet this standard, the employee must meet all of the following requirements.) As determined by the supervisor and from doctor/clinic feedback: ***QUALITY*** ▌ Paperwork is usually filed according to hospital documentation regulations, with only a few errors or complaints ▌ With few exceptions, paperwork is date stamped the same day it arrives in the Medical Records Section ▌ The employee can usually locate records, whether they are in their filing shelves or checked out to doctors/clinics ▌ With few exceptions, medical records requested by a doctor/clinic/emergency room contain the paperwork received by the Medical Records Section within the last 3 working days, with contents usually filed accurately ***QUANTITY*** ▌ The backlog of paperwork to be filed usually does not exceed the amount received within the last 3 working days ***TIMELINESS*** ▌ Medical records are usually supplied to requestors by the time requested. In emergency situations, medical records are supplied consistently within an hour of request ***OUTSTANDING* STANDARD** The employee exceeds the *Fully Successful* standard plus meets all of the following: ▌ On own initiative, systematically reviews assigned files to ensure accuracy of paperwork placement in the file ▌ Very few records are more than three inches thick (i.e., overly thick files have been split into additional volumes) ▌ Voluntarily conducts systematic searches for missing paperwork or records, including verifying checkout cards ▌ At least one of the employee's suggestions for improvements in the filing process or to records management is adopted ▌ Most medical record jackets are in good condition (i.e., torn or worn jackets have been replaced, as supplies allow) ***MINIMALLY SUCCESSFUL* STANDARD** To meet this standard, the employee completes the requirements of the *Fully Successful* standard except that the backlog often exceeds 3 days but usually does not exceed 4 days and the _third_ quality requirement is not met.

Note: We have purposely listed the Minimally Successful standard last to emphasize performance that is Fully Successful and higher more than performance that is less than Fully Successful.

**Exceeds Fully Successful* falls between the performance described for *Fully Successful* and that described for *Outstanding*. *Unacceptable* falls below *Minimally Successful*.

HUMAN RESOURCES SPECIALIST (EMPLOYEE RELATIONS)

ELEMENT	STANDARDS*
TECHNICAL INFORMATION, ADVICE, AND ASSISTANCE	*FULLY SUCCESSFUL* STANDARD ▌ Provides timely and reliable technical advice and assistance to agency and other officials on employee relations and appellate matters. Advice is based on good knowledge and proper application of regulation, precedent cases, and relationships among human resources programs. Discusses advantages, disadvantages, and feasible options in connection with issues and problems presented. Coordinates with other agency offices, as appropriate. Brings unique or potentially difficult issues and problems to the attention of the supervisor with options and recommendations for further action ▌ Gains useful feedback from agencies and other organizations within the agency on the impact of policies and processes under the employee relations program. Provides suggestions on how best to use information and insights to improve employee relations programs and procedures ▌ Thoroughly reviews and provides timely comments on materials presented for review by other offices. Comments take into account applicable regulations, case law, and policy objectives in the areas of employee relations and appellate policies. Training and briefings provided to employees are well conceived, effectively presented, and well received ***OUTSTANDING STANDARD:*** ▌ Is uncommonly effective in dealing with officials who present difficult issues and problems for resolution. Options and recommended solutions are creative, pertinent, and demonstrate an in-depth understanding of the issues. Where appropriate, recites successful practices and programs in other agencies. Displays deep knowledge of HRM policies, precedent cases, agency needs, and the likely impact on management and employees of solution proposed ▌ Based on knowledge and insights, is able to propose significant changes to policies and procedures which hold the potential for improvement ▌ In reviewing the products of other organizations, is able to point out major issues or problems not otherwise foreseen or to make suggestions for significant improvement as warranted ▌ Is able to cause major changes in policies to be considered, where appropriate, through the persuasiveness and thoroughness of written comments and/or informal meetings ▌ Review and commentary is timely, even in the event of competing priorities and large workload ***MINIMALLY SUCCESSFUL STANDARD:*** ▌ Answers to questions about employee relations policies are usually accurate and provided in a timely manner ▌ Regularly gains useful feedback from organizations on agency policies and programs in employee relations. Occasionally surfaces feedback in a manner that is useful to management ▌ As requested, furnishes comments to other offices on proposed policy materials, training courses, and legislation. Comments point out technical inaccuracies or inconsistency with established policy

Note: We have purposely listed the Minimally Successful standard last to emphasize performance that is Fully Successful and higher more than performance that is less than Fully Successful.

**Exceeds Fully Successful* falls between the performance described for *Fully Successful* and that described for *Outstanding*. *Unacceptable* falls below *Minimally Successful*. This example does not include a *Minimally Successful* standard.

ATTORNEY ADVISOR

ELEMENT	STANDARDS*
WRITTEN MATERIALS (e.g., legal memoranda, briefs, and pleadings)	***FULLY SUCCESSFUL* STANDARD** (must meet all of the following) **QUALITY** As determined by the supervisor, written materials • Are generally considered to be of average professional quality • Are infrequently returned for substantial revision • Usually fully analyze relevant legal and policy issues • Usually reflect thorough investigation of factual and legal resources • Usually do not contain significant extraneous or inappropriate material **QUANTITY** • In most instances, written materials are developed as needed **TIMELINESS** • Written materials are generally completed and presented in accordance with established deadlines or time frames ***OUTSTANDING* STANDARD** (must meet all of the following) Written materials: • Are routinely considered to be of highest professional quality • Are rarely returned for substantial revision • Consistently fully analyze relevant legal and policy issues • Reflect thorough investigation of factual and legal resources • Do not contain significant extraneous or inappropriate material • Are completed before established deadlines or time frames • Are always completed as needed

**Exceeds Fully Successful* falls between the performance described for *Fully Successful* and that described for *Outstanding*. *Unacceptable* falls below *Minimally Successful*. This example does not include a *Minimally Successful* standard.

NOTE: We have purposely left out a Minimally Successful standard in this example to emphasize performance that is Fully Successful and higher. In the event that an employee's performance fell below the Fully Successful level, a Minimally Successful standard would be established and communicated.

Three-Level Appraisal–Examples

THE FOLLOWING EXAMPLES OF ELEMENTS AND STANDARDS WERE WRITTEN SPECIFICALLY FOR APPRAISAL PROGRAMS THAT APPRAISE PERFORMANCE ON ELEMENTS AT THREE LEVELS.

TEAM LEADER, PACKAGING PRODUCTION TEAM

ELEMENT	FULLY SUCCESSFUL STANDARD* (To meet the *Fully Successful* standard for an element, all of the bullets listed for the element must be met.)
Quality products	▎Usually 90% to 95% of pallets have no defects ▎With few exceptions, no more than 1.5 to 2 hours of down time per week ▎Normally, the packaging production schedule is met 5 out of 7 days ▎Normally, the shipment schedule is met 5 out of 7 days
Safe work environment	▎Safety problems are corrected or improvements usually are made by agreed-on date ▎Routinely holds one safety audit per week ▎Very rarely has any lost time hours
Effective leadership	▎Team goals are met 60-80% of the time ▎Manager judges that the team leader periodically initiates ways to reduce costs ▎Manager judges that decisions are well thought out and support organizational goals.
Productive subordinates	Manager is generally satisfied that: ▎Training requirements of the team are met ▎Discipline is provided fairly and consistently ▎Most team members understand the department's goals and how their performance affects these goals ▎Team members understand how they're performing against their goals ▎Team members receive rewards for good performance

*To achieve the *Outstanding* level, the employee must consistently exceed a majority of the bullets listed for the *Fully Successful* standard. *Unacceptable* performance occurs when the employee fails to meet one or more of the bullets listed for *Fully Successful* performance.

PROGRAM ANALYST

ELEMENT: ORAL PRESENTATIONS

STANDARDS* (To meet a standard, all of the statements listed for the standard must be met.)

OUTSTANDING STANDARD

When attendee evaluations are available:

- Sixty to eighty-four percent of attendees rated the employee's presentation good or very good.

When attendee evaluations are not available, the supervisor determines that the employee:

- Presents information in a clear, concise, and well-organized manner
- Responds well to questions, including unanticipated ones
- Creates a favorable impression for effective communication by seeking the views of others and respecting different points of view
- Asks probing questions to ensure that everyone understands the matters discussed
- Clearly distinguishes between fact and opinion and avoids disclosing sensitive or tentative information prematurely
- Listens well, responds appropriately and articulately, and remains calm in adverse situations
- Knows when and how to use visual aids, speaks authoritatively on subject matter , and displays ability to respond directly to questions raised
- Encourages active participation by others
- Senses audience's receptivity to presentation and adjusts accordingly
- Shows thorough knowledge of issues and their relationship to broader issues
- Presents technical information clearly and persuasively, demonstrating the importance and relevancy of planning.

FULLY SUCCESSFUL STANDARD

When attendee evaluations are available:

- More than 60-84% of attendees rated the employee's presentation good or very good

When attendee evaluations are not available, the supervisor determines that the employee:

- Usually presents information clearly, concisely, and in a well-organized manner
- Routinely shows respect for comments of participants
- Generally keeps discussion on track
- Usually elicits comments of others
- Generally weighs consequences of statements before speaking, clearly distinguishing between fact and opinion, and avoids disclosing sensitive or tentative information prematurely
- Usually listens well, responds to issues at hand, and minimizes extraneous information
- Usually answers most questions and invites additional questions to ensure understanding

**Unacceptable* performance occurs when the employee fails to meet one or more of the bullets listed for *Fully Successful* performance.

GRAPHICS DESIGNER

ELEMENT: GRAPHIC DESIGNS

STANDARD

OUTSTANDING STANDARD

In addition to meeting all criteria of the *Fully Successful* standard, the supervisor determines that the employee meets at least four of the following:

- Designs are often of such high quality that they generate spontaneous praise from clients
- The elegance of designs often enhances their purpose in unexpected ways
- Designs consistently reflect the highest professional standards and raise the standards for other agency designers
- The most complex design tasks are handled with little or no difficulty
- Suggestions are made that improve the agency's design processes
- Potential problems are anticipated, brought to the supervisor's attention as appropriate, and usually solved independently

FULLY SUCCESSFUL STANDARD

To meet this standard, all of the following must be met:

The supervisor determines that:

- The quality of information-material design is usually acceptable to the client and sufficient to achieve the purposes intended
- In most cases, designs are in accordance with the agency's graphic standards system and meet commonly accepted criteria for professional work
- Logical planning, due consideration of priorities, and efficient application of technical graphics skills usually result in creation of graphic designs in time to meet reasonable deadlines
- Generally nonwasteful work habits reflect a consideration of costs to the Government
- Instructions from supervisors are most often followed as given, major revisions are rarely necessary, and routine problems are usually resolved with a minimum of supervision

TRAINING COORDINATOR

ELEMENT	FULLY SUCCESSFUL STANDARD* (To meet the *Fully Successful* standard for an element, **all** of the bullets listed for the element must be met.)
CERTIFIED PROGRAMMERS	Most of the supervisors of certified programmers say that the trained programmer(s): • Could handle their assignments right away • Didn't bother coworkers and supervisor for covered objectives • Demonstrated certified skill/knowledge assessment was accurate Recommended trainees generally complete the training within the following time frames: • Average of 18 to 25 working days to complete Phase I training • Average of 18 to 23 working days to complete Phase II training • Average of 10 to 15 working days to complete Phase III training Most of the supervisors of the trained programmers say that the topics covered match what is needed on the job
TRAINING PLANS	• Most internal customers agree that the training plan will meet their needs and commit dollars and trainee time • Supervisor is generally satisfied that the training plan contains standard components, has realistic time lines and objectives, is based on input from representative sample, and is consistent with agency long-range goals, objectives, and philosophy • The incumbent meets agreed-upon deadline for first approved draft
CROSS-TRAINED ANALYSTS	• 60%-80% trainees meet learning objectives • Trainees' supervisors are generally satisfied with analysts' improvement in their ability to communicate with programmers and solve minor problems without a programmer
TRAINING FACILITY READY FOR TRAINING	The supervisor is generally satisfied that: • The training room is ready for training when needed • Materials are available • Speaker's needs have been determined and addressed
CUSTOMER SERVICE MANUAL	The supervisor is generally satisfied that the manual: • Covers most if not all job dimensions • Has most if not all standard components • The customer service supervisor says the document is useful

*To achieve the *Outstanding* level, the employee must consistently exceed a majority of the bullets listed for the *Fully Successful* standard. *Unacceptable* performance occurs when the employee fails to meet one or more of the bullets listed for *Fully Successful* performance.

Two-Level Appraisal–Examples

THE FOLLOWING EXAMPLES OF ELEMENTS AND STANDARDS WERE WRITTEN SPECIFICALLY FOR APPRAISAL PROGRAMS THAT APPRAISE PERFORMANCE OF ELEMENTS AT ONLY TWO LEVELS.

POLICY PROCESSING CLERK

ELEMENT	***FULLY SUCCESSFUL STANDARD*** (To meet the *Fully Successful* standard for each element, **all** of the bullets listed for the element must be present or occur.)
COMPLETED AUDITS	▌No more than 5 errors per month are found on audits ▌For at least 10 weeks per year, no audits are more than 30 days old
QUOTES AND PROPOSALS	▌No more than 5 quotes and proposals per month are found to be inaccurate at issuing ▌No more than 5 quotes per month are processed in more than 5 days ▌No more than 5 proposals per month are processed in more than 24 hours
SOLUTIONS	▌No more than 2 times per quarter are incorrect results or procedures spotted by the supervisor or other team members ▌No more than 2 times per quarter are problems corrected in more than 3 business days
FINISHED POLICIES	▌No more than 5 errors per month are spotted by team members ▌No more than 5 times per month when someone can't do the next step on a policy due to illegibility, incompleteness, or vagueness in the file ▌No more than 3 times per month someone on the team gets a second call for the same issue/problem ▌For at least 10 weeks per year, there are no changes more than 30 days old ▌For at least 5 weeks per year, there is no new business more than 10 days old
ANSWERS TO QUESTIONS	▌60% of surveyed team members and a sample of people outside the team say: — The technician stops what (s)he's doing and immediately tries to answer the question — They don't find out later that the answer is wrong — If the technician doesn't know the answer, (s)he either researches the solution or directs the person to the correct source

RESEARCH CHEMIST

ELEMENT	***FULLY SUCCESSFUL STANDARD*** (To meet the *Fully Successful* standard for each element, **all** of the bullets listed for the element must be present or occur .)
ANALYTICAL RESULTS AND SPECIFICATIONS	The Research Manager is routinely satisfied that: ▌The method measures the appropriate variable ▌The results are relevant ▌The method is scientifically sound ▌There is a well-written protocol ▌The method is accurate, precise, reproducible, fast, and cost-effective The customer is generally satisfied that: ▌They can understand and observe the results ▌The cost is within the budget ▌The information gives understandable answers to their questions
SOLUTIONS TO CUSTOMER PROBLEMS	The Research Manager is routinely satisfied that: ▌Reports and solutions address the question that was asked ▌The assumptions or hypotheses are based on scientific principles ▌The proposed solutions, suggestions, and/or recommendations are understandable ▌The recommendations were provided within the agreed-on time frame. The customer is generally satisfied that: ▌The report and any answers to questions address the question that was asked ▌The proposed solutions, suggestions, and/or recommendations are understandable ▌The proposed recommendations were provided within the agreed-on time frame ▌The solutions work ▌The information gives understandable answers to their questions ▌They are able to implement the recommendations

ENGINEER

ELEMENT	FULLY SUCCESSFUL STANDARD (To meet the *Fully Successful* standard for each element, **all** of the bullets listed for the element must be present or occur .)
DESIGNS FOR CAPITAL IMPROVEMENTS AND OPERATIONS CHANGES	The supervisor is routinely satisfied that: ▎The cost estimate is sufficiently itemized ▎There is backup documentation for all cost estimates ▎There is consistency across design documents ▎The design looks like it will solve the problem or meet the need ▎The design doesn't cause new problems while solving the original problem In addition: ▎There is no significant cost overrun due to inaccurate quantities ▎The design is routinely completed by the agreed-on deadline
BUDGET REPORT	▎The budget report is generally submitted by the fifteenth day of the month ▎The engineer is routinely able to answer questions about project financial status at any time
COMPLETED PROJECTS	The supervisor is routinely satisfied that: ▎The project is constructed according to the design ▎Unexpected conditions are successfully worked around ▎Recommendations are made by agreed-on deadline ▎The contract cost is within 5% of the estimate

PROGRAM ANALYST (BUDGET)

ELEMENT	***FULLY SUCCESSFUL STANDARD*** (To meet the *Fully Successful* standard for each element, **all** of the bullets listed for the element must be present or occur .)
BUSINESS DECISION RECOMMENDATIONS, INCLUDING BUDGET ANALYSIS AND COST INFORMATION/ANALYSIS	The supervisor is routinely satisfied that: ▎Cost impacts surrounding the decision have been identified and evaluated ▎The numbers are accurate and do not require second-guessing or rework ▎Reports/analysis logically state the issues and reach conclusions that are supported by the data and analysis ▎The analysis is useful and answers the question asked ▎The analysis/information was provided by the agreed-on deadline
FINANCIAL SYSTEMS IMPROVED	The supervisor as well as the users of the system are generally satisfied that: ▎The system change is within the scope of control ▎The change provides information in a more efficient, accurate, and useful manner than previously ▎The time required to implement the change meets the customer's needs and deadlines ▎The value of the improvements exceeds the cost of the implementation
BUDGET PROCESS EVALUATION AND ANALYSIS	The supervisor is routinely satisfied that: ▎The reports/analysis logically state the issues and reach conclusions that are supported by the data and analysis ▎The evaluations address all issues and cost impacts

notes

answers from page 19

TRAINS EMPLOYEES— *ACTIVITY,* ***SUPERVISION—*** *CATEGORY,* ***A COMPLETED CASE—*** *ACCOMPLISHMENT,* ***PUBLIC RELATIONS—*** *CATEGORY,* ***RECOMMENDATIONS—*** *ACCOMPLISHMENT,* ***CUSTOMER SERVICE—*** *CATEGORY,* ***HR POLICY INTERPRETATIONS—*** *ACCOMPLISHMENT,* ***WRITES AGENCY POLICY—*** *ACTIVITY,* ***SOLUTIONS TO PROBLEMS—*** *ACCOMPLISHMENT,* ***DEVELOPS SOFTWARE PROGRAMS—*** *ACTIVITY,* ***IDEAS AND INNOVATIONS—*** *ACCOMPLISHMENT,* ***FILES PAPERWORK—*** *ACTIVITY,* ***WRITES MEMOS—*** *ACTIVITY,* ***COMPUTER SYSTEMS THAT WORK—*** *ACCOMPLISHMENT,* ***TEAMWORK—*** *CATEGORY,* ***A COMPLETED PROJECT—*** *ACCOMPLISHMENT,* ***SATISFIED CUSTOMERS—*** *ACCOMPLISHMENT,* ***ANSWERS THE PHONE—*** *ACTIVITY,* ***ASSISTS TEAM MEMBERS—*** *ACTIVITY*

answers from pages 70-71

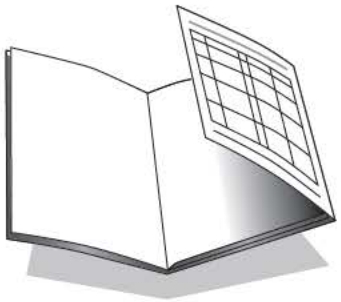
1— *A D E*
2— *B*
3— *A*
4— *C E*
5— *F*
6— *B*
7— *B*
8— *B*
9— *B*
10— *A B*
11— *A*

notes

notes

Please cut at this line. Line does not print

FOLD OVER INSIDE BACK COVER FLAP AS SHOWN TO FILL OUT CHART.
SEE PAGES 46, 51, 60, AND 66 FOR FURTHER INSTRUCTIONS



PRIORITY POINTS	*ELEMENT*	*TYPE*	*GENERAL MEASURE*	*SPECIFIC MEASURE*	*STANDARDS AND FEEDBACK*

Please cut at this line. Line does not print

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Guidance for Agency-Specific Diversity and Inclusion Strategic Plans

November 2011

a New Day for Federal Service

Table of Contents

Introduction

This Guidance on implementation of the Government-Wide Diversity and Inclusion Strategic Plan (the Guidance) provides agencies with direction to enable them to fulfill the goals identified in Executive Order 13583 and coordinate their diversity and inclusion efforts within the agency in a collaborative and integrated manner. Currently, in many agencies, human resource (HR) programs collect workforce data, advise management in making personnel decisions, and submit reports to the Office of Personnel Management (OPM). Equal employment opportunity (EEO) programs manage the discrimination complaint process, track data, identify potential barriers, and submit reports to the Equal Employment Opportunity Commission (EEOC). To deliver excellent service to the public through a skilled, engaged, and diverse workforce, HR, EEO, and diversity and inclusion (D&I) must work collaboratively and share data and information. Further, agencies that draw on the unique knowledge and expertise possessed by all three programs are better able to achieve the goal of becoming a model workplace. This guidance provides a path forward, drawing from leading practices identified by Federal, state, and private sector models of collaboration.

The Guidance is separated into two sections. Section 1 provides operational guidance and sets forth the roles, responsibilities, and requirements applicable to Federal agencies that will facilitate their successful execution of actions outlined in Executive Order 13583. Section 2 provides specific guidance to Federal agencies that will enable them to bring themselves into alignment with the priorities and actions outlined in the Government-Wide Diversity and Inclusion Strategic Plan (the Plan). In this section, each goal is listed along with its associated priorities and action items. Section 2 also provides guidance on possible measurements for the actions. The Office of Personnel Management, in coordination with the Office of Management and Budget (OMB) and the Equal Employment Opportunity Commission (EEOC), will continue to refine these measurements and provide additional guidance for agencies in subsequent issuances. Finally, in the conclusion of this Guidance, Federal departments and agencies are provided a pathway to connecting diversity and inclusion with innovation.

Below are the definitions, vision and mission statements, and goals from the Government-Wide Diversity and Inclusion Strategic Plan (the Plan).

Definitions of “Diversity” and “Inclusion”

Throughout this document, we define workforce diversity as a collection of individual attributes that together help agencies pursue organizational objectives efficiently and effectively. These include, but are not limited to, characteristics such as national origin, language, race, color, disability, ethnicity, gender, age, religion, sexual orientation, gender identity, socioeconomic status, veteran status, and family structures. The concept also encompasses differences among

people concerning where they are from and where they have lived and their differences of thought and life experiences.[1]

We define inclusion as a culture that connects each employee to the organization; encourages collaboration, flexibility, and fairness; and leverages diversity throughout the organization so that all individuals are able to participate and contribute to their full potential.

Federal Government-Wide Diversity and Inclusion Vision Statement

Be the Nation's model employer by leveraging diversity and fostering inclusion to deliver the best public service.

Federal Government-Wide Diversity and Inclusion Mission Statement

Recruit, retain, and develop a diverse, high-performing Federal workforce that draws from all segments of society and values fairness, diversity and inclusion.

Goals:

1. Workforce Diversity. Recruit from a diverse, qualified group of potential applicants to secure a high-performing workforce drawn from all segments of American society.

2. Workplace Inclusion. Cultivate a culture that encourages collaboration, flexibility, and fairness to enable individuals to contribute to their full potential and further retention.

3. Sustainability. Develop structures and strategies to equip leaders with the ability to manage diversity, be accountable, measure results, refine approaches on the basis of such data, and institutionalize a culture of inclusion.

The three goals listed above are absolutely necessary for the successful growth of diversity and inclusion. Other characteristics of diversity and inclusion best practice plans, such as leadership, accountability, measurement, and training are components of, and integrated in, the three goals.

[1] Data on all the characteristics listed in this definition of diversity is not collected. However, OPM, in coordination with OMB, EEOC, and DOJ, will continue to refine existing measurements and provide additional guidance for agencies in subsequent issuances.

Section 1

Operational Guidance

This operational guidance sets forth the roles, responsibilities, and requirements applicable to Federal agencies in successfully executing actions outlined in Executive Order 13583. Successful implementation of the Government-Wide Diversity and Inclusion Strategic Plan (the Plan) will help each agency achieve its diversity and inclusion objectives for the American people. Notably, the priorities outlined in the Plan will succeed only with the strong support of leaders, managers, and supervisors, as well as a coordinated and collaborative approach within HR, EEO and D&I functions. Further, because of the complexity of the relevant legal landscape, agencies should consult with their General Counsels when crafting and implementing their individual strategic plans, to ensure compliance with law.

Agency Guidance:

A) Pursuant to Executive Order 13583, section 3(a), each Agency will designate the Chief Human Capital Officer (CHCO) as the responsible official for enhancing employment and promotion (employee life cycle processes) goals of the Government-Wide Diversity and Inclusion Strategic Plan, in collaboration with the agency's Director of Equal Employment Opportunity and Director of Diversity (also known as the Chief Diversity Officer (CDO)), if any, including the development and implementation of the agency-specific Diversity and Inclusion Strategic Plan.

1. The agency will ensure that the EEO Director reports to the Head of the Agency, or his or her designee, and is not a direct report to the CHCO.

2. The role of CDO may be a separate or distinct role, or it may be held by the EEO Director or the CHCO. [2]

[2] Executive Order 13583 does not require agencies to designate a separate Director of Diversity or a Chief Diversity Officer. Our research has shown, however, that having three separate functions – Human Resources (HR), EEO and Diversity and Inclusion - has worked very well in the private sector and in those Federal agencies that have followed this tri-partite model. Where HR, EEO and Diversity and Inclusion work together as teams rather than competitors, organizations experience the best outcomes, and this is the model we recommend.

3. The agency will assign Human Resources to lead workforce planning.

4. The agency will assign EEO to lead barrier analysis.[3]

5. The agency's General Counsel or other chief legal officer shall ensure that agency specific plans are in compliance with laws, rules and regulations that make it unlawful for agencies to discriminate for or against an applicant or employee based on race, color, religion, sex (including pregnancy or gender identity), national origin, age, disability, sexual orientation or any other prohibited basis.

B) The CHCO, EEO, and CDO (if any) roles and responsibilities are dependent upon the unique needs, reporting structures, current laws, policies, regulations, and strategies utilized by the respective agency. (*See* Appendix A for a roles and responsibility matrix that identifies functional responsibilities of the CHCO, EEO, and Diversity and Inclusion functions).

C) 120 days after the issuance of Government-Wide Diversity and Inclusion Strategic Plan, each agency will submit to OPM and OMB an agency-specific Diversity and Inclusion Strategic Plan, which it shall then implement. The plan shall:

1. Outline the actions that will be taken to achieve the specific priorities identified in the Government-Wide Diversity and Inclusion Strategic Plan.

2. Identify a responsible management official for each action.

3. Be consistent with applicable law, the agency's Strategic Human Capital Plan, merit system principles, EEOC Management Directive 715 (MD-715) and other applicable workforce planning strategies, including but not limited to those prescribed in 5 CFR Part 250, Subpart B.

[3] As used in this guidance, "barrier analysis" refers to the process described in EEOC Management Directive 715. That Directive provides that "[w]here an agency's self-assessment indicates that a racial, national origin, gender, [or disability] group may have been denied equal access to employment opportunities, the agency must take steps to identify the potential barrier. Workplace barriers can take various forms and sometimes involve a policy or practice that is neutral on its face. Identifying and evaluating potential barriers requires an agency to examine all relevant policies, practices, procedures and conditions in the workplace." EEOC's Management Directive 715 (MD-715). For more information, see http://www.eeoc.gov/federal/directives/md715.cfm.

a. Agencies utilizing existing plans should modify plans to ensure alignment with the Government-Wide Diversity and Inclusion Strategic Plan goals and priorities.

b. Agencies that do not have Diversity and Inclusion Strategic Plans will develop plans that are in alignment with the Government-Wide Diversity and Inclusion Strategic Plan.

c. At a minimum:

1. The agency plan should incorporate the three Goals and seven Priorities established by the Government-Wide Diversity and Inclusion Strategic Plan.

2. Agencies are encouraged to employ the actions identified within the Government-wide Diversity and Inclusion Strategic Plan, as these actions will be utilized as part of the Measurement Indices currently under development.

D) OPM will review agency-specific Diversity and Inclusion Strategic Plans for alignment with the Government-Wide Diversity and Inclusion Strategic Plan and provide recommended modifications for agency consideration.

E) Agencies will use the Diversity and Inclusion Dashboard which OPM develops as the reporting mechanism to submit progress reports to OPM. [4]

[4] OPM, in coordination with OMB, EEOC and the President's Management Council, is currently in the process of developing a diversity and inclusion dashboard that will provide appropriate measures of agencies' progress in implementing their agency-specific strategic plans. OPM will provide reporting requirements under separate cover.

Section 2

Goal 1: Workforce Diversity…Draw from All Segments of American Society

Federal agencies shall recruit from a diverse, qualified group of potential applicants to secure a high performing workforce drawn from all segments of American society.

Workforce diversity is the first goal in the Government-Wide Diversity and Inclusion Strategic Plan and is grounded in the merit principle that: "Recruitment should be from qualified individuals from appropriate sources in an endeavor to achieve a workforce from all segments of society" while avoiding discrimination for or against any employee or applicant on the basis of race, color, religion, sex (including pregnancy or gender identity), national origin, age, disability, sexual orientation or any other prohibited basis. (5 U.S.C. 2301(b)(1), 2302(b)).

Analysis of Future Workforce Needs

Effective and efficient human capital management enables agencies to have a greater alignment of policies and programs with mission objectives. Workforce planning is a systematic approach to understanding the environment and the challenges in the people issues of an agency which impact mission achievement. To develop strategies to attract and retain high performers to accomplish organizational mission, agencies must: 1) understand their current Federal workforce, 2) project the number and competencies required for the future, and 3) understand the current and future composition of the civilian labor force and/or relevant civilian labor force.[5]

[5] As used in this guidance, the term "Civilian Labor Force" means the subset of Americans who are currently employed or are seeking employment and are eligible to work. The "Relevant Civilian Labor Force" (RCLF) is the CLF data that is directly comparable (or relevant) to the workforce population being studied. For example, if we were analyzing the representation of women as engineers in the Federal workforce, we might compare that representation with the percentage of women who are engineers in the CLF. In this example, the women engineers in the CLF represent the RCLF. For more information, see http://www.opm.gov/feorp01/DCAD.asp and http://www.census.gov/hhes/www/eeoindex/page_c.html.

Meeting and projecting future Federal workforce needs in a difficult budget environment presents challenges. However, demands for ever increasing innovation and greater efficiency provide agencies with an opportunity to make a strong case for building a diverse workforce.

For example, from 2008 to 2010, a study of hiring trends across Federal agencies showed that IT and cybersecurity professionals, nurses, contract and acquisition specialists, border patrol agents, and program analysts were among the top 15 most hired positions within government. In each of these fields, research shows that hiring with an emphasis on cultural, experiential, and cognitive diversity will ensure agencies have a workforce that is capable of addressing increasingly complex challenges more efficiently. Beyond traditional measures of diversity, seeking individuals with varying degree types and professional experience will also benefit agencies and offices across government.

Workforce planning data and analysis—including knowledge about the demographics of the current workforce, projections of attrition for the next 3-5 years, skills and competencies needed to perform the job, effectiveness of succession plans, projected demographics and anticipated changes in served populations—enable leaders to make informed decisions to attract, build and retain inclusive teams to serve customers and stakeholders.

Steps for Integration of Diversity and Inclusion into Workforce Planning

1. **Establish the Strategic Direction.** Align the workforce planning process with the agency's strategic plan, annual performance and business plans and work activities.

2. **Analyze the workforce.** Conduct an analysis of the current and future workforce for the mission critical occupations in coordination with HR, EEO and Diversity and Inclusion to then conduct a barrier analysis. For more information on barrier analyses, see EEOC's EEO Management Directive 715, at http://www.eeoc.gov/Federal/directives/md715.cfm.

    a. Project attrition rates for the next 3-5 years.
    b. Project promotion opportunities to fill gaps for positions requiring experience.

3. **Develop the Competency Action Plan.** Analyze the future skills and competencies needed for mission critical occupations.

4. **Implement Workforce Plan.**

    a. Conduct a comparative analysis between the current supply and demand (projected need) to determine projected requirements.
    b. Use analysis to develop actions in outreach, recruiting, hiring, retaining, developing and promotion activities.

c. Establish internal controls or checks for fairness and advancing inclusion in workforce policies and practices.

5. **Evaluate and Measure.** Assure linkage of workforce planning to accountability system and processes.

For more information about workforce planning, see OPM's End-to-End Hiring Initiative at http://www.opm.gov/publications/EndToEnd-HiringInitiative.pdf, p.p. 11-17.

Priorities, Actions, and Sample Practices for Goal 1

Priority 1.1: Design and implement strategic recruitment and outreach to reach all segments of society.

Actions:

1. Collect and analyze applicant flow data.[6]

2. Coordinate outreach and recruitment strategies to maximize ability to recruit from a diverse, broad spectrum of potential applicants, including a variety of geographic regions, academic sources, and professional disciplines.

3. Ensure that outreach and recruitment strategies designed to draw from all segments of society, including but not limited to those who are underrepresented,[7] are employed when using staffing flexibilities and alternative hiring authorities.

4. Develop strategic partnerships with a diverse range of colleges and universities, trade schools, apprentice programs, and affinity organizations from across the country.

[6] Rigorous collection of applicant flow data is a key to crafting effective recruitment strategies. On March 3, 2010, OPM and EEOC issued a joint memorandum (Available at: http://www.chcoc.gov/Transmittals/TransmittalDetails.aspx?TransmittalID=2920) supporting the collection of demographic data, "including applicant flow data, because such collection is an integral part of the barrier identification process described in [EEOC's Management Directive] 715." OPM also strongly supports the collection of this data because it is a necessary component for effective workforce planning. A form for collecting applicant data has been approved by the Office of Management and Budget (OMB) and is available at: http://www.eeoc.gov/federal/upload/OMB-3046-0046.pdf.

[7] Underrepresentation, as defined in 5 CFR 720.202, "means a situation in which the number of women or members of a minority group within a category of civil service employment constitutes a lower percentage of the total number of employees within the employment category than the percentage that women or the minority group constitutes within the civilian labor force of the United States. . ."

5. Involve managers and supervisors in recruitment activities and take appropriate action to ensure that outreach efforts are effective in addressing barriers.

6. Review and ensure that student internship and fellowship programs have diverse pipelines to draw candidates from all segments of society.

Measurements:

- Review applicant flow data to determine whether outreach and recruitment efforts are effectively reaching all segments of society.
- Measure percentage of qualified applicants from various hiring authorities used by the agency within the past 12 months by demographic group.
- Enter into strategic partnerships and memorialize relationships with the following: colleges and universities, trade schools, apprentice programs, and affinity organizations from all parts of the country.
- Measure applicant flow data to determine whether applicant pools are reflective of the relevant civilian labor force (RCLF).
- Measure percentage of managers and supervisors involved in recruitment activities and outcomes of outreach efforts to all segments of society.
- Review applicant flow data of agency internship program to determine whether applicant pools are reflective of the relevant civilian labor force (RCLF).
- Review applicant flow data of agency Presidential Management Fellows to determine whether applicant pools are reflective of the relevant civilian labor force (RCLF).
- Measure percentage of interns converted and/or hired for permanent employment.

Sample practices for Priority 1.1:

CHCOs, in collaboration with appropriate offices and senior managers, should design and perform strategic outreach to, and recruitment of, communities identified as underrepresented, as well as other communities as appropriate. Below are sample practices for conducting strategic outreach and recruitment:

- Use recruiters who possess the cultural competency necessary to communicate effectively with underrepresented groups.

- Create a diverse integrated recruitment team under which the recruiting function is centralized to plan and coordinate its campaigns. This central group works with agency contacts nationwide to take full advantage of local assets, including staff and managers who can serve as recruiters at local events.

- Generate and disseminate quarterly Workforce Diversity and Inclusion Reports to agency leadership conveying progress/status of organizational workforce diversity, in

order to ensure that outreach and recruitment strategies are effective. Furthermore, interact regularly with hiring managers and supervisors and make them aware of the agency's strategic human capital plan.

- Connect with university disability support service offices to find qualified individuals with disabilities; and conduct campus visits and one-on-one interviews with the university disability support center.

- Utilize Federal Student Service Ambassadors as a peer-to-peer marketing strategy. Use ambassador programs to tap college students who have successfully completed internships to send these former interns back to their campuses as public service emissaries, who host educational visits from agency representatives, promote job and internship opportunities to classmates, share their intern experience and meet with key staff and faculty to bolster the government's effort in recruiting young people.

- Post advertisements and job announcements in locations, and through multiple technologies, that are likely to reach underrepresented groups.

- Hold Outreach Forums and job fairs in conjunction with human resources staff where the agency recruiters interface with organizations and the community.

- Foster early talent detection through the adoption of schools where there is a broad diverse student population.

- Partner with diverse professional organizations and diverse institutions of postsecondary education to identify networking opportunities, student/staff exchange programs and rotational assignments to expand the pipeline to agency employment; Designate Executive Sponsors to build strong, active relationships with these organizations.

- Utilize diversity focused student internship and fellowship programs where underrepresentation exists as identified by barrier analysis conducted in the agency's MD-715 Report.

- Utilize employee resource groups (ERGs) and affinity groups to assist in outreach to diverse organizations.

Priority 1.2: Use strategic hiring initiatives for people with disabilities and for veterans, conduct barrier analyses, and support Special Emphasis Programs, to promote diversity within the workforce.

Actions:

1. Review results of barrier analysis required by MD 715 (if any), develop action plans to eliminate any identified barrier(s), and coordinate implementation of action plans.

2. Use Schedule A hiring authority for people with disabilities and Veteran Hiring Authorities as part of strategy to recruit and retain a diverse workforce.

3. Support Special Emphasis Programs (SEPs) and appoint SEP Managers as advisors on hiring, retaining and promoting a diverse workforce.

Measurements:

- Measure percentage of hires under the Schedule A hiring authority for people with disabilities.
- Measure percentage of hires under Veteran Hiring Authorities within the past 12 months.
- Evaluate outcomes of SEPs and the quality of engagement of SEP Managers in the recruitment outreach, retention, and promotion process in collaboration with human resources staff.

Sample practices for Priority 1.2:

The CHCO, EEO Director, and CDO (if any) should partner in reviewing and modifying the agency's existing HR policies, specifically by performing, at a minimum, the following actions—

- Modifying the agency's outreach and recruitment methods, to ensure that job advertisements are reaching a diverse audience.

- Eliminating job or promotion criteria that are not job related and consistent with business necessity.

- Ensuring to the greatest extent possible that a diverse group of individuals are involved in individual selection, promotion and award decisions.

Below are sample practices for implementing Priority 1.2:

- Utilize automated programs that prepare the agency's MD-715 Report in its totality and provide specific data on diversity in narrative, as well as graphic formats. Such data can be utilized to identify where variances exist between the agency's workforce and the Civilian Labor Force (CLF) or the Relevant Civilian Labor Force (RCLF), and share that information with managers.

- Conduct barrier analyses consistent with MD-715 with respect to various terms and conditions of employment (*e.g.*, hire, promotion, training, leadership development, separation, discipline, awards, *etc.*).

- Use OPM's Shared Register of Candidates with Disabilities. OPM, in collaboration with the Chief Human Capital Officer (CHCO) Council, has established a shared register of individuals with disabilities who have an interest in working for Federal agencies and who satisfy the requirements of positions Federal agencies are frequently required to fill. Agencies that wish to access the register or that have questions should contact their human capital office.

- For more information about hiring under Schedule A for people with disabilities, see Model Strategies for Recruitment and Hiring of People with Disabilities as Required under Executive Order 13548 at: http://www.chcoc.gov/Transmittals/TransmittalDetails.aspx?TransmittalID=3228#Attachment1.

- Use the updated SF 256, Self-Identification of Disability, as a tool to measure progress toward hiring people with disabilities by resurveying the workforce at least every other year to request that people with disabilities self-identify. The form is available at: http://www.opm.gov/forms/pdf_fill/sf256.pdf.

- For information about hiring Veterans, and Executive Order 13518, which established the Veterans Employment Initiative, see the Feds Hire Vets website at: http://www.fedshirevets.gov/hire/hrp/regs/index.aspx.

- Pursuant to 29 C.F.R. 1614.102(b)(4), appoint full-time Special Emphasis Program Managers (SEPMs) (e.g., People with Disabilities Program, Federal Women's Program and Hispanic Employment Program) to address employment initiatives and programs, grade these positions commensurate with the work performed, adequately fund the programs, and ensure access to leadership. *See* appendix C for a model SEPM position description.

- Create SEP committees for various diverse groups as needed to address underrepresentation, utilizing agency-wide staff in field components to expand the reach of SEPs; and gather information from employee affinity and resource groups.

Goal 2: Workplace Inclusion…Include All Federal Employees

Federal agencies shall cultivate a culture that encourages collaboration, flexibility, and fairness to enable individuals to contribute to their full potential.

The merit system principles directly advocate that "the Federal workforce should be used efficiently and effectively." [5 USC 2301(b)(5)]. The workplace inclusion goal focuses on the reality that a diverse workforce alone is no guarantee to organizational productivity or to employees reaching their full potential. Inclusion strategies are the necessary link to harness and leverage the potential inherent in all diverse workforces. Studies have shown that, absent the facilitating conditions in the workplace (*i.e.*, inclusion strategies), workforce diversity will not yield the promised performance benefits.[8] The inclusion emphasis is also an important component of the employee lifecycle stages of retaining, developing, and promoting.

Analysis of Workforce Environment

Employee satisfaction and commitment are two necessary ingredients in developing high-performing organizations and attracting and retaining top talent. Creating an organizational culture that respects and values diversity and inclusion is a business imperative that is critical to the continued success of the Federal government.[9]

Ensuring that diversity and inclusion permeates an organization helps drive performance, productivity and mission success.[10]

- Performance – D&I drives innovation and creativity. In studies and research, diverse teams are better at problem solving, better at critical analysis, and more innovative as they introduce new perspectives and ideas and learn how to be flexible and adaptable in working with one another.

- Productivity – D&I fosters a culture that respects and values each employee and his or her contributions; provides opportunity; and increases individual commitment, team

[8] Diversity Research Network, October 2002.

[9] The Partnership for Public Service, The Best Places to Work in the Federal Government 2010 Rankings, 2010, available at http://www.bestplacestowork.org/BPTW/assets/BPTW10.pdf.

[10] Scott E. Page, The Difference: How the Power of Diversity Creates Better Groups, Firms, Schools, and Societies, 2007.

motivation and trust. High level of employee engagement translates into increased productivity and retention of top talent in highly competitive markets.

- Mission Success - D&I adds value as a critical element tied to mission success. "The how" we can accomplish our mission is D&I – by capitalizing on the strengths of our diverse workforce to better perform our mission through teamwork and innovation.

When employees feel included, perceive they have a voice, and are given the opportunity to develop and maximize their potential, the employer creates an organization of choice and becomes a model employer. To accomplish this transformation, agencies should review and analyze programs, policies, and procedures to ensure that they are inclusive, transparent, and fair to all employees, and that employees perceive them as so. Data can also be gathered from exit interviews, new employee follow-up, and focus group meetings with affinity groups and employee resource groups.

An example of how to gather relevant employee engagement data is outlined below.

Steps for environment analysis

1. Conduct employee surveys (Employee Viewpoint Survey and/or agency survey) to assess: (a) leadership and management practices that contribute to an agency's performance; and (b) employee satisfaction with workplace policies and practices, work environment, rewards and recognition, access to resources, and opportunity for development and growth.[11]

2. Review and analyze survey results, including trend data by demographic category to include, for example, age, length of service, *etc*.

3. Assess workplace programs, policies, and procedures to ensure they are fair and transparent.

4. Analyze exit interview results and other available data.

5. Identify barriers and other issues and develop improvement strategies.

6. Incorporate strategies into human capital planning efforts and in retention, development and promotion activities.

[11] 5 C.F.R. Pt. 250, Subpart C..

Priorities, Actions, and Sample Practices for Goal 2

Priority 2.1: Promote diversity, inclusion, and equity in leadership development programs.

Actions:

1. Review leadership development programs, determine whether they draw from all segments of the workforce, and develop strategies to eliminate barrier(s) where they exist.[12]

2. Enhance mentoring programs within agencies for employees at all levels with an emphasis on aspiring Executive level employees.

3. Develop and implement a succession planning system for mission-critical occupations that includes broad outreach to a wide variety of potential leaders.

Measurements:

- Measure the total percentage of GS-11 through GS-15 level employees (or equivalent) by demographic group and compare with the percent of each group that participated in leadership development programs in the past 12 months.
- Analyze applicant pool data for all leadership development programs by demographic groups.
- Measure percentage of agency employees engaged in mentoring relationships by all demographic categories.
- Measure number of GS-11 through GS-15 level employees engaged in mentoring relationships by demographic categories.
- Measure percentage of all demographic groups incorporated into agency succession planning system.

Sample practices for Priority 2.1:

CHCOs, in collaboration with appropriate offices and senior managers, should review existing leadership development, training, and mentoring programs and conduct succession planning that ensures all employees have the opportunity to develop to their full potential. Below are sample practices for Priority 2.1:

[12] When conducting analysis of leadership development programs and succession planning, agencies should consider the entire workforce and determine whether programs and plans draw from the talent present throughout the agency with consideration of all dimensions of diversity to the greatest extent practicable.

- Where underrepresentation exists, conduct analyses of leadership development selection processes to identify barriers to equal opportunity in the process.

- Ensure programs are competency-based; provide potential for career path change; and consist of a variety of developmental activities including: training, rotational assignments, executive interviews, and shadow assignments.

- Ensure Program participants receive guidance through a Mentoring Program, made up of volunteer managers and supervisors; support mentoring programs that are sponsored by employee affinity or resource groups; conduct reverse mentoring programs and coaching programs. For more information on mentoring, go to OPM's Best Practices: Mentoring, available at: http://www.opm.gov/hrd/lead/BestPractices-Mentoring.pdf (See page 15 for definition of reverse mentoring).

- Routinely offer temporary detail assignments, special assignments, leadership shadowing programs, and opportunities to transfer to other regions for advancement to help upgrade employees' skills and improve their visibility. Widely advertise such assignments.

- Use a career executive service, which provides extensive training, executive simulations, targeted Individual Development Plans, and places candidates on succession planning lists.

- Measure employee perceptions on the availability and utility of agency development programs to access effectiveness and identify areas for improvement through the Employee Viewpoint Survey.

Priority 2.2: Cultivate a supportive, welcoming, inclusive and equitable work environment.

Actions:

1. Use flexible workplace policies that encourage employee engagement and empowerment, including, but not limited to, telework, flexiplace, wellness programs, and other work-life flexibilities and benefits.

2. Support participation in employee affinity and resource groups and provide such groups with access to agency senior leadership.

3. Administer a robust orientation process for new Federal employees and new members of the SES to introduce them to the agency culture and to provide networking opportunities.

Measurements:

- Measure percentage of workforce participating in 1) telework, 2) flexiplace and 3) Wellness programs.
- Review Employee Viewpoint Survey (EVS) results each year.
- Measure number of new initiatives implemented by employee affinity and/or resource groups.
- Measure percentage of agency executives involved in employee affinity and/or resource groups.
- Measure percentage of positive replies received on agency on-boarding (newcomers) process through survey feedback.

Sample practices for Priority 2.2:

The CHCO, EEO Director, and CDO (if any) should partner in reviewing and modifying the agency's existing policies and practices related to workforce flexibilities, employee affinity and/or resource groups, and new employee and SES onboarding. Below are sample practices for Priority 2.2:

- Review workplace policies and revise those that unnecessarily limit employee flexibility. Specifically, ensure employees are able to request flexible work arrangements that allow them to balance work and personal responsibilities. General Flexible Options include:

    - Flextime Programs. Flextime policies generally permit employees to vary their work day start and stop times within a specified range, such as allowing an employee to arrive at work at any time between 8:00 and 10:00 a.m. and then work for 8 hours.
    - Flexible Week Opportunities. Flexible week opportunities may include compressed work weeks, such as a work week consisting of four ten-hour work days.
    - Telecommuting, Work-at-Home, or Flexiplace Programs. These options enable employees to work from home or alternate office locations.
    - Reduced-time options. These options permit employees to work part-time while juggling other responsibilities, such as caregiving.

- Consistent with OPM regulations, provide reasonable personal or sick leave to allow employees to engage in caregiving even if not required to do so by the Family and Medical Leave Act of 1993 (FMLA).[13]

- Set forth guidelines for employees to use when establishing employee affinity or resource groups with a senior organizational advisor and a charter that sets forth roles, responsibilities, activities, funding parameters, recognition, community outreach, talent management and outreach roles.

- Conduct regular meetings, at least semi-annually, between employee affinity and resource groups and agency leadership.

- Conduct multi-day orientation program in which a high level official and functional areas (or their designees) share their roles and responsibilities, and which includes tours of different work locations.

- Assign new employees "mentors" or "ambassadors" (one from work area and one outside work area) to help new employees navigate the workplace for the first 6 months.

[13] Definitions Related to Family Member and Immediate Relative for Purposes of Sick Leave, Funeral Leave, Voluntary Leave Transfer, Voluntary Leave Bank, and Emergency Leave Transfer, available at http://www.opm.gov/oca/leave/HTML/FamilyDefs.asp.

Goal 3: Sustainability…Institutionalize Diversity and Inclusion

Federal Agencies shall develop structures and strategies to equip leaders with the ability to manage diversity, be accountable, measure results refine approaches on the basis of such data, and engender a culture of inclusion.

Coping with labor force changes and navigating the altered environment of the evolving workplace requires acquisition of new knowledge and development of new skills for all employees. For a diversity and inclusion program to be successful, not only must new roles and responsibilities be defined, but employees must be held accountable for delivering on expectations and meeting program requirements. Moreover, management accountability and innovation must be emphasized in order for progress to be made in employing, retaining, and developing all employees in the Federal government.

First, diversity and inclusion must be strategically integrated and aligned with the organization's mission, goals, objectives, staffing and budgets. Then, managers and supervisors at all levels of an organization must be required to make measurable and sustainable progress toward established priorities. This requires making diversity management a part of both performance evaluation and training, as well as incentivizing the development of programs that succeed and meet the organization's goals. Finally, development of such evaluation criteria underscores diversity and inclusion as an important and strategic organizational initiative. When these actions are performed, all employees, from entry level to SES, share in such accountability. This encourages teamwork and compliance at all levels of the Federal workforce.

Analysis of Diversity & Inclusion Institutionalization

Institutionalization is a key imperative of sustainable diversity and inclusion efforts. However, even when institutionalization efforts have been utilized, organizational progress has been frustratingly slow, sporadic, and dependent on enlightened leadership rather than sound sustainability practices.

Effective sustainability efforts are dependent upon identifying and weaving key diversity principles into organizational systems, processes, and policies. Following is a list of possible areas and questions agencies can utilize in sustaining diversity and inclusion progress by using sound institutionalizing strategies (Jarvis, 2009).

1. **Include diversity and inclusion in GPRA Required Strategic Planning.** Agencies should affirm the value of workforce diversity and inclusion in GPRA Required Strategic Planning, and where barriers have been identified, the agency Strategic Plan and/or Annual Performance Plan should incorporate strategies to address those areas and describe how it will monitor progress.

2. **Discover Ways to Integrate Diversity within Your Organizational Culture.** In what ways can diversity become a part of the organization's structure, mission and vision? What quick successes exist for the organization to leverage diversity engagement in consistent ways? What are the key indicators from the employees' perspectives that would define their agency as both valuing and rewarding diversity and inclusion in the workplace?

3. **Create an Organizational Core Value Focused on Diversity.** How could a core value of diversity demonstrate the organization's commitment? Who would be responsible for developing the diversity value? What would the diversity statement be and why?

4. **Blend Diversity into All Learning and Development Initiatives.** Which aspects of diversity make the most sense to integrate with training goals? How will the agency know when diversity goals have been successful? What will motivate employees to go to diversity training?

5. **Incorporate Diversity into Your Performance Management System.** In what ways can the Performance Management System have meaningful aspects of diversity within it? What performance metrics focused on diversity would be relevant at varying employee levels?

6. **Proactively Seek New Hires from All Segments of Society.** Where can organizations go to recruit individuals who can advance the organization's mission and business? What areas of talent have not been located and how might the organization deploy resources to achieve this goal?

7. **Generate a New Idea Factory to Engage Diverse Thinking.** How might a new idea generating system contribute to diversity of thought? What would the system look like? Who would manage it and how would it ensure the great ideas become a reality with significant impact on the business enterprise?

Priorities, Actions, and Sample Practices for Goal 3

Priority 3.1: Demonstrate leadership accountability, commitment, and involvement regarding diversity and inclusion in the workplace.

Actions:

1. Affirm the value of workforce diversity and inclusion in each agency's strategic plan and include them in workforce planning activities.

2. Develop an agency-specific diversity and inclusion strategic plan, and implement that plan, through the collaboration and coordination of the Chief Human Capital Officer, the EEO Director, and the Director of Diversity (if any).

3. Ensure that all SES members, managers, supervisors and employees throughout the agency have performance measures in place to ensure the proper execution of the agency's strategic plan, which includes diversity and inclusion.

4. Develop and widely distribute a set of diversity and inclusion measures to track agency efforts and provide a mechanism for refining plans.

Measurements:

- Provide documentation verifying diversity and inclusion language has been inserted into agency planning documentation.
- Issue annual diversity and inclusion policy statements by the agency head.
- Develop and submit agency-specific Diversity and Inclusion Strategic Plan outlining agency strategy to ensure a diverse, inclusive, high performance workplace.
- Submit percentage of SES members, managers, and supervisors, who have diversity and inclusion performance measures as a part of their performance evaluation.
- Provide diversity and inclusion metrics to OPM with short narrative on how metrics are embedded in the agency culture.

Sample practices for Priority 3.1:

Agencies should affirm the value of workforce diversity and inclusion in GPRA Required Strategic Planning, and where barriers have been identified, the agency Strategic Plan and/or Annual Performance Plans should incorporate strategies to address those areas and describe how it will monitor progress. Below are sample practices for achieving Priority 3.1:

- Tie vision, role and commitment of diversity and inclusion to strategic organizational goals and leadership plans and behavior that demonstrates diversity and inclusion principles and practices and that integrate these practices into the culture of the organization.

- Include a non-numerical, qualitative goal on diversity and inclusion in the Agency's Strategic Plan. For example:

    - "Identify, cultivate, and sustain a diverse workforce and inclusive work environment…."
    - "Improve retention of [diverse] students in STEM disciplines by providing opportunities and activities along the full length of the education pipeline."
    - "[E]nsure that beneficiaries of our Agency-funded educational programs are afforded equal opportunities, regardless of race, ethnicity, gender, age, or disability…."[14]

- List diversity and inclusion efforts as one of the agency's major initiatives for "Executing the Plan" under human capital management.[15]

- Coordinate efforts to ensure that MD-715 barrier analysis regarding D&I is not redundant with workforce planning, but rather complements and supports the agency's overall goals with each reflecting their own distinctive features and cross-referencing where there is overlap.

- Include a D&I and EEO element in SES and supervisors/managers Performance Plans specifically focused on making measurable progress in advancing the goals of the Diversity and Inclusion Strategic Plan. Language for a member of the Senior Executive Service may include, for example:

    > Designs and implements strategies that maximize employee potential, connects the organization vertically and horizontally, and fosters high ethical standards in meeting the organization's vision, mission, and goals. Provides an inclusive workplace that fosters the development of others to their full

[14] For example, see the NASA Strategic Plan, available at: http://www.nasa.gov/pdf/516579main_NASA2011StrategicPlan.pdf.

[15] For example, see the Department of Veterans Affairs (VA) Strategic Plan, page 59 at http://www.va.gov/VA_2011-2015_Strategic_Plan_Refresh_wv.pdf.

potential; allows for full participation by all employees; facilitates collaboration, cooperation and teamwork; and supports constructive resolution of conflicts. Ensures employee performance plans are aligned with the organization's mission and goals, that employees receive constructive feedback, and that employees are realistically appraised against clearly defined and communicated performance standards. Seeks and considers employee input. Recruits, retains, and develops the talent needed to achieve a high quality, diverse workforce that reflects the nation, with the skills needed to accomplish organizational performance objectives while supporting workforce diversity, workplace inclusion and equal employment policies and programs.

- Establish diversity and inclusion metrics including statistics on employee hiring, retention, promotions, EEO compliance, grievances and diversity of talent pipeline/outreach efforts and employee affinity and resource group accomplishments; disseminate quarterly workforce diversity reports to leadership; and issue Agency Annual Performance Report conveying accomplishments, progress, status on attainment of goals and priorities contained in agency Diversity and Inclusion Strategic Plan.

Priority 3.2: Fully and timely comply with all related Federal laws, regulations, Executive orders, management directives, and policies related to promoting diversity and inclusion in the federal workforce.

Actions:

1. Employ a diversity and inclusion dashboard with metrics as a tool for agency workforce planning and reporting.

2. Timely submit to the U.S. Office of Personnel Management (OPM) reports required by Federal laws, regulations, Executive orders, management directives, and policies. Where an agency fails to do so, OPM will issue a Diversity and Inclusion Improvement Notice and notify the President's Management Council (PMC) of the deficiency.

Measurements:

- Provide agency metric diversity and inclusion information for posting on designated reporting system by due date to avoid Diversity and Inclusion Performance Notice.

Priority 3.3: Involve employees as participants and responsible agents of diversity, mutual respect and inclusion.

Actions:

1. Create a formal diversity and inclusion council at each agency with visible leadership involvement.

2. Participate in, and contribute to, OPM's Diversity and Inclusion Best Practice Program, pursuant to Executive Order 13583.

3. Ensure all employees have access to diversity and inclusion training and education to include the proper implementation of the Agency-Specific Diversity and Inclusion Strategic Plan, as well as relevant legal requirements.

Measurements:

- Provide quarterly updates on progress of council/taskforce in achieving items listed in the Agency Specific Diversity and Inclusion Strategic Plan.
- Provide two Best Practices to the OPM Best Practice Initiative annually.
- Measure percentage of workforce (counting managers/supervisors separately) completing diversity and inclusion related training (both mandatory and elective).

Sample practices for Priority 3.3:

The CHCO, EEO Director, and CDO (if any) should partner in developing the diversity and inclusion council, as well as training and education. Below are sample practices for Priority 3.3:

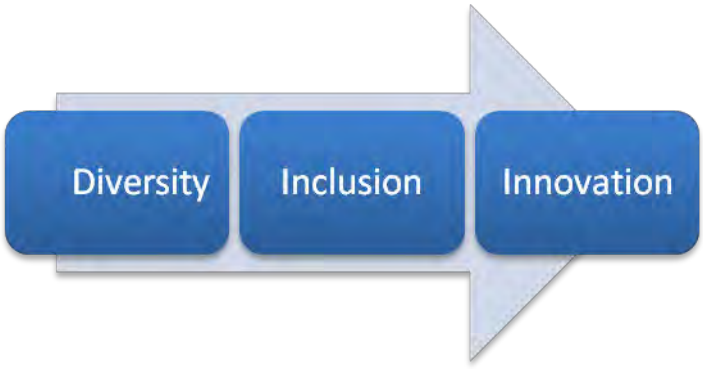
- Establish a Diversity and Inclusion Council which is chaired by an organizational head (or direct report designee) and include senior level officials and the heads of employee affinity and/or resource groups.

- Promote cultural competency at your agency by educating and training Senior Executives, supervisors and HR professionals on the importance of D&I, as well as on how to conduct effective outreach, recruitment, interviewing and decision-making that is consistent with all legal requirements.

- Ensure that appropriate agency personnel are trained in strategic planning, workforce planning, strategic recruitment, as well as cross-cultural and cross-generational training.

Conclusion

The Path Forward: Diversity, Inclusion, and the Innovation Connection



Connecting Different Minds in Different Ways to Achieve Common Goals…

One of the significant benefits of the Government-Wide Diversity and Inclusion Strategic Plan is innovation. Innovation is the mechanism that provides creative and unique solutions to the complex and seemingly intractable problems many agencies face today. However, to ensure sustainability of diversity and inclusion progress in this era of budget constraints, demographic shifts, and emerging technologies, there is a core requirement for agencies to focus on nurturing and harnessing the rich and critical benefits of innovation. The ultimate benefit of a diverse and inclusive workplace is the resulting innovation that is produced when different minds are connected in different ways to achieve common goals.

The primary key to innovation is diversity of thought. Diversity of thought in the social sciences is referred to as cognitive diversity. Cognitive diversity is comprised of primarily two components - "seeing" and "thinking."[16] In other words, people have different perspectives

[16] Page, S. E. (2007). *The difference: How the power of diversity creates better groups, firms, schools, and societies*. Princeton: Princeton University Press.

and different heuristics or “rules of thumb” which are a product of their unique upbringing, culture, and unique experiences. Perspectives are responsible for innovative breakthroughs. They are the game-changers. Once a breakthrough has been established then subsequent innovations and improvements are made through the “thinking” part of the innovation equation. This type of constant innovation can only take place through an environment where people feel included, connected, and engaged. Connecting different minds is the key to moving innovation forward for Federal agencies.

The primary goal of Federal agencies is to serve the American people. Because the world is becoming more complex, social, and interconnected, agencies must be poised to harness diversity of thought and leverage it to generate innovative ideas to solve the tough problems they face.

To build a culture that fosters innovation, agencies must hire for innovation talent; build teams that are diverse in talent, perspective and discipline; and place individuals in the right role to drive success. Once employees have been identified and placed, management can then provide them with the right training and onboarding relative to innovation and train managers for skills needed to drive talent.

In addition, Federal agencies must have useful metrics that are embedded in the culture of the organization. These metrics include benchmarking tools that allow organizations to compare themselves to the best in industry.

An agency that emphasizes connecting different minds, in different ways to achieve common goals is an agency that understands the functional importance of diversity. It is diversity of thought that is the engine that drives innovation. And it is innovation that ultimately determines the long term success of Federal agencies.

References

29 C.F.R. 1614. 102(b)(4). Outlines requirements for the establishment of a Special Emphasis Program Manager.

Axelrod, R. M., & Cohen, M. D. (1999). Harnessing complexity: Organizational implications of a scientific frontier. New York: Free Press.

Backes-Gellner, U & Veen, S (2009). The impact of aging and age diversity on company performance. ISU Working Paper 78, University of Zurich.)

Baghai, M., & Quigley, J. H. (2011). *As one: Individual action, collective power*. London: Portfolio/Penguin.

Bargh, J., & Morsella, E. (2008). *The unconscious mind*. Perspectives on Psychological Science, 3, 1, 73-79.

Blass, R., & Levy, D., & Parco, J. (July 2008), *Intolerable tolerance: the problem with diversity training in the military;* Armed Forces Journal.

Cross, R. L. (2010). *The organizational network fieldbook: Best practices, techniques, and exercises to drive organizational innovation and performance*. San Francisco, CA: Jossey-Bass.

Davidson., M. (2002). *Leveraging difference for organizational excellence: Managing diversity differently* . , Retrieved from http://www.lemoyne.edu/LinkClick.aspx?fileticket=K7njIZ4lBZM%3D&tabid=2132&mid=5371 .

Ernst, C., & Chrobot-Mason, D. (2011). *Boundary spanning leadership: Six practices for solving problems, driving innovation, and transforming organizations*. New York: McGraw-Hill.

Gill Kirton, (2003), *Strategic approaches to diversity*, Queen Mary, University of London, UK.

Gladwell, M. (2005). *Blink: The power of thinking without thinking*. New York, Little, Brown and Co.

Grunin, Susan (2011). *Becoming ore competitive: How diversity and inclusion can transform your organization,* American Council for Technology. Retrieved August 5, 2011 from http://www.actgov.org/knowledgebank/documentsandpresentations/Documents/Shared%20Interest%20Groups/Human%20Capital%20SIG/How%20Diversity%20and%20Inclusion%20Can%20Transform%20Your%20Organization%20-%20Susan%20Grunin-HC%20SIG%2005-11-11.pdf

Hannum, K. (2010). *Leading across differences: Cases and perspectives*. San Francisco, Calif: Wiley.

Heath, C., & Heath, D. (2010). *Switch: How to change things when change is hard*. New York: Broadway Books.

Homan, A. C. (2006). *Interacting dimensions of diversity: Cross-categorization and the functioning of diverse work groups*. Rotterdam: Erasmus Research Institute of Management (ERIM).

Huckman, R. S., Staats, B. R., & Harvard Business School. (2010). *Fluid teams and fluid tasks: The impact of diversity in experience and team familiarity*. Boston: Harvard Business School.

Ioannides, Y. M. (2010). *A review of Scott E. Page's The Difference: How the power of diversity creates better groups, firms, schools, and societies. Journal of Economic Literature, 48,* 1, 108-122.

Jackson, S., & Joshi, A. (2003), *International handbook of organizational teamwork and cooperative Working, Chapter 14: Managing workforce diversity to enhance cooperation in organizations*, John Wiley & Sons, Ltd.

Jarvis, E.D., (2009, September 4). *Sevens strategies to drive diversity*, Retrieved October 15, 2009, available at: http://www.danajarvis.org/?p=213.

ORC Networks. (2009). *ORC guides to diversity and inclusion best practice, for good measure: Diversity and Inclusion Metrics,* ORC Worldwide Networks Retrieved on September 22, 2011 from https://www.orcnetworks.com/resources/good-measure-diversity-and-inclusion-metrics

Osterwalder, A. (2010). *Business model generation: A handbook for visionaries, game changers, and challengers*. Hoboken, NJ: Wiley.

Page, S. E. (2007). *The difference: How the power of diversity creates better groups, firms, schools, and societies*. Princeton: Princeton University Press.

Page, S. E. (2011). *Diversity and complexity*. Princeton, NJ: Princeton University Press.

Partnership for Public Service. (2010). *America has talent: Breaking the mold for federal recruiting*, retrieved September 15, 2011 from http://www.ourpublicservice.org/OPS/publications/viewcontentdetails.php?id=153

Perretti, F. (2007). *Mixing genres, matching people : a study in innovation and team composition in Hollywood*. John Wiley.

Pink, D. H. (2009). *Drive: The surprising truth about what motivates us*. New York, NY: Riverhead Books.

Rhode, D.L. & Packel, A. K. (September 2010), *Diversity on corporate boards: how much difference does difference make?*, Rock Center for Corporate Governance, Stanford University.

Rushford & Associates. (2011). *Role of the special emphasis program manager.* Lakewood, CO.

Thomas, D. A. (January 01, 2004). Diversity as strategy. *Harvard Business Review, 82,* 9, 98-108.

United States. (2008). *Human capital: Diversity in the federal SES and processes for selecting new executives : report to congressional requesters*. Washington, D.C.: U.S. Govt. Accountability Office.

United States. (2008). *Report on the hispanic employment challenge in the federal government*. Washington, D.C.: U.S. Equal Employment Opportunity Commission.

United States. (2004). *Instructions to federal agencies for equal employment opportunity Management Directive 715 (EEO MD-715)*. Washington, D.C.: U.S. Equal Employment Opportunity Commission.

U.S. Government Accountability Office, *Diversity in the Federal SES and Senior Levels of the U.S. Postal Service and Processes for Selecting New Executives*, Report No. GAO-08-609T, p. 7 (Apr. 3, 2008). In FY 2007, the "feeder grades" to Senior Pay Level positions (GS-14 and 15) showed the following representation rates: men (65.80%), women (34.20%), Hispanic or Latino employees (4.34%), White employees (77.72%), Black or African American employees (10.26%), Asian employees (6.48%), Native Hawaiian / Other Pacific Islander (0.05%), American Indian / Alaska Native employees (1.01%), and Individuals with Targeted Disabilities (0.52%). FY 2007 Annual Report, *supra* note 25, Tables A-1 and A-3.

U.S. Office of Personnel Management, *Federal Hiring Flexibilities Resource Center*, *available at*: https://www.opm.gov/Strategic_Management_of_Human_Capital/fhfrc/FLX03020.asp

APPENDIX A

ORGANIZATIONAL STRUCTURES AND DIVISION OF RESPONSIBILITIES

Agencies have requested guidance on the division of responsibilities between HR, EEO, and D&I. The following table is adapted from *Becoming More Competitive: How Diversity and Inclusion Can Transform Your Organization, American Council for Technology*, and provides the typical allocation of key duties and responsibilities from six Federal agencies included in the Human Capital Shared Interest Group's benchmark study:

Key Duties and Responsibilities	**Chief Human Capital Officer**	**Office of Civil Rights / Civil Liberties & EEO**	**Office of Diversity and Inclusion**
Strategic Human Capital Planning and Organizational Assessments/Climate Surveys	Leads process	Has input	Builds D&I Strategy aligned with overall plan and/or co-leads SHC planning efforts
Workforce Planning-Workforce Analysis	Leads process	Has input	Has input
Writes Vacancy Announcement	Leads - coordinates with line	Has input	Has input
Outreach and Assistance	Has input	Works with D&I to identify pipelines & organizations that are disadvantaged including people with disabilities	Leads process - handles outreach and works with Affinity or Employee Resource Groups
Hiring Process	Leads process	Provides data/metrics	Provides data/metrics
Reasonable Accommodation	Has input	Lead process	Has input

Key Duties and Responsibilities	Chief Human Capital Officer	Office of Civil Rights / Civil Liberties & EEO	Office of Diversity and Inclusion
Training – Supervisor/ On-boarding – Orientation *etc*.	Manages overall training program/ Grievances	Focus on EEO, Alternative Dispute Resolution (ADR) and Complaint process	Focus on D&I and Conflict Management
Writing Policy	Lead on all HR policies	Focus on EEO, ADR and Complaint process – reviews other HR policies	Focus on D&I -– reviews other HR policies
Communications Plan and Metrics	Communicates all HR policies and collects data	Focus on EEO, ADR and Complaint process	Focus on D&I – works with Diversity Councils
Talent Management	Leads process	Ensures opportunities are fair, transparent and open to all	Ensures opportunities are fair, transparent and open to all
Awards/Recognitions/ Accountability Framework – bonuses and compensation	Leads process	Ensures opportunities are fair, transparent and open to all	Ensures opportunities are fair, transparent and open to all
Exit Interviews etc.	May manage	Reviews data	May manage

As noted in *Becoming More Competitive*:

> From this benchmark study, we noted that no "one size fits all" solution exists and that agencies assign and perform the various [] functions differently, depending on the size and geographic locations of the offices…. One key organizational finding was that regardless of who was assigned responsibility for a particular function, it must be clear that input and feedback are required from [all three organizations] for the process to work efficiently and effectively. A second key finding was that flexibility and collaboration were key to ensuring that all [] functions are effectively managed across any [F]ederal agency to ensure that D&I strategies are developed, implemented, and acted upon.

United States
Office of Personnel Management
Diversity and Inclusion
1900 E Street, NW
Washington, DC 20415

DI-SP-01

Government-Wide Diversity and Inclusion Strategic Plan 2011

Our Nation derives strength from the diversity of its population and from its commitment to equal opportunity for all. We are at our best when we draw on the talents of all parts of our society, and our greatest accomplishments are achieved when diverse perspectives are brought to bear to overcome our greatest challenges.

— President Obama,
Executive Order 13583

Table of Contents

Overview

This Government-Wide Diversity and Inclusion Strategic Plan (Plan) outlines the implementation of the President's Executive Order 13583 on Establishing a Coordinated Government-Wide Initiative to Promote Diversity and Inclusion in the Federal Workforce (the Executive order). This document incorporates recommendations from stakeholders with expertise in the areas of diversity and inclusion, equal employment opportunity, and organizational change.

The Plan provides a shared direction, encourages commitment, and creates alignment so agencies can approach their workplace diversity and inclusion efforts in a coordinated, collaborative, and integrated manner. Three key goals provide a path for successful agency diversity and inclusion efforts: workforce diversity, workplace inclusion, and sustainability.

Background

The Executive order directs executive departments and agencies (agencies) to develop and implement a more comprehensive, integrated, and strategic focus on diversity and inclusion as a key component of their human resources strategies. This approach should include a continuing effort to identify and adopt best practices to promote diversity and inclusion and to identify and remove any barriers to equal employment opportunity, consistent with merit system principles and applicable law.

A commitment to equal opportunity, diversity, and inclusion is critical to accomplishing the Federal government's missions. By law, the Federal government's recruitment policies should "endeavor to achieve a work force from all segments of society," while avoiding discrimination for or against any employee or applicant on the basis of race, color, religion, sex (including pregnancy or gender identity), national origin, age, disability, sexual orientation or any other prohibited basis. (5 U.S.C. 2301(b)(1), 2302(b)). As the Nation's largest employer, the Federal government has an obligation to lead by example. Seeking to attain a diverse, qualified workforce is a cornerstone of the merit-based civil service.

In order to cultivate high performing organizations for the 21st century, the Federal government must tap into the rich resources of our global community and ensure fairness and justice in the workplace. To accomplish this, we define diversity broadly, including, but not limited to, the legally protected categories. Diversity encompasses all that makes us unique, including the diversity of thought and perspective that accompanies our identity. Only then can we realize the full performance potential and harness the innovation that diversity offers. This is more than a legal or moral imperative, it is a business imperative for public service.

The difficult budget environment and the increased demand for innovation and efficiency present challenges to projecting and meeting future Federal human resources needs. Agencies can address these challenges with a diverse and inclusive workforce built by casting a broad net in the search for top talent, wherever it may be found. Agencies that

employ a workforce that draws from all corners of America – in filling positions from the Senior Executive Service (SES) to the entry level - will create a culture that fosters creativity and benefits from a greater return on investments in the workforce.

Moreover, research has demonstrated that, while organizations may have diversity in their midst, employees may not perceive that their social identities are appreciated and included in the workplace. For this reason, building inclusive workplaces ensures that all employees feel included, connected, and engaged.

A comprehensive strategic human capital plan is critical to the ability of all Federal agencies to carry out assigned missions and properly manage their diverse workforces. An important dimension of each agency's human capital plan is the ability to identify and close current and emerging skill gaps thereby enabling the agency to carry out its mission more cost-effectively. The U.S. Office of Personnel Management is working with the Chief Human Capital Officers (CHCO) Council and agencies to assess current and emerging skill gaps and develop strategies to close skill gaps in mission-critical occupations and skills areas that have the greatest impact on Government-Wide, and agency-specific, performance. The desired outcomes of this effort are: (1) increased proficiency levels in targeted skills areas through training, and (2) institutionalized processes for identifying and addressing skills gaps (Government-wide and agency-specific).

From 2008 to 2010, a study of hiring trends across Federal agencies revealed that information technology (IT) and cyber security professionals, nurses, contract and acquisition specialists, border patrol agents, and program analysts were among the top 15 most-hired positions within government. In each of these fields, research shows that recruiting with an emphasis on cultural, experiential, and cognitive diversity will improve agencies' prospects of having a workforce that is capable of addressing increasingly complex challenges more efficiently. Beyond traditional measures of diversity, seeking individuals with varying degree types; Science, Technology, Engineering and Mathematics (STEM) backgrounds; and professional experience will also benefit agencies and offices Government-Wide.

Creating a diverse Federal workforce that draws from all segments of society requires sustained commitment to ensuring a level playing field upon which applicants and employees may compete for opportunities within government. Sustaining the highest levels of integrity and professionalism through new outreach and recruiting efforts is paramount to achieving the strategic vision set out in this Plan.

Definitions of "Diversity" and "Inclusion"

We define workforce diversity as a collection of individual attributes that together help agencies pursue organizational objectives efficiently and effectively. These include, but are not limited to, characteristics such as national origin, language, race, color, disability, ethnicity, gender, age, religion, sexual orientation, gender identity, socioeconomic status, veteran status, and family structures. The concept also encompasses differences among people concerning where they are from and where they have lived and their differences of thought and life experiences.

We define inclusion as a culture that connects each employee to the organization; encourages collaboration, flexibility, and fairness; and leverages diversity throughout the organization so that all individuals are able to participate and contribute to their full potential.

Federal Government-Wide Diversity and Inclusion Vision Statement

Be the Nation's model employer by leveraging diversity and fostering inclusion to deliver the best public service.

Federal Government-Wide Diversity and Inclusion Mission Statement

Recruit, retain, and develop a diverse, high-performing Federal workforce that draws from all segments of society and values fairness, diversity and inclusion.

Goals:

1. Workforce Diversity. Recruit from a diverse, qualified group of potential applicants to secure a high-performing workforce drawn from all segments of American society.

2. Workplace Inclusion. Cultivate a culture that encourages collaboration, flexibility, and fairness to enable individuals to contribute to their full potential and further retention.

3. Sustainability. Develop structures and strategies to equip leaders with the ability to manage diversity, be accountable, measure results, refine approaches on the basis of such data, and institutionalize a culture of inclusion.

The three goals listed above are absolutely necessary for the successful growth of diversity and inclusion. Other characteristics of diversity and inclusion best practice plans, such as leadership, accountability, measurement, and training are components of, and integrated in, the three goals.

Goal 1: Workforce Diversity

Federal agencies shall recruit from a diverse, qualified group of potential applicants to secure a high-performing workforce drawn from all segments of American society.

Priority 1.1: Design and perform strategic outreach and recruitment to reach all segments of society.

Actions:

1. Collect and analyze applicant flow data.

2. Coordinate outreach and recruitment strategies to maximize ability to recruit from a diverse, broad spectrum of potential applicants, including a variety of geographic regions, academic sources, and professional disciplines.

3. Ensure that outreach and recruitment strategies designed to draw from all segments of society, including those who are underrepresented, are employed when using staffing flexibilities and alternative hiring authorities.

4. Develop strategic partnerships with a diverse range of colleges and universities, trade schools, apprentice programs, and affinity organizations from across the country.

5. Involve managers and supervisors in recruitment activities and take appropriate action to ensure that outreach efforts are effective in addressing barriers.

6. Review and ensure that student internship and fellowship programs have diverse pipelines to draw candidates from all segments of society.

Priority 1.2: Use strategic hiring initiatives for people with disabilities and for veterans, conduct barrier analysis, and support Special Emphasis Programs (SEPs), to promote diversity within the workforce.

Actions:

1. Review results of barrier analyses required under MD 715, develop action plans to eliminate any identified barrier(s), and coordinate implementation of action plans.

2. Use Schedule A hiring authority for people with disabilities and Veteran Hiring Authorities as part of strategy to recruit and retain a diverse workforce.

3. Support SEPs and appoint SEP Managers as advisors on hiring, retaining and promoting a diverse workforce.

Goal 2: Workplace Inclusion

Federal agencies shall cultivate a culture that encourages collaboration, flexibility, and fairness to enable individuals to contribute to their full potential and further retention.

Priority 2.1: Promote diversity and inclusion in leadership development programs.

Actions:

1. Review leadership development programs, determine whether they draw from all segments of the workforce, and develop strategies to eliminate barrier(s) where they exist.

2. Enhance mentoring programs within agencies for employees at all levels with an emphasis on aspiring Executive level employees.

3. Develop and implement a succession planning system for mission-critical occupations that includes broad outreach to a wide variety of potential leaders.

Priority 2.2: Cultivate a supportive, welcoming, inclusive and fair work environment.

Actions:

1. Use flexible workplace policies that encourage employee engagement and empowerment, including, but not limited to, telework, flexiplace, wellness programs, and other work-life flexibilities and benefits.

2. Support participation in employee affinity and resource groups and provide such groups with access to agency senior leadership.

3. Administer a robust orientation process for new Federal employees and new members of the SES to introduce them to the agency culture and to provide networking opportunities.

Goal 3: Sustainability

Federal agencies shall develop structures and strategies to equip leaders with the ability to manage diversity, be accountable, measure results, refine approaches on the basis of such data, and engender a culture of inclusion.

Priority 3.1: Demonstrate leadership accountability, commitment, and involvement regarding diversity and inclusion in the workplace.

Actions:

1. Affirm the value of workforce diversity and inclusion in each agency's strategic plan and include them in workforce planning activities.

2. Develop an agency-specific diversity and inclusion strategic plan, and implement that plan, through the collaboration and coordination of the Chief Human Capital Officer, the EEO Director, and the Director of Diversity (if any).

3. Ensure that all SES members, managers, supervisors and employees throughout the agency have performance measures in place to ensure the proper execution of the agency's strategic plan, which includes diversity and inclusion, and that all are trained regarding relevant legal requirements.

4. Develop and widely distribute a set of diversity and inclusion measures to track agency efforts and provide a mechanism for refining plans.

Priority 3.2: Fully and timely comply with all Federal laws, regulations, Executive orders, management directives, and policies related to promoting diversity and inclusion in the Federal workforce.

Actions:

1. Employ a diversity and inclusion dashboard with metrics as a tool for agency workforce planning and reporting.

2. Timely submit to the U.S. Office of Personnel Management (OPM) reports required by Federal laws, regulations, Executive orders, management directives, and policies. Where an agency fails to do so, OPM will issue a Diversity and Inclusion Improvement Notice and notify the President's Management Council (PMC) of the deficiency.

Priority 3.3: Involve employees as participants and responsible agents of diversity, mutual respect and inclusion.

Actions:

1. Create a formal diversity and inclusion council at each agency with visible leadership involvement.

2. Participate in, and contribute to, OPM's Diversity and Inclusion Best Practice Program, pursuant to Executive Order 13583.

3. Ensure all employees have access to diversity and inclusion training and education, including the proper implementation of the Agency-Specific Diversity and Inclusion Strategic Plan as well as relevant legal requirements.

Click here to skip navigation

- Facebook
- Twitter

(b) (5)

- A–Z Index
- Contact Us
- Forms
- FAQs

(b) (5)

(b) (5)

Operating Status:
Open

Search for Change Search Collection Go

Select a Search Collection:

- All of OPM
- About
- Policy
- Insurance
- Retirement
- Investigations
- Agency Services
- News
- FAQs

U.S. Office of Personnel Management

- About Open "About" Submenu
  - Our Agency
  - Our Director
  - Our Inspector General
  - Our Mission, Role & History
  - Our People & Organization
  - Careers at OPM
  - Doing Business with OPM
  - Budget & Performance
  - Open Government
  - Get Help
  - Contact Us

Featured Topics

Our Vision

The Federal Government will Become America's Model Employer for the 21st Century.

Our Mission

Recruit, Retain and Honor a World-Class Workforce to Serve the American People.

Close Menu
- Policy Open "Policy" Submenu
  - Assessment & Selection
  - Classification & Qualifications
  - Data, Analysis & Documentation
  - Disability Employment
  - Diversity & Inclusion
  - Employee Relations
  - Hiring Authorities
  - Human Capital Management
  - Labor-Management Relations
  - Oversight Activities
  - Pandemic Information
  - Pay & Leave
  - Performance Management
  - Senior Executive Service
  - Settlement Guidelines
  - Snow & Dismissal Procedures
  - Training & Development
  - Veterans Services
  - Work-Life
  - Workforce Restructuring
  - Policy FAQs
  - Contact Policymakers

Featured Topics

Salaries and Wages

Find out more about Federal compensation throughout your career and around the world.

Schedule A Hiring Authority

Staffing to align with your agency's mission

Close Menu
- Insurance Open "Insurance" Submenu
  - Life Events
  - Changes in Health Coverage
  - Healthcare
  - Dental & Vision
  - Life Insurance
  - Flexible Spending Accounts
  - Long Term Care
  - Multi-State Plan Program
  - Tribal Employers
  - Special Initiatives
  - Insurance Glossary
  - Insurance FAQs
  - Contact Healthcare & Insurance
  - The Affordable Care Act

Featured Topics

2014 FEGLI Handbook

Review the new 2014 Federal Employees' Group Life Insurance (FEGLI) Handbook

Frequently Asked Questions

Answering your questions about Healthcare and Insurance

Close Menu

- Retirement Open "Retirement" Submenu
  - My Annuity and Benefits
  - CSRS Information
  - FERS Information
  - Phased Retirement
  - Special Notices
  - Calculators
  - Publications & Forms
  - Benefits Officers Center
  - Retirement FAQs
  - Contact Retirement

Featured Topics

2013 Cost of Living Adjustment (COLA)

Congress approved a cost of living increase for Federal retirees.

Services Online

Manage your retirement online.

Close Menu

- Investigations Open "Investigations" Submenu
  - e-QIP Application
  - Background Investigations
  - Requesting Investigation Copies
  - Investigations FAQs
  - Contact Investigations

Featured Topics

Position Designation Tool

Human Resources and Security Specialists should use this tool to determine the correct investigation level for any covered position within the U.S. Federal Government.

Close Menu

- Agency Services Open "Agency Services" Submenu
  - Classification & Job Design

- Workforce Restructuring
- Workforce & Succession Planning
- Recruiting & Staffing Solutions
- Assessment & Evaluation
- Federal Leadership Programs
- Leadership Development
- Federal Executive Institute
- Performance Management
- Telework Solutions
- Technology Systems
- Training-Management Assistance
- HR Line of Business
- Administrative Law Judges
- Federal Executive Boards
- Contact Agency Services

Featured Topics

Telework: Is Your Agency Ready?

OPM's Human Resources Solutions organization can help your agency answer this critically important question.

Federal Executive Institute

Developing senior leaders in the U.S. Government through Leadership for a Democratic Society, Custom Programs and Interagency Courses.

Close Menu

- News Open "News" Submenu
  - Latest News
  - Speeches & Remarks
  - Memos to Agencies
  - Testimony
  - Video Gallery
  - Photo Gallery
  - Legislative Proposals
  - Reports & Publications
  - Social Media Presence
  - Feeds, Blogs & Lists
  - Website Archive

Featured Topics

Federal Register Notices

Visit this federal site to search for our regulatory notices, proposed and final rules.

Connect With Us On Social Media

See the latest tweets on our Twitter feed, like our Facebook pages, watch our YouTube videos, and page through our Flickr photos.

Close Menu

OPM.gov MainPolicyPerformance ManagementOverview & History
Skip Navigation

In This Section

- Assessment & SelectionToggle submenu
  - Job Analysis
  - Occupational Questionnaires
  - Structured Interviews
  - Competencies
  - Other Assessment Methods
  - Designing an Assessment Strategy
  - Assessment Glossary
  - Reference Materials
  - Contact Us
- Classification & QualificationsToggle submenu
  - Classifying General Schedule Positions
  - Classifying Federal Wage System Positions
  - General Schedule Qualification Policies
  - General Schedule Qualification Standards
  - Federal Wage System Qualifications
  - Appeals Decisions
  - Reference Materials
- Data, Analysis & DocumentationToggle submenu
  - Personnel Documentation
  - Data, Policy & Guidance
  - Enterprise Human Resources Integration
  - FedScope
  - Federal Employment Reports
  - Employee Surveys
  - Health Insurance Analysis
  - Other Insurance Analysis
  - Raw Datasets
- Disability EmploymentToggle submenu
  - Getting a Job
  - Reasonable Accommodations
  - Selective Placement Program Coordinator
  - Recruiting
  - Hiring
  - Retention
  - Providing Accommodations
  - Disability FAQs
  - Reference Materials
- Diversity & InclusionToggle submenu
  - About Us
  - People
  - Lesbian, Gay, Bisexual & Transgender (LGBT)
  - Reports
  - Workforce at a Glance
  - Diversity & Inclusion FAQs
  - Reference Materials

Employee RelationsToggle submenu
- Training
- Employee Rights & Appeals
- Reasonable Accommodation
- Employee Relations FAQs
- Reference Materials

- Hiring AuthoritiesToggle submenu
  - Competitive Hiring
  - Excepted Service
  - Veterans Authorities
  - Direct Hire Authority
  - Students & Recent Graduates
  - Part-Time & Job Sharing
  - Dual Compensation Waivers
  - Details & Transfers
  - Intergovernment Personnel Act
  - Reinstatement
  - Variations
- Human Capital ManagementToggle submenu
  - Strategic Planning & Alignment
  - Talent Management
  - Performance Culture
  - Evaluation
  - Hiring Reform
  - Reference Materials
- Labor-Management RelationsToggle submenu
  - Training
  - Reports on Official Time
  - Federal Labor-Management Information System
  - Events
  - Law & Policy Resources
- Oversight ActivitiesToggle submenu
  - Accountability
  - Compliance
  - Political Conversions
  - Voting Rights
  - Oversight FAQs
- Pandemic InformationToggle submenu
  - Benefits
  - Work & Hiring Arrangements
  - Pay & Leave
  - Agency Preparations
- Pay & LeaveToggle submenu
  - Pay SystemsToggle submenu
    - General Schedule
    - Federal Wage System
    - Special Rates Requests
    - Nonforeign Areas
  - Salaries & WagesToggle submenu
    - Special Rate
    - Fact Sheets
  - Pay Administration
  - Recruitment, Relocation & Retention Incentives
  - Student Loan Repayment

- Feds Hire Vets
- Vet Guide
- Veterans Services FAQs

- Work-LifeToggle submenu
  - Find Your Agency POC
  - Announcements & News
  - Telework
  - Health & Wellness
  - Employee Assistance Programs
  - Family Resources
  - Work-Life FAQs
  - Reference Materials
  - Contact Us
- Workforce RestructuringToggle submenu
  - Reductions in Force
  - Voluntary Early Retirement Authority
  - Voluntary Separation Incentive Payments
  - Career Transition
- Policy FAQs
- Contact Policymakers

Resources For

- New / Prospective Employees
- Federal Employees
- HR Professionals
- Managers

Performance Management Overview & History

- Overview
- Setting the Stage
- Historical Chronology

Overview

Performance management is the systematic process by which an agency involves its employees, as individuals and members of a group, in improving organizational effectiveness in the accomplishment of agency mission and goals.

Employee performance management includes:

- planning work and setting expectations,
- continually monitoring performance,
- developing the capacity to perform,
- periodically rating performance in a summary fashion, and
- rewarding good performance.

The revisions made in 1995 to the Governmentwide performance appraisal and awards regulations support sound management principles. Great care was taken to ensure that the requirements those regulations establish would complement and not conflict with the kinds of activities and actions practiced in effective organizations as a matter of

course.

Additional background information on performance management can be found in the following articles:

- Chronology of Employee Performance Management in the Federal Government
- Setting the Stage for Performance Management Today

Planning

In an effective organization, work is planned out in advance. Planning means setting performance expectations and goals for groups and individuals to channel their efforts toward achieving organizational objectives. Getting employees involved in the planning process will help them understand the goals of the organization, what needs to be done, why it needs to be done, and how well it should be done.

The regulatory requirements for planning employees' performance include establishing the elements and standards of their performance appraisal plans. Performance elements and standards should be measurable, understandable, verifiable, equitable, and achievable. Through critical elements, employees are held accountable as individuals for work assignments or responsibilities. Employee performance plans should be flexible so that they can be adjusted for changing program objectives and work requirements. When used effectively, these plans can be beneficial working documents that are discussed often, and not merely paperwork that is filed in a drawer and seen only when ratings of record are required.

Monitoring

In an effective organization, assignments and projects are monitored continually. Monitoring well means consistently measuring performance and providing ongoing feedback to employees and work groups on their progress toward reaching their goals.

Regulatory requirements for monitoring performance include conducting progress reviews with employees where their performance is compared against their elements and standards. Ongoing monitoring provides the opportunity to check how well employees are meeting predetermined standards and to make changes to unrealistic or problematic standards. And by monitoring continually, unacceptable performance can be identified at any time during the appraisal period and assistance provided to address such performance rather than wait until the end of the period when summary rating levels are assigned.

Back to Top

Developing

In an effective organization, employee developmental needs are evaluated and addressed. Developing in this instance means increasing the capacity to perform through training, giving assignments that introduce new skills or higher levels of responsibility, improving work processes, or other methods. Providing employees with training and developmental opportunities encourages good performance, strengthens job-related skills and competencies, and helps employees keep up with changes in the workplace, such as the introduction of new technology.

Carrying out the processes of performance management provides an excellent opportunity to identify developmental needs. During planning and monitoring of work, deficiencies in performance become evident and can be addressed. Areas for improving good performance also stand out, and action can be taken to help successful employees improve even further.

Rating

From time to time, organizations find it useful to summarize employee performance. This can be helpful for looking at and comparing performance over time or among various employees. Organizations need to know who their best performers are.

Within the context of formal performance appraisal requirements, rating means evaluating employee or group performance against the elements and standards in an employee's performance plan and assigning a summary rating of record. The rating of record is assigned according to procedures included in the organization's appraisal program. It is based on work performed during an entire appraisal period. The rating of record has a bearing on various other personnel actions, such as granting within-grade pay increases and determining additional retention service credit in a reduction in force.

Note:

Although group performance may have an impact on an employee's summary rating, a rating of record is assigned only to an individual, not to a group.

Back to Top

Rewarding

In an effective organization, rewards are used well. Rewarding means recognizing employees, individually and as members of groups, for their performance and acknowledging their contributions to the agency's mission. A basic principle of effective management is that all behavior is controlled by its consequences. Those consequences can and should be both formal and informal and both positive and negative.

Good performance is recognized without waiting for nominations for formal awards to be solicited. Recognition is an ongoing, natural part of day-to-day experience. A lot of the actions that reward good performance like saying "Thank you" don't require a specific regulatory authority. Nonetheless, awards regulations provide a broad range of forms that more formal rewards can take, such as cash, time off, and many nonmonetary items. The regulations also cover a variety of contributions that can be rewarded, from suggestions to group accomplishments.

Managing Performance Effectively

In effective organizations, managers and employees have been practicing good performance management naturally all their lives, executing each key component process well. Goals are set and work is planned routinely. Progress toward those goals is measured and employees get feedback. High standards are set, but care is also taken to develop the skills needed to reach them. Formal and informal rewards are used to recognize the behavior and results that accomplish the mission. All five component processes working together and supporting each other achieve natural, effective performance management.

Back to Top

U.S. Office of Personnel Management

1900 E Street, NW, Washington, DC 20415

202-606-1800

Federal Relay Service (external link)

- A - Z Index
- FAQs

- Forms
- Reports & Publications
- Combined Federal Campaign

- Sustainability
- Recovery Act
- FOIA
- Information Management
- No Fear Act

- Inspector General
- Ethics (external link)
- USA.gov (external link)
- Office of Special Counsel (external link)
- Privacy Policy

- About
  - Our Agency
  - Our Director
  - Our Inspector General
  - Our Mission, Role & History
  - Our People & Organization
  - Careers at OPM
  - Doing Business with OPM
  - Budget & Performance
  - Open Government
  - Get Help
  - Contact Us
- Policy
  - Assessment & Selection
  - Classification & Qualifications
  - Data, Analysis & Documentation
  - Disability Employment
  - Diversity & Inclusion
  - Employee Relations
  - Hiring Authorities
  - Human Capital Management
  - Labor-Management Relations
  - Oversight Activities
  - Pandemic Information
  - Pay & Leave
  - Performance Management
  - Senior Executive Service
  - Settlement Guidelines
  - Snow & Dismissal Procedures
  - Training & Development
  - Veterans Services
  - Work-Life
  - Workforce Restructuring
  - Policy FAQs
  - Contact Policymakers
- Insurance
  - Life Events
  - Changes in Health Coverage

- Reports & Publications
- Social Media Presence
- Feeds, Blogs & Lists
- Website Archive

Feedback

Public Law 88-352

AN ACT

July 2, 1964
[H. R. 7152]

To enforce the constitutional right to vote, to confer jurisdiction upon the district courts of the United States to provide injunctive relief against discrimination in public accommodations, to authorize the Attorney General to institute suits to protect constitutional rights in public facilities and public education, to extend the Commission on Civil Rights, to prevent discrimination in federally assisted programs, to establish a Commission on Equal Employment Opportunity, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Civil Rights Act of 1964".

Civil Rights Act of 1964.

TITLE I—VOTING RIGHTS

SEC. 101. Section 2004 of the Revised Statutes (42 U.S.C. 1971), as amended by section 131 of the Civil Rights Act of 1957 (71 Stat. 637), and as further amended by section 601 of the Civil Rights Act of 1960 (74 Stat. 90), is further amended as follows:

Operation and enforcement.

(a) Insert "1" after "(a)" in subsection (a) and add at the end of subsection (a) the following new paragraphs:

"(2) No person acting under color of law shall—

"(A) in determining whether any individual is qualified under State law or laws to vote in any Federal election, apply any standard, practice, or procedure different from the standards, practices, or procedures applied under such law or laws to other individuals within the same county, parish, or similar political subdivision who have been found by State officials to be qualified to vote;

Voting qualifications.

"(B) deny the right of any individual to vote in any Federal election because of an error or omission on any record or paper relating to any application, registration, or other act requisite to voting, if such error or omission is not material in determining whether such individual is qualified under State law to vote in such election; or

Registration, etc.

"(C) employ any literacy test as a qualification for voting in any Federal election unless (i) such test is administered to each individual and is conducted wholly in writing, and (ii) a certified copy of the test and of the answers given by the individual is furnished to him within twenty-five days of the submission of his request made within the period of time during which records and papers are required to be retained and preserved pursuant to title III of the Civil Rights Act of 1960 (42 U.S.C. 1974–74e; 74 Stat. 88): *Provided, however*, That the Attorney General may enter into agreements with appropriate State or local authorities that preparation, conduct, and maintenance of such tests in accordance with the provisions of applicable State or local law, including such special provisions as are necessary in the preparation, conduct, and maintenance of such tests for persons who are blind or otherwise physically handicapped, meet the purposes of this subparagraph and constitute compliance therewith.

Literacy tests. Records.

Attorney General. Agreements with State and local authorities.

"(3) For purposes of this subsection—

"(A) the term 'vote' shall have the same meaning as in subsection (e) of this section;

"Vote."

"(B) the phrase 'literacy test' includes any test of the ability to read, write, understand, or interpret any matter."

"Literacy test."

(b) Insert immediately following the period at the end of the first sentence of subsection (c) the following new sentence: "If in any such proceeding literacy is a relevant fact there shall be a rebuttable

presumption that any person who has not been adjudged an incompetent and who has completed the sixth grade in a public school in, or a private school accredited by, any State or territory, the District of Columbia, or the Commonwealth of Puerto Rico where instruction is carried on predominantly in the English language, possesses sufficient literacy, comprehension, and intelligence to vote in any Federal election."

(c) Add the following subsection "(f)" and designate the present subsection "(f)" as subsection "(g)":

"Federal election."

"(f) When used in subsection (a) or (c) of this section, the words 'Federal election' shall mean any general, special, or primary election held solely or in part for the purpose of electing or selecting any candidate for the office of President, Vice President, presidential elector, Member of the Senate, or Member of the House of Representatives."

(d) Add the following subsection "(h)":

Suits by Attorney General.

"(h) In any proceeding instituted by the United States in any district court of the United States under this section in which the Attorney General requests a finding of a pattern or practice of discrimination pursuant to subsection (e) of this section the Attorney General, at the time he files the complaint, or any defendant in the proceeding, within twenty days after service upon him of the complaint, may file with the clerk of such court a request that a court of three judges be convened to hear and determine the entire case. A copy of the request for a three-judge court shall be immediately furnished by such clerk to the chief judge of the circuit (or in his absence, the presiding circuit judge of the circuit) in which the case is pending. Upon receipt of the copy of such request it shall be the duty of the chief judge of the circuit or the presiding circuit judge, as the case may be, to designate immediately three judges in such circuit, of whom at least one shall be a circuit judge and another of whom shall be a district judge of the court in which the proceeding was instituted, to hear and determine such case, and it shall be the duty of the judges so designated to assign the case for hearing at the earliest practicable date, to participate in the hearing and determination thereof, and to cause the case to be in every way expedited. An appeal from the final judgment of such court will lie to the Supreme Court.

Appeals.

Designation of judges.

"In any proceeding brought under subsection (c) of this section to enforce subsection (b) of this section, or in the event neither the Attorney General nor any defendant files a request for a three-judge court in any proceeding authorized by this subsection, it shall be the duty of the chief judge of the district (or in his absence, the acting chief judge) in which the case is pending immediately to designate a judge in such district to hear and determine the case. In the event that no judge in the district is available to hear and determine the case, the chief judge of the district, or the acting chief judge, as the case may be, shall certify this fact to the chief judge of the circuit (or, in his absence, the acting chief judge) who shall then designate a district or circuit judge of the circuit to hear and determine the case.

"It shall be the duty of the judge designated pursuant to this section to assign the case for hearing at the earliest practicable date and to cause the case to be in every way expedited."

TITLE II—INJUNCTIVE RELIEF AGAINST DISCRIMINATION IN PLACES OF PUBLIC ACCOMMODATION

Equal access.

SEC. 201. (a) All persons shall be entitled to the full and equal enjoyment of the goods, services, facilities, privileges, advantages, and accommodations of any place of public accommodation, as defined in this section, without discrimination or segregation on the ground of race, color, religion, or national origin.

Establishments affecting interstate commerce.

(b) Each of the following establishments which serves the public is a place of public accommodation within the meaning of this title if its operations affect commerce, or if discrimination or segregation by it is supported by State action:

Lodgings.

(1) any inn, hotel, motel, or other establishment which provides lodging to transient guests, other than an establishment located within a building which contains not more than five rooms for rent or hire and which is actually occupied by the proprietor of such establishment as his residence;

Restaurants, etc.

(2) any restaurant, cafeteria, lunchroom, lunch counter, soda fountain, or other facility principally engaged in selling food for consumption on the premises, including, but not limited to, any such facility located on the premises of any retail establishment; or any gasoline station;

Theaters, stadiums, etc.

(3) any motion picture house, theater, concert hall, sports arena, stadium or other place of exhibition or entertainment; and

Other covered establishments.

(4) any establishment (A) (i) which is physically located within the premises of any establishment otherwise covered by this subsection, or (ii) within the premises of which is physically located any such covered establishment, and (B) which holds itself out as serving patrons of such covered establishment.

Operations affecting commerce criteria.

(c) The operations of an establishment affect commerce within the meaning of this title if (1) it is one of the establishments described in paragraph (1) of subsection (b); (2) in the case of an establishment described in paragraph (2) of subsection (b), it serves or offers to serve interstate travelers or a substantial portion of the food which it serves, or gasoline or other products which it sells, has moved in commerce; (3) in the case of an establishment described in paragraph (3) of subsection (b), it customarily presents films, performances, athletic teams, exhibitions, or other sources of entertainment which move in commerce; and (4) in the case of an establishment described in paragraph (4) of subsection (b), it is physically located within the premises of, or there is physically located within its premises, an establishment the operations of which affect commerce within the meaning of this subsection. For purposes of this section, "commerce" means travel, trade, traffic, commerce, transportation, or communication among the several States, or between the District of Columbia and any State, or between any foreign country or any territory or possession and any State or the District of Columbia, or between points in the same State but through any other State or the District of Columbia or a foreign country.

"Commerce."

Support by State action.

(d) Discrimination or segregation by an establishment is supported by State action within the meaning of this title if such discrimination or segregation (1) is carried on under color of any law, statute, ordinance, or regulation; or (2) is carried on under color of any custom or usage required or enforced by officials of the State or political subdivision thereof; or (3) is required by action of the State or political subdivision thereof.

Private establishments.

(e) The provisions of this title shall not apply to a private club or other establishment not in fact open to the public, except to the extent that the facilities of such establishment are made available

to the customers or patrons of an establishment within the scope of subsection (b).

Entitlement.

SEC. 202. All persons shall be entitled to be free, at any establishment or place, from discrimination or segregation of any kind on the ground of race, color, religion, or national origin, if such discrimination or segregation is or purports to be required by any law, statute, ordinance, regulation, rule, or order of a State or any agency or political subdivision thereof.

Interference.

SEC. 203. No person shall (a) withhold, deny, or attempt to withhold or deny, or deprive or attempt to deprive, any person of any right or privilege secured by section 201 or 202, or (b) intimidate, threaten, or coerce, or attempt to intimidate, threaten, or coerce any person with the purpose of interfering with any right or privilege secured by section 201 or 202, or (c) punish or attempt to punish any person for exercising or attempting to exercise any right or privilege secured by section 201 or 202.

Restraining orders, etc.

SEC. 204. (a) Whenever any person has engaged or there are reasonable grounds to believe that any person is about to engage in any act or practice prohibited by section 203, a civil action for preventive relief, including an application for a permanent or temporary injunction, restraining order, or other order, may be instituted by the person aggrieved and, upon timely application, the court may, in its discretion, permit the Attorney General to intervene in such civil action if he certifies that the case is of general public importance. Upon application by the complainant and in such circumstances as the court may deem just, the court may appoint an attorney for such complainant and may authorize the commencement of the civil action without the payment of fees, costs, or security.

Attorneys' fees.

(b) In any action commenced pursuant to this title, the court, in its discretion, may allow the prevailing party, other than the United States, a reasonable attorney's fee as part of the costs, and the United States shall be liable for costs the same as a private person.

Notification of State.

(c) In the case of an alleged act or practice prohibited by this title which occurs in a State, or political subdivision of a State, which has a State or local law prohibiting such act or practice and establishing or authorizing a State or local authority to grant or seek relief from such practice or to institute criminal proceedings with respect thereto upon receiving notice thereof, no civil action may be brought under subsection (a) before the expiration of thirty days after written notice of such alleged act or practice has been given to the appropriate State or local authority by registered mail or in person, provided that the court may stay proceedings in such civil action pending the termination of State or local enforcement proceedings.

Community Relations Service.

(d) In the case of an alleged act or practice prohibited by this title which occurs in a State, or political subdivision of a State, which has no State or local law prohibiting such act or practice, a civil action may be brought under subsection (a): *Provided*, That the court may refer the matter to the Community Relations Service established by title X of this Act for as long as the court believes there is a reasonable possibility of obtaining voluntary compliance, but for not more than sixty days: *Provided further*, That upon expiration of such sixty-day period, the court may extend such period for an additional period, not to exceed a cumulative total of one hundred and twenty days, if it believes there then exists a reasonable possibility of securing voluntary compliance.

Hearings and investigations.

SEC. 205. The Service is authorized to make a full investigation of any complaint referred to it by the court under section 204(d) and may hold such hearings with respect thereto as may be necessary.

The Service shall conduct any hearings with respect to any such complaint in executive session, and shall not release any testimony given therein except by agreement of all parties involved in the complaint with the permission of the court, and the Service shall endeavor to bring about a voluntary settlement between the parties.

Suits by Attorney General.

SEC. 206. (a) Whenever the Attorney General has reasonable cause to believe that any person or group of persons is engaged in a pattern or practice of resistance to the full enjoyment of any of the rights secured by this title, and that the pattern or practice is of such a nature and is intended to deny the full exercise of the rights herein described, the Attorney General may bring a civil action in the appropriate district court of the United States by filing with it a complaint (1) signed by him (or in his absence the Acting Attorney General), (2) setting forth facts pertaining to such pattern or practice, and (3) requesting such preventive relief, including an application for a permanent or temporary injunction, restraining order or other order against the person or persons responsible for such pattern or practice, as he deems necessary to insure the full enjoyment of the rights herein described.

(b) In any such proceeding the Attorney General may file with the clerk of such court a request that a court of three judges be convened to hear and determine the case. Such request by the Attorney General shall be accompanied by a certificate that, in his opinion, the case is of general public importance. A copy of the certificate and request for a three-judge court shall be immediately furnished by such clerk to the chief judge of the circuit (or in his absence, the presiding circuit judge of the circuit) in which the case is pending.

Designation of judges.

Upon receipt of the copy of such request it shall be the duty of the chief judge of the circuit or the presiding circuit judge, as the case may be, to designate immediately three judges in such circuit, of whom at least one shall be a circuit judge and another of whom shall be a district judge of the court in which the proceeding was instituted, to hear and determine such case, and it shall be the duty of the judges so designated to assign the case for hearing at the earliest practicable date, to participate in the hearing and determination thereof, and to cause the case to be in every way expedited.

Appeals.

An appeal from the final judgment of such court will lie to the Supreme Court.

In the event the Attorney General fails to file such a request in any such proceeding, it shall be the duty of the chief judge of the district (or in his absence, the acting chief judge) in which the case is pending immediately to designate a judge in such district to hear and determine the case. In the event that no judge in the district is available to hear and determine the case, the chief judge of the district, or the acting chief judge, as the case may be, shall certify this fact to the chief judge of the circuit (or in his absence, the acting chief judge) who shall then designate a district or circuit judge of the circuit to hear and determine the case.

It shall be the duty of the judge designated pursuant to this section to assign the case for hearing at the earliest practicable date and to cause the case to be in every way expedited.

District courts, jurisdiction.

SEC. 207. (a) The district courts of the United States shall have jurisdiction of proceedings instituted pursuant to this title and shall exercise the same without regard to whether the aggrieved party shall have exhausted any administrative or other remedies that may be provided by law.

Enforcement.

(b) The remedies provided in this title shall be the exclusive means of enforcing the rights based on this title, but nothing in this title shall preclude any individual or any State or local agency from asserting any right based on any other Federal or State law not inconsistent with this title, including any statute or ordinance requiring nondiscrimination in public establishments or accommodations, or from pursuing any remedy, civil or criminal, which may be available for the vindication or enforcement of such right.

TITLE III—DESEGREGATION OF PUBLIC FACILITIES

Suits by Attorney General.

SEC. 301. (a) Whenever the Attorney General receives a complaint in writing signed by an individual to the effect that he is being deprived of or threatened with the loss of his right to the equal protection of the laws, on account of his race, color, religion, or national origin, by being denied equal utilization of any public facility which is owned, operated, or managed by or on behalf of any State or subdivision thereof, other than a public school or public college as defined in section 401 of title IV hereof, and the Attorney General believes the complaint is meritorious and certifies that the signer or signers of such complaint are unable, in his judgment, to initiate and maintain appropriate legal proceedings for relief and that the institution of an action will materially further the orderly progress of desegregation in public facilities, the Attorney General is authorized to institute for or in the name of the United States a civil action in any appropriate district court of the United States against such parties and for such relief as may be appropriate, and such court shall have and shall exercise jurisdiction of proceedings instituted pursuant to this section. The Attorney General may implead as defendants such additional parties as are or become necessary to the grant of effective relief hereunder.

(b) The Attorney General may deem a person or persons unable to initiate and maintain appropriate legal proceedings within the meaning of subsection (a) of this section when such person or persons are unable, either directly or through other interested persons or organizations, to bear the expense of the litigation or to obtain effective legal representation; or whenever he is satisfied that the institution of such litigation would jeopardize the personal safety, employment, or economic standing of such person or persons, their families, or their property.

Costs, fees.

SEC. 302. In any action or proceeding under this title the United States shall be liable for costs, including a reasonable attorney's fee, the same as a private person.

SEC. 303. Nothing in this title shall affect adversely the right of any person to sue for or obtain relief in any court against discrimination in any facility covered by this title.

62 Stat. 749.

SEC. 304. A complaint as used in this title is a writing or document within the meaning of section 1001, title 18, United States Code.

TITLE IV—DESEGREGATION OF PUBLIC EDUCATION

DEFINITIONS

SEC. 401. As used in this title—

"Commissioner."

(a) "Commissioner" means the Commissioner of Education.

"Desegregation."

(b) "Desegregation" means the assignment of students to public schools and within such schools without regard to their race, color, religion, or national origin, but "desegregation" shall not mean the assignment of students to public schools in order to overcome racial imbalance.

(c) "Public school" means any elementary or secondary educational institution, and "public college" means any institution of higher education or any technical or vocational school above the secondary school level, provided that such public school or public college is operated by a State, subdivision of a State, or governmental agency within a State, or operated wholly or predominantly from or through the use of governmental funds or property, or funds or property derived from a governmental source. "Public school."

(d) "School board" means any agency or agencies which administer a system of one or more public schools and any other agency which is responsible for the assignment of students to or within such system. "School board."

SURVEY AND REPORT OF EDUCATIONAL OPPORTUNITIES

SEC. 402. The Commissioner shall conduct a survey and make a report to the President and the Congress, within two years of the enactment of this title, concerning the lack of availability of equal educational opportunities for individuals by reason of race, color, religion, or national origin in public educational institutions at all levels in the United States, its territories and possessions, and the District of Columbia. Report to the President and Congress.

TECHNICAL ASSISTANCE

SEC. 403. The Commissioner is authorized, upon the application of any school board, State, municipality, school district, or other governmental unit legally responsible for operating a public school or schools, to render technical assistance to such applicant in the preparation, adoption, and implementation of plans for the desegregation of public schools. Such technical assistance may, among other activities, include making available to such agencies information regarding effective methods of coping with special educational problems occasioned by desegregation, and making available to such agencies personnel of the Office of Education or other persons specially equipped to advise and assist them in coping with such problems.

TRAINING INSTITUTES

SEC. 404. The Commissioner is authorized to arrange, through grants or contracts, with institutions of higher education for the operation of short-term or regular session institutes for special training designed to improve the ability of teachers, supervisors, counselors, and other elementary or secondary school personnel to deal effectively with special educational problems occasioned by desegregation. Individuals who attend such an institute on a full-time basis may be paid stipends for the period of their attendance at such institute in amounts specified by the Commissioner in regulations, including allowances for travel to attend such institute. Stipends, etc.

GRANTS

SEC. 405. (a) The Commissioner is authorized, upon application of a school board, to make grants to such board to pay, in whole or in part, the cost of—

(1) giving to teachers and other school personnel inservice training in dealing with problems incident to desegregation, and

(2) employing specialists to advise in problems incident to desegregation.

(b) In determining whether to make a grant, and in fixing the amount thereof and the terms and conditions on which it will be made, the Commissioner shall take into consideration the amount available Conditions.

for grants under this section and the other applications which are pending before him; the financial condition of the applicant and the other resources available to it; the nature, extent, and gravity of its problems incident to desegregation; and such other factors as he finds relevant.

PAYMENTS

SEC. 406. Payments pursuant to a grant or contract under this title may be made (after necessary adjustments on account of previously made overpayments or underpayments) in advance or by way of reimbursement, and in such installments, as the Commissioner may determine.

SUITS BY THE ATTORNEY GENERAL

SEC. 407. (a) Whenever the Attorney General receives a complaint in writing—

(1) signed by a parent or group of parents to the effect that his or their minor children, as members of a class of persons similarly situated, are being deprived by a school board of the equal protection of the laws, or

(2) signed by an individual, or his parent, to the effect that he has been denied admission to or not permitted to continue in attendance at a public college by reason of race, color, religion, or national origin,

and the Attorney General believes the complaint is meritorious and certifies that the signer or signers of such complaint are unable, in his judgment, to initiate and maintain appropriate legal proceedings for relief and that the institution of an action will materially further the orderly achievement of desegregation in public education, the Attorney General is authorized, after giving notice of such complaint to the appropriate school board or college authority and after certifying that he is satisfied that such board or authority has had a reasonable time to adjust the conditions alleged in such complaint, to institute for or in the name of the United States a civil action in any appropriate district court of the United States against such parties and for such relief as may be appropriate, and such court shall have and shall exercise jurisdiction of proceedings instituted pursuant to this section, provided that nothing herein shall empower any official or court of the United States to issue any order seeking to achieve a racial balance in any school by requiring the transportation of pupils or students from one school to another or one school district to another in order to achieve such racial balance, or otherwise enlarge the existing power of the court to insure compliance with constitutional standards. The Attorney General may implead as defendants such additional parties as are or become necessary to the grant of effective relief hereunder.

Persons unable to initiate suits.

(b) The Attorney General may deem a person or persons unable to initiate and maintain appropriate legal proceedings within the meaning of subsection (a) of this section when such person or persons are unable, either directly or through other interested persons or organizations, to bear the expense of the litigation or to obtain effective legal representation; or whenever he is satisfied that the institution of such litigation would jeopardize the personal safety, employment, or economic standing of such person or persons, their families, or their property.

"Parent."

"Complaint."

62 Stat. 749.

(c) The term "parent" as used in this section includes any person standing in loco parentis. A "complaint" as used in this section is a writing or document within the meaning of section 1001, title 18, United States Code.

SEC. 408. In any action or proceeding under this title the United States shall be liable for costs the same as a private person.

SEC. 409. Nothing in this title shall affect adversely the right of any person to sue for or obtain relief in any court against discrimination in public education.

SEC. 410. Nothing in this title shall prohibit classification and assignment for reasons other than race, color, religion, or national origin.

TITLE V—COMMISSION ON CIVIL RIGHTS

SEC. 501. Section 102 of the Civil Rights Act of 1957 (42 U.S.C. 1975a; 71 Stat. 634) is amended to read as follows:

"RULES OF PROCEDURE OF THE COMMISSION HEARINGS

"SEC. 102. (a) At least thirty days prior to the commencement of any hearing, the Commission shall cause to be published in the Federal Register notice of the date on which such hearing is to commence, the place at which it is to be held and the subject of the hearing. The Chairman, or one designated by him to act as Chairman at a hearing of the Commission, shall announce in an opening statement the subject of the hearing. Publication in Federal Register.

"(b) A copy of the Commission's rules shall be made available to any witness before the Commission, and a witness compelled to appear before the Commission or required to produce written or other matter shall be served with a copy of the Commission's rules at the time of service of the subpena.

"(c) Any person compelled to appear in person before the Commission shall be accorded the right to be accompanied and advised by counsel, who shall have the right to subject his client to reasonable examination, and to make objections on the record and to argue briefly the basis for such objections. The Commission shall proceed with reasonable dispatch to conclude any hearing in which it is engaged. Due regard shall be had for the convenience and necessity of witnesses. Right of counsel.

"(d) The Chairman or Acting Chairman may punish breaches of order and decorum by censure and exclusion from the hearings.

"(e) If the Commission determines that evidence or testimony at any hearing may tend to defame, degrade, or incriminate any person, it shall receive such evidence or testimony or summary of such evidence or testimony in executive session. The Commission shall afford any person defamed, degraded, or incriminated by such evidence or testimony an opportunity to appear and be heard in executive session, with a reasonable number of additional witnesses requested by him, before deciding to use such evidence or testimony. In the event the Commission determines to release or use such evidence or testimony in such manner as to reveal publicly the identity of the person defamed, degraded, or incriminated, such evidence or testimony, prior to such public release or use, shall be given at a public session, and the Commission shall afford such person an opportunity to appear as a voluntary witness or to file a sworn statement in his behalf and to submit brief and pertinent sworn statements of others. The Commission shall receive and dispose of requests from such person to subpena additional witnesses. Executive sessions.

"(f) Except as provided in sections 102 and 105(f) of this Act, the Chairman shall receive and the Commission shall dispose of requests to subpena additional witnesses.

"(g) No evidence or testimony or summary of evidence or testimony taken in executive session may be released or used in public Testimony, release restrictions.

sessions without the consent of the Commission. Whoever releases or uses in public without the consent of the Commission such evidence or testimony taken in executive session shall be fined not more than $1,000, or imprisoned for not more than one year.

"(h) In the discretion of the Commission, witnesses may submit brief and pertinent sworn statements in writing for inclusion in the record. The Commission shall determine the pertinency of testimony and evidence adduced at its hearings.

Transcript copies.

"(i) Every person who submits data or evidence shall be entitled to retain or, on payment of lawfully prescribed costs, procure a copy or transcript thereof, except that a witness in a hearing held in executive session may for good cause be limited to inspection of the official transcript of his testimony. Transcript copies of public sessions may be obtained by the public upon the payment of the cost thereof. An accurate transcript shall be made of the testimony of all witnesses at all hearings, either public or executive sessions, of the Commission or of any subcommittee thereof.

Witness fees.

"(j) A witness attending any session of the Commission shall receive $6 for each day's attendance and for the time necessarily occupied in going to and returning from the same, and 10 cents per mile for going from and returning to his place of residence. Witnesses who attend at points so far removed from their respective residences as to prohibit return thereto from day to day shall be entitled to an additional allowance of $10 per day for expenses of subsistence, including the time necessarily occupied in going to and returning from the place of attendance. Mileage payments shall be tendered to the witness upon service of a subpena issued on behalf of the Commission or any subcommittee thereof.

Subpena of witnesses.

"(k) The Commission shall not issue any subpena for the attendance and testimony of witnesses or for the production of written or other matter which would require the presence of the party subpenaed at a hearing to be held outside of the State wherein the witness is found or resides or is domiciled or transacts business, or has appointed an agent for receipt of service of process except that, in any event, the Commission may issue subpenas for the attendance and testimony of witnesses and the production of written or other matter at a hearing held within fifty miles of the place where the witness is found or resides or is domiciled or transacts business or has appointed an agent for receipt of service of process.

Organization statement, etc. Publication in Federal Register.

"(l) The Commission shall separately state and currently publish in the Federal Register (1) descriptions of its central and field organization including the established places at which, and methods whereby, the public may secure information or make requests; (2) statements of the general course and method by which its functions are channeled and determined, and (3) rules adopted as authorized by law. No person shall in any manner be subject to or required to resort to rules, organization, or procedure not so published."

SEC. 502. Section 103(a) of the Civil Rights Act of 1957 (42 U.S.C. 1975b(a); 71 Stat. 634) is amended to read as follows:

Payments to members.

"SEC. 103. (a) Each member of the Commission who is not otherwise in the service of the Government of the United States shall receive the sum of $75 per day for each day spent in the work of the Commission, shall be paid actual travel expenses, and per diem in lieu of subsistence expenses when away from his usual place of residence, in accordance with section 5 of the Administrative Expenses Act of 1946, as amended (5 U.S.C. 73b-2; 60 Stat. 808)."

75 Stat. 339, 340.

SEC. 503. Section 103(b) of the Civil Rights Act of 1957 (42 U.S.C. 1975b(b); 71 Stat. 634) is amended to read as follows:

"(b) Each member of the Commission who is otherwise in the service of the Government of the United States shall serve without compensation in addition to that received for such other service, but while engaged in the work of the Commission shall be paid actual travel expenses, and per diem in lieu of subsistence expenses when away from his usual place of residence, in accordance with the provisions of the Travel Expenses Act of 1949, as amended (5 U.S.C. 835–42; 63 Stat. 166)." 75 Stat. 339, 340.

SEC. 504. (a) Section 104(a) of the Civil Rights Act of 1957 (42 U.S.C. 1975c(a); 71 Stat. 635), as amended, is further amended to read as follows:

"DUTIES OF THE COMMISSION

"SEC. 104. (a) The Commission shall—

"(1) investigate allegations in writing under oath or affirmation that certain citizens of the United States are being deprived of their right to vote and have that vote counted by reason of their color, race, religion, or national origin; which writing, under oath or affirmation, shall set forth the facts upon which such belief or beliefs are based;

"(2) study and collect information concerning legal developments constituting a denial of equal protection of the laws under the Constitution because of race, color, religion or national origin or in the administration of justice;

"(3) appraise the laws and policies of the Federal Government with respect to denials of equal protection of the laws under the Constitution because of race, color, religion or national origin or in the administration of justice;

"(4) serve as a national clearinghouse for information in respect to denials of equal protection of the laws because of race, color, religion or national origin, including but not limited to the fields of voting, education, housing, employment, the use of public facilities, and transportation, or in the administration of justice;

"(5) investigate allegations, made in writing and under oath or affirmation, that citizens of the United States are unlawfully being accorded or denied the right to vote, or to have their votes properly counted, in any election of presidential electors, Members of the United States Senate, or of the House of Representatives, as a result of any patterns or practice of fraud or discrimination in the conduct of such election; and

"(6) Nothing in this or any other Act shall be construed as authorizing the Commission, its Advisory Committees, or any person under its supervision or control to inquire into or investigate any membership practices or internal operations of any fraternal organization, any college or university fraternity or sorority, any private club or any religious organization."

(b) Section 104(b) of the Civil Rights Act of 1957 (42 U.S.C. 1975c(b); 71 Stat. 635), as amended, is further amended by striking out the present subsection "(b)" and by substituting therefor: 77 Stat. 271.

"(b) The Commission shall submit interim reports to the President and to the Congress at such times as the Commission, the Congress or the President shall deem desirable, and shall submit to the President and to the Congress a final report of its activities, findings, and recommendations not later than January 31, 1968." Reports to the President and Congress.

SEC. 505. Section 105(a) of the Civil Rights Act of 1957 (42 U.S.C. 1975d(a); 71 Stat. 636) is amended by striking out in the last sentence thereof "$50 per diem" and inserting in lieu thereof "$75 per diem."

Powers.

SEC. 506. Section 105(f) and section 105(g) of the Civil Rights Act of 1957 (42 U.S.C. 1975d (f) and (g); 71 Stat. 636) are amended to read as follows:

"(f) The Commission, or on the authorization of the Commission any subcommittee of two or more members, at least one of whom shall be of each major political party, may, for the purpose of carrying out the provisions of this Act, hold such hearings and act at such times and places as the Commission or such authorized subcommittee may deem advisable. Subpenas for the attendance and testimony of witnesses or the production of written or other matter may be issued in accordance with the rules of the Commission as contained in section 102 (j) and (k) of this Act, over the signature of the Chairman of the Commission or of such subcommittee, and may be served by any person designated by such Chairman. The holding of hearings by the Commission, or the appointment of a subcommittee to hold hearings pursuant to this subparagraph, must be approved by a majority of the Commission, or by a majority of the members present at a meeting at which at least a quorum of four members is present.

Ante, p. 250.

"(g) In case of contumacy or refusal to obey a subpena, any district court of the United States or the United States court of any territory or possession, or the District Court of the United States for the District of Columbia, within the jurisdiction of which the inquiry is carried on or within the jurisdiction of which said person guilty of contumacy or refusal to obey is found or resides or is domiciled or transacts business, or has appointed an agent for receipt of service of process, upon application by the Attorney General of the United States shall have jurisdiction to issue to such person an order requiring such person to appear before the Commission or a subcommittee thereof, there to produce pertinent, relevant and nonprivileged evidence if so ordered, or there to give testimony touching the matter under investigation; and any failure to obey such order of the court may be punished by said court as a contempt thereof."

SEC. 507. Section 105 of the Civil Rights Act of 1957 (42 U.S.C. 1975d; 71 Stat. 636), as amended by section 401 of the Civil Rights Act of 1960 (42 U.S.C. 1975d(h); 74 Stat. 89), is further amended by adding a new subsection at the end to read as follows:

"(i) The Commission shall have the power to make such rules and regulations as are necessary to carry out the purposes of this Act."

TITLE VI—NONDISCRIMINATION IN FEDERALLY ASSISTED PROGRAMS

SEC. 601. No person in the United States shall, on the ground of race, color, or national origin, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any program or activity receiving Federal financial assistance.

Rules governing grants, loans, and contracts.

SEC. 602. Each Federal department and agency which is empowered to extend Federal financial assistance to any program or activity, by way of grant, loan, or contract other than a contract of insurance or guaranty, is authorized and directed to effectuate the provisions of section 601 with respect to such program or activity by issuing rules, regulations, or orders of general applicability which shall be consistent with achievement of the objectives of the statute authorizing the financial assistance in connection with which the action is taken.

Approval by President.

No such rule, regulation, or order shall become effective unless and until approved by the President. Compliance with any requirement adopted pursuant to this section may be effected (1) by the termination of or refusal to grant or to continue assistance under such program or activity to any recipient as to whom there has been an express find-

ing on the record, after opportunity for hearing, of a failure to comply with such requirement, but such termination or refusal shall be limited to the particular political entity, or part thereof, or other recipient as to whom such a finding has been made and, shall be limited in its effect to the particular program, or part thereof, in which such noncompliance has been so found, or (2) by any other means authorized by law: *Provided, however*, That no such action shall be taken until the department or agency concerned has advised the appropriate person or persons of the failure to comply with the requirement and has determined that compliance cannot be secured by voluntary means. In the case of any action terminating, or refusing to grant or continue, assistance because of failure to comply with a requirement imposed pursuant to this section, the head of the Federal department or agency shall file with the committees of the House and Senate having legislative jurisdiction over the program or activity involved a full written report of the circumstances and the grounds for such action. No such action shall become effective until thirty days have elapsed after the filing of such report.

Termination.

SEC. 603. Any department or agency action taken pursuant to section 602 shall be subject to such judicial review as may otherwise be provided by law for similar action taken by such department or agency on other grounds. In the case of action, not otherwise subject to judicial review, terminating or refusing to grant or to continue financial assistance upon a finding of failure to comply with any requirement imposed pursuant to section 602, any person aggrieved (including any State or political subdivision thereof and any agency of either) may obtain judicial review of such action in accordance with section 10 of the Administrative Procedure Act, and such action shall not be deemed committed to unreviewable agency discretion within the meaning of that section.

Judicial review.

60 Stat. 243.
5 USC 1009.

SEC. 604. Nothing contained in this title shall be construed to authorize action under this title by any department or agency with respect to any employment practice of any employer, employment agency, or labor organization except where a primary objective of the Federal financial assistance is to provide employment.

SEC. 605. Nothing in this title shall add to or detract from any existing authority with respect to any program or activity under which Federal financial assistance is extended by way of a contract of insurance or guaranty.

TITLE VII—EQUAL EMPLOYMENT OPPORTUNITY

DEFINITIONS

SEC. 701. For the purposes of this title—

(a) The term "person" includes one or more individuals, labor unions, partnerships, associations, corporations, legal representatives, mutual companies, joint-stock companies, trusts, unincorporated organizations, trustees, trustees in bankruptcy, or receivers.

"Person."

(b) The term "employer" means a person engaged in an industry affecting commerce who has twenty-five or more employees for each working day in each of twenty or more calendar weeks in the current or preceding calendar year, and any agent of such a person, but such term does not include (1) the United States, a corporation wholly owned by the Government of the United States, an Indian tribe, or a State or political subdivision thereof, (2) a bona fide private membership club (other than a labor organization) which is exempt from taxation under section 501(c) of the Internal Revenue Code of 1954: *Provided*, That during the first year after the effective date prescribed in subsection (a) of section 716, persons having fewer than one hun-

"Employer."

68A Stat. 163; 74 Stat. 534.
26 USC 501.

dred employees (and their agents) shall not be considered employers, and, during the second year after such date, persons having fewer than seventy-five employees (and their agents) shall not be considered employers, and, during the third year after such date, persons having fewer than fifty employees (and their agents) shall not be considered employers: *Provided further*, That it shall be the policy of the United States to insure equal employment opportunities for Federal employees without discrimination because of race, color, religion, sex or national origin and the President shall utilize his existing authority to effectuate this policy.

"Employment agency."

(c) The term "employment agency" means any person regularly undertaking with or without compensation to procure employees for an employer or to procure for employees opportunities to work for an employer and includes an agent of such a person; but shall not include an agency of the United States, or an agency of a State or political subdivision of a State, except that such term shall include the United States Employment Service and the system of State and local employment services receiving Federal assistance.

"Labor organization."

(d) The term "labor organization" means a labor organization engaged in an industry affecting commerce, and any agent of such an organization, and includes any organization of any kind, any agency, or employee representation committee, group, association, or plan so engaged in which employees participate and which exists for the purpose, in whole or in part, of dealing with employers concerning grievances, labor disputes, wages, rates of pay, hours, or other terms or conditions of employment, and any conference, general committee, joint or system board, or joint council so engaged which is subordinate to a national or international labor organization.

(e) A labor organization shall be deemed to be engaged in an industry affecting commerce if (1) it maintains or operates a hiring hall or hiring office which procures employees for an employer or procures for employees opportunities to work for an employer, or (2) the number of its members (or, where it is a labor organization composed of other labor organizations or their representatives, if the aggregate number of the members of such other labor organization) is (A) one hundred or more during the first year after the effective date prescribed in subsection (a) of section 716, (B) seventy-five or more during the second year after such date or fifty or more during the third year, or (C) twenty-five or more thereafter, and such labor organization—

61 Stat. 136.
29 USC 167.
44 Stat. 577;
49 Stat. 1189.
45 USC 151.

(1) is the certified representative of employees under the provisions of the National Labor Relations Act, as amended, or the Railway Labor Act, as amended;

(2) although not certified, is a national or international labor organization or a local labor organization recognized or acting as the representative of employees of an employer or employers engaged in an industry affecting commerce; or

(3) has chartered a local labor organization or subsidiary body which is representing or actively seeking to represent employees of employers within the meaning of paragraph (1) or (2); or

(4) has been chartered by a labor organization representing or actively seeking to represent employees within the meaning of paragraph (1) or (2) as the local or subordinate body through which such employees may enjoy membership or become affiliated with such labor organization; or

(5) is a conference, general committee, joint or system board, or joint council subordinate to a national or international labor organization, which includes a labor organization engaged in an

industry affecting commerce within the meaning of any of the preceding paragraphs of this subsection.

"Employee." (f) The term "employee" means an individual employed by an employer.

"Commerce." (g) The term "commerce" means trade, traffic, commerce, transportation, transmission, or communication among the several States; or between a State and any place outside thereof; or within the District of Columbia, or a possession of the United States; or between points in the same State but through a point outside thereof.

"Industry affecting commerce." (h) The term "industry affecting commerce" means any activity, business, or industry in commerce or in which a labor dispute would hinder or obstruct commerce or the free flow of commerce and includes any activity or industry "affecting commerce" within the meaning of the Labor-Management Reporting and Disclosure Act of 1959.

73 Stat. 519. 29 USC 401 note.

"State." (i) The term "State" includes a State of the United States, the District of Columbia, Puerto Rico, the Virgin Islands, American Samoa, Guam, Wake Island, the Canal Zone, and Outer Continental Shelf lands defined in the Outer Continental Shelf Lands Act.

67 Stat. 462. 43 USC 1331 note.

EXEMPTION

Religious organizations, etc. SEC. 702. This title shall not apply to an employer with respect to the employment of aliens outside any State, or to a religious corporation, association, or society with respect to the employment of individuals of a particular religion to perform work connected with the carrying on by such corporation, association, or society of its religious activities or to an educational institution with respect to the employment of individuals to perform work connected with the educational activities of such institution.

DISCRIMINATION BECAUSE OF RACE, COLOR, RELIGION, SEX, OR NATIONAL ORIGIN

Unlawful practices. SEC. 703. (a) It shall be an unlawful employment practice for an employer—

Employers. (1) to fail or refuse to hire or to discharge any individual, or otherwise to discriminate against any individual with respect to his compensation, terms, conditions, or privileges of employment, because of such individual's race, color, religion, sex, or national origin; or

(2) to limit, segregate, or classify his employees in any way which would deprive or tend to deprive any individual of employment opportunities or otherwise adversely affect his status as an employee, because of such individual's race, color, religion, sex, or national origin.

Employment agency. (b) It shall be an unlawful employment practice for an employment agency to fail or refuse to refer for employment, or otherwise to discriminate against, any individual because of his race, color, religion, sex, or national origin, or to classify or refer for employment any individual on the basis of his race, color, religion, sex, or national origin.

Labor organization. (c) It shall be an unlawful employment practice for a labor organization—

(1) to exclude or to expel from its membership, or otherwise to discriminate against, any individual because of his race, color, religion, sex, or national origin;

(2) to limit, segregate, or classify its membership, or to classify or fail or refuse to refer for employment any individual, in any

way which would deprive or tend to deprive any individual of employment opportunities, or would limit such employment opportunities or otherwise adversely affect his status as an employee or as an applicant for employment, because of such individual's race, color, religion, sex, or national origin; or

(3) to cause or attempt to cause an employer to discriminate against an individual in violation of this section.

Training programs.

(d) It shall be an unlawful employment practice for any employer, labor organization, or joint labor-management committee controlling apprenticeship or other training or retraining, including on-the-job training programs to discriminate against any individual because of his race, color, religion, sex, or national origin in admission to, or employment in, any program established to provide apprenticeship or other training.

Exceptions.

(e) Notwithstanding any other provision of this title, (1) it shall not be an unlawful employment practice for an employer to hire and employ employees, for an employment agency to classify, or refer for employment any individual, for a labor organization to classify its membership or to classify or refer for employment any individual, or for an employer, labor organization, or joint labor-management committee controlling apprenticeship or other training or retraining programs to admit or employ any individual in any such program, on the basis of his religion, sex, or national origin in those certain instances where religion, sex, or national origin is a bona fide occupational qualification reasonably necessary to the normal operation of that particular business or enterprise, and (2) it shall not be an unlawful employment practice for a school, college, university, or other educational institution or institution of learning to hire and employ employees of a particular religion if such school, college, university, or other educational institution or institution of learning is, in whole or in substantial part, owned, supported, controlled, or managed by a particular religion or by a particular religious corporation, association, or society, or if the curriculum of such school, college, university, or other educational institution or institution of learning is directed toward the propagation of a particular religion.

(f) As used in this title, the phrase "unlawful employment practice" shall not be deemed to include any action or measure taken by an employer, labor organization, joint labor-management committee, or employment agency with respect to an individual who is a member of the Communist Party of the United States or of any other organization required to register as a Communist-action or Communist-front organization by final order of the Subversive Activities Control Board pursuant to the Subversive Activities Control Act of 1950.

64 Stat. 987. 50 USC 781 note.

(g) Notwithstanding any other provision of this title, it shall not be an unlawful employment practice for an employer to fail or refuse to hire and employ any individual for any position, for an employer to discharge any individual from any position, or for an employment agency to fail or refuse to refer any individual for employment in any position, or for a labor organization to fail or refuse to refer any individual for employment in any position, if—

(1) the occupancy of such position, or access to the premises in or upon which any part of the duties of such position is performed or is to be performed, is subject to any requirement imposed in the interest of the national security of the United States under any security program in effect pursuant to or administered under any statute of the United States or any Executive order of the President; and

(2) such individual has not fulfilled or has ceased to fulfill that requirement.

(h) Notwithstanding any other provision of this title, it shall not be an unlawful employment practice for an employer to apply different standards of compensation, or different terms, conditions, or privileges of employment pursuant to a bona fide seniority or merit system, or a system which measures earnings by quantity or quality of production or to employees who work in different locations, provided that such differences are not the result of an intention to discriminate because of race, color, religion, sex, or national origin, nor shall it be an unlawful employment practice for an employer to give and to act upon the results of any professionally developed ability test provided that such test, its administration or action upon the results is not designed, intended or used to discriminate because of race, color, religion, sex or national origin. It shall not be an unlawful employment practice under this title for any employer to differentiate upon the basis of sex in determining the amount of the wages or compensation paid or to be paid to employees of such employer if such differentiation is authorized by the provisions of section 6(d) of the Fair Labor Standards Act of 1938, as amended (29 U.S.C. 206(d)).

77 Stat. 56.
29 USC 206.

(i) Nothing contained in this title shall apply to any business or enterprise on or near an Indian reservation with respect to any publicly announced employment practice of such business or enterprise under which a preferential treatment is given to any individual because he is an Indian living on or near a reservation.

Indians.

(j) Nothing contained in this title shall be interpreted to require any employer, employment agency, labor organization, or joint labor-management committee subject to this title to grant preferential treatment to any individual or to any group because of the race, color, religion, sex, or national origin of such individual or group on account of an imbalance which may exist with respect to the total number or percentage of persons of any race, color, religion, sex, or national origin employed by any employer, referred or classified for employment by any employment agency or labor organization, admitted to membership or classified by any labor organization, or admitted to, or employed in, any apprenticeship or other training program, in comparison with the total number or percentage of persons of such race, color, religion, sex, or national origin in any community, State, section, or other area, or in the available work force in any community, State, section, or other area.

Preferential treatment.

OTHER UNLAWFUL EMPLOYMENT PRACTICES

SEC. 704. (a) It shall be an unlawful employment practice for an employer to discriminate against any of his employees or applicants for employment, for an employment agency to discriminate against any individual, or for a labor organization to discriminate against any member thereof or applicant for membership, because he has opposed any practice made an unlawful employment practice by this title, or because he has made a charge, testified, assisted, or participated in any manner in an investigation, proceeding, or hearing under this title.

(b) It shall be an unlawful employment practice for an employer, labor organization, or employment agency to print or publish or cause to be printed or published any notice or advertisement relating to employment by such an employer or membership in or any classification or referral for employment by such a labor organization, or relating to any classification or referral for employment by such an employment agency, indicating any preference, limitation, specification, or discrimination, based on race, color, religion, sex, or national origin, except that such a notice or advertisement may indicate a preference, limitation, specification, or discrimination based on reli-

gion, sex, or national origin when religion, sex, or national origin is a bona fide occupational qualification for employment.

EQUAL EMPLOYMENT OPPORTUNITY COMMISSION

Establishment.

SEC. 705. (a) There is hereby created a Commission to be known as the Equal Employment Opportunity Commission, which shall be composed of five members, not more than three of whom shall be members of the same political party, who shall be appointed by the President by and with the advice and consent of the Senate. One of the original members shall be appointed for a term of one year, one for a term of two years, one for a term of three years, one for a term of four years, and one for a term of five years, beginning from the date of enactment of this title, but their successors shall be appointed for terms of five years each, except that any individual chosen to fill a vacancy shall be appointed only for the unexpired term of the member whom he shall succeed. The President shall designate one member to serve as Chairman of the Commission, and one member to serve as Vice Chairman. The Chairman shall be responsible on behalf of the Commission for the administrative operations of the Commission, and shall appoint, in accordance with the civil service laws, such officers, agents, attorneys, and employees as it deems necessary to assist it in the performance of its functions and to fix their compensation in accordance with the Classification Act of 1949, as amended. The Vice Chairman shall act as Chairman in the absence or disability of the Chairman or in the event of a vacancy in that office.

Term of office.

Post, p. 400.
5 USC 1071 note.

(b) A vacancy in the Commission shall not impair the right of the remaining members to exercise all the powers of the Commission and three members thereof shall constitute a quorum.

(c) The Commission shall have an official seal which shall be judicially noticed.

Reports to the President and Congress.

(d) The Commission shall at the close of each fiscal year report to the Congress and to the President concerning the action it has taken; the names, salaries, and duties of all individuals in its employ and the moneys it has disbursed; and shall make such further reports on the cause of and means of eliminating discrimination and such recommendations for further legislation as may appear desirable.

70 Stat. 736.
5 USC 2201 note.

(e) The Federal Executive Pay Act of 1956, as amended (5 U.S.C. 2201–2209), is further amended—

(1) by adding to section 105 thereof (5 U.S.C. 2204) the following clause:

"(32) Chairman, Equal Employment Opportunity Commission"; and

70 Stat. 737.
5 USC 2205.

(2) by adding to clause (45) of section 106(a) thereof (5 U.S.C. 2205(a)) the following: "Equal Employment Opportunity Commission (4)."

(f) The principal office of the Commission shall be in or near the District of Columbia, but it may meet or exercise any or all its powers at any other place. The Commission may establish such regional or State offices as it deems necessary to accomplish the purpose of this title.

Powers.

(g) The Commission shall have power—

(1) to cooperate with and, with their consent, utilize regional, State, local, and other agencies, both public and private, and individuals;

(2) to pay to witnesses whose depositions are taken or who are summoned before the Commission or any of its agents the same witness and mileage fees as are paid to witnesses in the courts of the United States;

(3) to furnish to persons subject to this title such technical assistance as they may request to further their compliance with this title or an order issued thereunder;

(4) upon the request of (i) any employer, whose employees or some of them, or (ii) any labor organization, whose members or some of them, refuse or threaten to refuse to cooperate in effectuating the provisions of this title, to assist in such effectuation by conciliation or such other remedial action as is provided by this title;

(5) to make such technical studies as are appropriate to effectuate the purposes and policies of this title and to make the results of such studies available to the public;

(6) to refer matters to the Attorney General with recommendations for intervention in a civil action brought by an aggrieved party under section 706, or for the institution of a civil action by the Attorney General under section 707, and to advise, consult, and assist the Attorney General on such matters.

(h) Attorneys appointed under this section may, at the direction of the Commission, appear for and represent the Commission in any case in court.

(i) The Commission shall, in any of its educational or promotional activities, cooperate with other departments and agencies in the performance of such educational and promotional activities.

(j) All officers, agents, attorneys, and employees of the Commission shall be subject to the provisions of section 9 of the Act of August 2, 1939, as amended (the Hatch Act), notwithstanding any exemption contained in such section.

53 Stat. 1148; 64 Stat. 475. 5 USC 118i.

PREVENTION OF UNLAWFUL EMPLOYMENT PRACTICES

SEC. 706. (a) Whenever it is charged in writing under oath by a person claiming to be aggrieved, or a written charge has been filed by a member of the Commission where he has reasonable cause to believe a violation of this title has occurred (and such charge sets forth the facts upon which it is based) that an employer, employment agency, or labor organization has engaged in an unlawful employment practice, the Commission shall furnish such employer, employment agency, or labor organization (hereinafter referred to as the "respondent") with a copy of such charge and shall make an investigation of such charge, provided that such charge shall not be made public by the Commission. If the Commission shall determine, after such investigation, that there is reasonable cause to believe that the charge is true, the Commission shall endeavor to eliminate any such alleged unlawful employment practice by informal methods of conference, conciliation, and persuasion. Nothing said or done during and as a part of such endeavors may be made public by the Commission without the written consent of the parties, or used as evidence in a subsequent proceeding. Any officer or employee of the Commission, who shall make public in any manner whatever any information in violation of this subsection shall be deemed guilty of a misdemeanor and upon conviction thereof shall be fined not more than $1,000 or imprisoned not more than one year.

Legal proceedings.

(b) In the case of an alleged unlawful employment practice occurring in a State, or political subdivision of a State, which has a State or local law prohibiting the unlawful employment practice alleged and establishing or authorizing a State or local authority to grant or seek relief from such practice or to institute criminal proceedings with respect thereto upon receiving notice thereof, no charge may be filed under subsection (a) by the person aggrieved before the expira-

tion of sixty days after proceedings have been commenced under the State or local law, unless such proceedings have been earlier terminated, provided that such sixty-day period shall be extended to one hundred and twenty days during the first year after the effective date of such State or local law. If any requirement for the commencement of such proceedings is imposed by a State or local authority other than a requirement of the filing of a written and signed statement of the facts upon which the proceeding is based, the proceeding shall be deemed to have been commenced for the purposes of this subsection at the time such statement is sent by registered mail to the appropriate State or local authority.

Time requirements.

(c) In the case of any charge filed by a member of the Commission alleging an unlawful employment practice occurring in a State or political subdivision of a State, which has a State or local law prohibiting the practice alleged and establishing or authorizing a State or local authority to grant or seek relief from such practice or to institute criminal proceedings with respect thereto upon receiving notice thereof, the Commission shall, before taking any action with respect to such charge, notify the appropriate State or local officials and, upon request, afford them a reasonable time, but not less than sixty days (provided that such sixty-day period shall be extended to one hundred and twenty days during the first year after the effective day of such State or local law), unless a shorter period is requested, to act under such State or local law to remedy the practice alleged.

(d) A charge under subsection (a) shall be filed within ninety days after the alleged unlawful employment practice occurred, except that in the case of an unlawful employment practice with respect to which the person aggrieved has followed the procedure set out in subsection (b), such charge shall be filed by the person aggrieved within two hundred and ten days after the alleged unlawful employment practice occurred, or within thirty days after receiving notice that the State or local agency has terminated the proceedings under the State or local law, whichever is earlier, and a copy of such charge shall be filed by the Commission with the State or local agency.

(e) If within thirty days after a charge is filed with the Commission or within thirty days after expiration of any period of reference under subsection (c) (except that in either case such period may be extended to not more than sixty days upon a determination by the Commission that further efforts to secure voluntary compliance are warranted), the Commission has been unable to obtain voluntary compliance with this title, the Commission shall so notify the person aggrieved and a civil action may, within thirty days thereafter, be brought against the respondent named in the charge (1) by the person claiming to be aggrieved, or (2) if such charge was filed by a member of the Commission, by any person whom the charge alleges was aggrieved by the alleged unlawful employment practice. Upon application by the complainant and in such circumstances as the court may deem just, the court may appoint an attorney for such complainant and may authorize the commencement of the action without the payment of fees, costs, or security. Upon timely application, the court may, in its discretion, permit the Attorney General to intervene in such civil action if he certifies that the case is of general public importance. Upon request, the court may, in its discretion, stay further proceedings for not more than sixty days pending the termination of State or local proceedings described in subsection (b) or the efforts of the Commission to obtain voluntary compliance.

Courts. Jurisdiction.

(f) Each United States district court and each United States court of a place subject to the jurisdiction of the United States shall

have jurisdiction of actions brought under this title. Such an action may be brought in any judicial district in the State in which the unlawful employment practice is alleged to have been committed, in the judicial district in which the employment records relevant to such practice are maintained and administered, or in the judicial district in which the plaintiff would have worked but for the alleged unlawful employment practice, but if the respondent is not found within any such district, such an action may be brought within the judicial district in which the respondent has his principal office. For purposes of sections 1404 and 1406 of title 28 of the United States Code, the judicial district in which the respondent has his principal office shall in all cases be considered a district in which the action might have been brought.

62 Stat. 937; 74 Stat. 912; 76A Stat. 699.

(g) If the court finds that the respondent has intentionally engaged in or is intentionally engaging in an unlawful employment practice charged in the complaint, the court may enjoin the respondent from engaging in such unlawful employment practice, and order such affirmative action as may be appropriate, which may include reinstatement or hiring of employees, with or without back pay (payable by the employer, employment agency, or labor organization, as the case may be, responsible for the unlawful employment practice). Interim earnings or amounts earnable with reasonable diligence by the person or persons discriminated against shall operate to reduce the back pay otherwise allowable. No order of the court shall require the admission or reinstatement of an individual as a member of a union or the hiring, reinstatement, or promotion of an individual as an employee, or the payment to him of any back pay, if such individual was refused admission, suspended, or expelled or was refused employment or advancement or was suspended or discharged for any reason other than discrimination on account of race, color, religion, sex or national origin or in violation of section 704(a).

(h) The provisions of the Act entitled "An Act to amend the Judicial Code and to define and limit the jurisdiction of courts sitting in equity, and for other purposes," approved March 23, 1932 (29 U.S.C. 101–115), shall not apply with respect to civil actions brought under this section.

47 Stat. 70.

(i) In any case in which an employer, employment agency, or labor organization fails to comply with an order of a court issued in a civil action brought under subsection (e), the Commission may commence proceedings to compel compliance with such order.

(j) Any civil action brought under subsection (e) and any proceedings brought under subsection (i) shall be subject to appeal as provided in sections 1291 and 1292, title 28, United States Code.

62 Stat. 929; 65 Stat. 726; 72 Stat. 348, 1770.

(k) In any action or proceeding under this title the court, in its discretion, may allow the prevailing party, other than the Commission or the United States, a reasonable attorney's fee as part of the costs, and the Commission and the United States shall be liable for costs the same as a private person.

Costs, fees.

SEC. 707. (a) Whenever the Attorney General has reasonable cause to believe that any person or group of persons is engaged in a pattern or practice of resistance to the full enjoyment of any of the rights secured by this title, and that the pattern or practice is of such a nature and is intended to deny the full exercise of the rights herein described, the Attorney General may bring a civil action in the appropriate district court of the United States by filing with it a complaint (1) signed by him (or in his absence the Acting Attorney General), (2) setting forth facts pertaining to such pattern or practice, and (3) requesting such relief, including an application for a permanent or temporary injunction, restraining order or other order against the

Suits by Attorney General.

person or persons responsible for such pattern or practice, as he deems necessary to insure the full enjoyment of the rights herein described.

(b) The district courts of the United States shall have and shall exercise jurisdiction of proceedings instituted pursuant to this section, and in any such proceeding the Attorney General may file with the clerk of such court a request that a court of three judges be convened to hear and determine the case. Such request by the Attorney General shall be accompanied by a certificate that, in his opinion, the case is of general public importance. A copy of the certificate and request for a three-judge court shall be immediately furnished by such clerk to the chief judge of the circuit (or in his absence, the presiding circuit judge of the circuit) in which the case is pending. Upon receipt of such request it shall be the duty of the chief judge of the circuit or the presiding circuit judge, as the case may be, to designate immediately three judges in such circuit, of whom at least one shall be a circuit judge and another of whom shall be a district judge of the court in which the proceeding was instituted, to hear and determine such case, and it shall be the duty of the judges so designated to assign the case for hearing at the earliest practicable date, to participate in the hearing and determination thereof, and to cause the case to be in every way expedited. An appeal from the final judgment of such court will lie to the Supreme Court.

In the event the Attorney General fails to file such a request in any such proceeding, it shall be the duty of the chief judge of the district (or in his absence, the acting chief judge) in which the case is pending immediately to designate a judge in such district to hear and determine the case. In the event that no judge in the district is available to hear and determine the case, the chief judge of the district, or the acting chief judge, as the case may be, shall certify this fact to the chief judge of the circuit (or in his absence, the acting chief judge) who shall then designate a district or circuit judge of the circuit to hear and determine the case.

It shall be the duty of the judge designated pursuant to this section to assign the case for hearing at the earliest practicable date and to cause the case to be in every way expedited.

EFFECT ON STATE LAWS

SEC. 708. Nothing in this title shall be deemed to exempt or relieve any person from any liability, duty, penalty, or punishment provided by any present or future law of any State or political subdivision of a State, other than any such law which purports to require or permit the doing of any act which would be an unlawful employment practice under this title.

INVESTIGATIONS, INSPECTIONS, RECORDS, STATE AGENCIES

SEC. 709. (a) In connection with any investigation of a charge filed under section 706, the Commission or its designated representative shall at all reasonable times have access to, for the purposes of examination, and the right to copy any evidence of any person being investigated or proceeded against that relates to unlawful employment practices covered by this title and is relevant to the charge under investigation.

Agreements, State and local agencies.

(b) The Commission may cooperate with State and local agencies charged with the administration of State fair employment practices laws and, with the consent of such agencies, may for the purpose of carrying out its functions and duties under this title and within the limitation of funds appropriated specifically for such purpose, utilize the services of such agencies and their employees and, notwithstand-

ing any other provision of law, may reimburse such agencies and their employees for services rendered to assist the Commission in carrying out this title. In furtherance of such cooperative efforts, the Commission may enter into written agreements with such State or local agencies and such agreements may include provisions under which the Commission shall refrain from processing a charge in any cases or class of cases specified in such agreements and under which no person may bring a civil action under section 706 in any cases or class of cases so specified, or under which the Commission shall relieve any person or class of persons in such State or locality from requirements imposed under this section. The Commission shall rescind any such agreement whenever it determines that the agreement no longer serves the interest of effective enforcement of this title.

Records.

(c) Except as provided in subsection (d), every employer, employment agency, and labor organization subject to this title shall (1) make and keep such records relevant to the determinations of whether unlawful employment practices have been or are being committed, (2) preserve such records for such periods, and (3) make such reports therefrom, as the Commission shall prescribe by regulation or order, after public hearing, as reasonable, necessary, or appropriate for the enforcement of this title or the regulations or orders thereunder. The Commission shall, by regulation, require each employer, labor organization, and joint labor-management committee subject to this title which controls an apprenticeship or other training program to maintain such records as are reasonably necessary to carry out the purpose of this title, including, but not limited to, a list of applicants who wish to participate in such program, including the chronological order in which such applications were received, and shall furnish to the Commission, upon request, a detailed description of the manner in which persons are selected to participate in the apprenticeship or other training program. Any employer, employment agency, labor organization, or joint labor-management committee which believes that the application to it of any regulation or order issued under this section would result in undue hardship may (1) apply to the Commission for an exemption from the application of such regulation or order, or (2) bring a civil action in the United States district court for the district where such records are kept. If the Commission or the court, as the case may be, finds that the application of the regulation or order to the employer, employment agency, or labor organization in question would impose an undue hardship, the Commission or the court, as the case may be, may grant appropriate relief.

Exceptions.

(d) The provisions of subsection (c) shall not apply to any employer, employment agency, labor organization, or joint labor-management committee with respect to matters occurring in any State or political subdivision thereof which has a fair employment practice law during any period in which such employer, employment agency, labor organization, or joint labor-management committee is subject to such law, except that the Commission may require such notations on records which such employer, employment agency, labor organization, or joint labor-management committee keeps or is required to keep as are necessary because of differences in coverage or methods of enforcement between the State or local law and the provisions of this title. Where an employer is required by Executive Order 10925, issued March 6, 1961, or by any other Executive order prescribing fair employment practices for Government contractors and subcontractors, or by rules or regulations issued thereunder, to file reports relating to his employment practices with any Federal agency or committee, and he is substantially in compliance with such requirements, the Commission shall not require him to file additional reports pursuant to subsection (c) of this section.

3 CFR, 1961 Supp., p. 86.
5 USC 631 note.

Prohibited disclosures.

(e) It shall be unlawful for any officer or employee of the Commission to make public in any manner whatever any information obtained by the Commission pursuant to its authority under this section prior to the institution of any proceeding under this title involving such information. Any officer or employee of the Commission who shall make public in any manner whatever any information in violation of this subsection shall be guilty of a misdemeanor and upon conviction thereof, shall be fined not more than $1,000, or imprisoned not more than one year.

INVESTIGATORY POWERS

SEC. 710. (a) For the purposes of any investigation of a charge filed under the authority contained in section 706, the Commission shall have authority to examine witnesses under oath and to require the production of documentary evidence relevant or material to the charge under investigation.

(b) If the respondent named in a charge filed under section 706 fails or refuses to comply with a demand of the Commission for permission to examine or to copy evidence in conformity with the provisions of section 709(a), or if any person required to comply with the provisions of section 709 (c) or (d) fails or refuses to do so, or if any person fails or refuses to comply with a demand by the Commission to give testimony under oath, the United States district court for the district in which such person is found, resides, or transacts business, shall, upon application of the Commission, have jurisdiction to issue to such person an order requiring him to comply with the provisions of section 709 (c) or (d) or to comply with the demand of the Commission, but the attendance of a witness may not be required outside the State where he is found, resides, or transacts business and the production of evidence may not be required outside the State where such evidence is kept.

Petitions.

(c) Within twenty days after the service upon any person charged under section 706 of a demand by the Commission for the production of documentary evidence or for permission to examine or to copy evidence in conformity with the provisions of section 709(a), such person may file in the district court of the United States for the judicial district in which he resides, is found, or transacts business, and serve upon the Commission a petition for an order of such court modifying or setting aside such demand. The time allowed for compliance with the demand in whole or in part as deemed proper and ordered by the court shall not run during the pendency of such petition in the court. Such petition shall specify each ground upon which the petitioner relies in seeking such relief, and may be based upon any failure of such demand to comply with the provisions of this title or with the limitations generally applicable to compulsory process or upon any constitutional or other legal right or privilege of such person. No objection which is not raised by such a petition may be urged in the defense to a proceeding initiated by the Commission under subsection (b) for enforcement of such a demand unless such proceeding is commenced by the Commission prior to the expiration of the twenty-day period, or unless the court determines that the defendant could not reasonably have been aware of the availability of such ground of objection.

(d) In any proceeding brought by the Commission under subsection (b), except as provided in subsection (c) of this section, the defendant may petition the court for an order modifying or setting aside the demand of the Commission.

NOTICES TO BE POSTED

SEC. 711. (a) Every employer, employment agency, and labor organization, as the case may be, shall post and keep posted in conspicuous places upon its premises where notices to employees, applicants for employment, and members are customarily posted a notice to be prepared or approved by the Commission setting forth excerpts from or, summaries of, the pertinent provisions of this title and information pertinent to the filing of a complaint.

(b) A willful violation of this section shall be punishable by a fine of not more than $100 for each separate offense.

VETERANS' PREFERENCE

SEC. 712. Nothing contained in this title shall be construed to repeal or modify any Federal, State, territorial, or local law creating special rights or preference for veterans.

RULES AND REGULATIONS

SEC. 713. (a) The Commission shall have authority from time to time to issue, amend, or rescind suitable procedural regulations to carry out the provisions of this title. Regulations issued under this section shall be in conformity with the standards and limitations of the Administrative Procedure Act. 60 Stat. 237. 5 USC 1001 note.

(b) In any action or proceeding based on any alleged unlawful employment practice, no person shall be subject to any liability or punishment for or on account of (1) the commission by such person of an unlawful employment practice if he pleads and proves that the act or omission complained of was in good faith, in conformity with, and in reliance on any written interpretation or opinion of the Commission, or (2) the failure of such person to publish and file any information required by any provision of this title if he pleads and proves that he failed to publish and file such information in good faith, in conformity with the instructions of the Commission issued under this title regarding the filing of such information. Such a defense, if established, shall be a bar to the action or proceeding, notwithstanding that (A) after such act or omission, such interpretation or opinion is modified or rescinded or is determined by judicial authority to be invalid or of no legal effect, or (B) after publishing or filing the description and annual reports, such publication or filing is determined by judicial authority not to be in conformity with the requirements of this title.

FORCIBLY RESISTING THE COMMISSION OR ITS REPRESENTATIVES

SEC. 714. The provisions of section 111, title 18, United States Code, shall apply to officers, agents, and employees of the Commission in the performance of their official duties. 62 Stat. 688.

SPECIAL STUDY BY SECRETARY OF LABOR

SEC. 715. The Secretary of Labor shall make a full and complete study of the factors which might tend to result in discrimination in employment because of age and of the consequences of such discrimination on the economy and individuals affected. The Secretary of Labor shall make a report to the Congress not later than June 30, 1965, containing the results of such study and shall include in such report such recommendations for legislation to prevent arbitrary discrimination in employment because of age as he determines advisable. Report to Congress.

EFFECTIVE DATE

SEC. 716. (a) This title shall become effective one year after the date of its enactment.

(b) Notwithstanding subsection (a), sections of this title other than sections 703, 704, 706, and 707 shall become effective immediately.

Presidential conferences.

(c) The President shall, as soon as feasible after the enactment of this title, convene one or more conferences for the purpose of enabling the leaders of groups whose members will be affected by this title to become familiar with the rights afforded and obligations imposed by its provisions, and for the purpose of making plans which will result in the fair and effective administration of this title when all of its provisions become effective. The President shall invite the participation in such conference or conferences of (1) the members of the President's Committee on Equal Employment Opportunity, (2) the members of the Commission on Civil Rights, (3) representatives of State and local agencies engaged in furthering equal employment opportunity, (4) representatives of private agencies engaged in furthering equal employment opportunity, and (5) representatives of employers, labor organizations, and employment agencies who will be subject to this title.

Membership.

TITLE VIII—REGISTRATION AND VOTING STATISTICS

Survey.

SEC. 801. The Secretary of Commerce shall promptly conduct a survey to compile registration and voting statistics in such geographic areas as may be recommended by the Commission on Civil Rights. Such a survey and compilation shall, to the extent recommended by the Commission on Civil Rights, only include a count of persons of voting age by race, color, and national origin, and determination of the extent to which such persons are registered to vote, and have voted in any statewide primary or general election in which the Members of the United States House of Representatives are nominated or elected, since January 1, 1960. Such information shall also be collected and compiled in connection with the Nineteenth Decennial Census, and at such other times as the Congress may prescribe. The provisions of section 9 and chapter 7 of title 13, United States Code, shall apply to any survey, collection, or compilation of registration and voting statistics carried out under this title: *Provided, however*, That no person shall be compelled to disclose his race, color, national origin, or questioned about his political party affiliation, how he voted, or the reasons therefore, nor shall any penalty be imposed for his failure or refusal to make such disclosure. Every person interrogated orally, by written survey or questionnaire or by any other means with respect to such information shall be fully advised with respect to his right to fail or refuse to furnish such information.

68 Stat. 1013, 1022; 76 Stat. 922. 13 USC 9, 211-241.

TITLE IX—INTERVENTION AND PROCEDURE AFTER REMOVAL IN CIVIL RIGHTS CASES

63 Stat. 102.

SEC. 901. Title 28 of the United States Code, section 1447(d), is amended to read as follows:

"An order remanding a case to the State court from which it was removed is not reviewable on appeal or otherwise, except that an order remanding a case to the State court from which it was removed pursuant to section 1443 of this title shall be reviewable by appeal or otherwise."

62 Stat. 938.

SEC. 902. Whenever an action has been commenced in any court of the United States seeking relief from the denial of equal protection of the laws under the fourteenth amendment to the Constitution on ac-

count of race, color, religion, or national origin, the Attorney General for or in the name of the United States may intervene in such action upon timely application if the Attorney General certifies that the case is of general public importance. In such action the United States shall be entitled to the same relief as if it had instituted the action.

TITLE X—ESTABLISHMENT OF COMMUNITY RELATIONS SERVICE

SEC. 1001. (a) There is hereby established in and as a part of the Department of Commerce a Community Relations Service (hereinafter referred to as the "Service"), which shall be headed by a Director who shall be appointed by the President with the advice and consent of the Senate for a term of four years. The Director is authorized to appoint, subject to the civil service laws and regulations, such other personnel as may be necessary to enable the Service to carry out its functions and duties, and to fix their compensation in accordance with the Classification Act of 1949, as amended. The Director is further authorized to procure services as authorized by section 15 of the Act of August 2, 1946 (60 Stat. 810; 5 U.S.C. 55(a)), but at rates for individuals not in excess of $75 per diem.

Post, p. 400.
5 USC 1071 note.

(b) Section 106(a) of the Federal Executive Pay Act of 1956, as amended (5 U.S.C. 2205(a)), is further amended by adding the following clause thereto:

70 Stat. 737.

"(52) Director, Community Relations Service."

Functions.

SEC. 1002. It shall be the function of the Service to provide assistance to communities and persons therein in resolving disputes, disagreements, or difficulties relating to discriminatory practices based on race, color, or national origin which impair the rights of persons in such communities under the Constitution or laws of the United States or which affect or may affect interstate commerce. The Service may offer its services in cases of such disputes, disagreements, or difficulties whenever, in its judgment, peaceful relations among the citizens of the community involved are threatened thereby, and it may offer its services either upon its own motion or upon the request of an appropriate State or local official or other interested person.

SEC. 1003. (a) The Service shall, whenever possible, in performing its functions, seek and utilize the cooperation of appropriate State or local, public, or private agencies.

(b) The activities of all officers and employees of the Service in providing conciliation assistance shall be conducted in confidence and without publicity, and the Service shall hold confidential any information acquired in the regular performance of its duties upon the understanding that it would be so held. No officer or employee of the Service shall engage in the performance of investigative or prosecuting functions of any department or agency in any litigation arising out of a dispute in which he acted on behalf of the Service. Any officer or other employee of the Service, who shall make public in any manner whatever any information in violation of this subsection, shall be deemed guilty of a misdemeanor and, upon conviction thereof, shall be fined not more than $1,000 or imprisoned not more than one year.

Report to Congress.

SEC. 1004. Subject to the provisions of sections 205 and 1003(b), the Director shall, on or before January 31 of each year, submit to the Congress a report of the activities of the Service during the preceding fiscal year.

TITLE XI—MISCELLANEOUS

Trial by jury.

SEC. 1101. In any proceeding for criminal contempt arising under title II, III, IV, V, VI, or VII of this Act, the accused, upon demand therefor, shall be entitled to a trial by jury, which shall conform as near as may be to the practice in criminal cases. Upon conviction, the accused shall not be fined more than $1,000 or imprisoned for more than six months.

Exceptions.

This section shall not apply to contempts committed in the presence of the court, or so near thereto as to obstruct the administration of justice, nor to the misbehavior, misconduct, or disobedience of any officer of the court in respect to writs, orders, or process of the court. No person shall be convicted of criminal contempt hereunder unless the act or omission constituting such contempt shall have been intentional, as required in other cases of criminal contempt.

Nor shall anything herein be construed to deprive courts of their power, by civil contempt proceedings, without a jury, to secure compliance with or to prevent obstruction of, as distinguished from punishment for violations of, any lawful writ, process, order, rule, decree, or command of the court in accordance with the prevailing usages of law and equity, including the power of detention.

Double jeopardy.

SEC. 1102. No person should be put twice in jeopardy under the laws of the United States for the same act or omission. For this reason, an acquittal or conviction in a prosecution for a specific crime under the laws of the United States shall bar a proceeding for criminal contempt, which is based upon the same act or omission and which arises under the provisions of this Act; and an acquittal or conviction in a proceeding for criminal contempt, which arises under the provisions of this Act, shall bar a prosecution for a specific crime under the laws of the United States based upon the same act or omission.

Attorney General, etc., authority.

SEC. 1103. Nothing in this Act shall be construed to deny, impair, or otherwise affect any right or authority of the Attorney General or of the United States or any agency or officer thereof under existing law to institute or intervene in any action or proceeding.

States' authority.

SEC. 1104. Nothing contained in any title of this Act shall be construed as indicating an intent on the part of Congress to occupy the field in which any such title operates to the exclusion of State laws on the same subject matter, nor shall any provision of this Act be construed as invalidating any provision of State law unless such provision is inconsistent with any of the purposes of this Act, or any provision thereof.

Appropriation.

SEC. 1105. There are hereby authorized to be appropriated such sums as are necessary to carry out the provisions of this Act.

Separability clause.

SEC. 1106. If any provision of this Act or the application thereof to any person or circumstances is held invalid, the remainder of the Act and the application of the provision to other persons not similarly situated or to other circumstances shall not be affected thereby.

Approved July 2, 1964.

59 to 61, 64a, 71a, 78, 84, 85, 170, 181, 192, 221a, 228, 241, 242, 244, 247a, 248, 263, 287, 288, 321, 324, 336, 341, 343, 347b, 352a, 355, 357, 371, 371b, 371c, 375a, 377, 378, 461, 462a–1, 462b, 465, 481, 482, 486, 619, 1702, 1703, 1709, and 1713 of this title; section 101 of Title 11, Bankruptcy; section 19 of Title 15, Commerce and Trade. See, also, sections 217, 218, 334, 655, 656, 709, 1005, 1906, 1909, and 2113 of Title 18, Crimes and Criminal Procedure. For complete classification of this Act to the Code see Tables.

SEPARABILITY

Section 346 of act Aug. 23, 1935, provided: ''If any provision of this Act, or the application thereof to any person or circumstances, is held invalid, the remainder of the Act, and the application of such provision to other persons and circumstances, shall not be affected thereby.''

SUBCHAPTER II—BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

§ 241. Creation; membership; compensation and expenses

The Board of Governors of the Federal Reserve System (hereinafter referred to as the ''Board'') shall be composed of seven members, to be appointed by the President, by and with the advice and consent of the Senate, after August 23, 1935, for terms of fourteen years except as hereinafter provided, but each appointive member of the Federal Reserve Board in office on such date shall continue to serve as a member of the Board until February 1, 1936, and the Secretary of the Treasury and the Comptroller of the Currency shall continue to serve as members of the Board until February 1, 1936. In selecting the members of the Board, not more than one of whom shall be selected from any one Federal Reserve district, the President shall have due regard to a fair representation of the financial, agricultural, industrial, and commercial interests, and geographical divisions of the country. The members of the Board shall devote their entire time to the business of the Board and shall each receive basic compensation at the rate of $15,000 per annum, payable monthly, together with actual necessary traveling expenses.

(Dec. 23, 1913, ch. 6, § 10 (par.), 38 Stat. 260; June 3, 1922, ch. 205, 42 Stat. 620; Aug. 23, 1935, ch. 614, title II, § 203(b), 49 Stat. 704.)

CODIFICATION

Section is comprised of first par. of section 10 of act Dec. 23, 1913. Pars. 2–7 and 8 of section 10; par. 9 of section 10, as added June 3, 1922, ch. 205, 42 Stat. 621; par. 10 of section 10, as added Aug. 23, 1935, ch. 614, § 203(d), 49 Stat. 705; and par. (12) of section 10, as added Pub. L. 111–203, title XI, § 1108(b), July 21, 2010, 124 Stat. 2126, are classified to sections 242 to 247, 1, 522, 247a, and 247b, respectively, of this title. No par. between pars. (10) and (12) has been enacted.

AMENDMENTS

1935—Act Aug. 23, 1935, § 203(b), increased the appointive membership from six to seven, terminated the membership of the Secretary of the Treasury and the Comptroller of the Currency, raised the tenure from twelve to fourteen years and increased the annual salary from $12,000 to $15,000.

CHANGE OF NAME

Section 203(a) of act Aug. 23, 1935, provided that: ''Hereafter the Federal Reserve Board shall be known as the 'Board of Governors of the Federal Reserve System,' and the governor and the vice governor of the Federal Reserve Board shall be known as the 'chairman' and the 'vice chairman,' respectively, of the Board of Governors of the Federal Reserve System.''

REPEALS

Act Oct. 15, 1949, ch. 695, § 4, 63 Stat. 880, formerly cited as a credit to this section, which was used as authority to substitute ''$16,000'' for ''$15,000'' in the last sentence, was repealed by Pub. L. 89–554, § 8(a), Sept. 6, 1966, 80 Stat. 655.

GENERAL ACCOUNTING OFFICE STUDY OF CONFLICTS OF INTEREST

Pub. L. 106–102, title VII, § 728, Nov. 12, 1999, 113 Stat. 1475, provided that the Comptroller General of the United States was to conduct a study analyzing the conflict of interest faced by the Board of Governors of the Federal Reserve System between its role as a primary regulator of the banking industry and its role as a vendor of services to the banking and financial services industry and, before the end of the 1-year period beginning on Nov. 12, 1999, submit a report to the Congress, together with recommendations for such legislative or administrative actions as the Comptroller General determined to be appropriate.

COMPENSATION OF BOARD OF GOVERNORS

Annual basic compensation of Chairman and Members of Board of Governors, see sections 5313 and 5314 of Title 5, Government Organization and Employees.

§ 242. Ineligibility to hold office in member banks; qualifications and terms of office of members; chairman and vice chairman; oath of office

The members of the Board shall be ineligible during the time they are in office and for two years thereafter to hold any office, position, or employment in any member bank, except that this restriction shall not apply to a member who has served the full term for which he was appointed. Upon the expiration of the term of any appointive member of the Federal Reserve Board in office on August 23, 1935, the President shall fix the term of the successor to such member at not to exceed fourteen years, as designated by the President at the time of nomination, but in such manner as to provide for the expiration of the term of not more than one member in any two-year period, and thereafter each member shall hold office for a term of fourteen years from the expiration of the term of his predecessor, unless sooner removed for cause by the President. Of the persons thus appointed, 1 shall be designated by the President, by and with the advice and consent of the Senate, to serve as Chairman of the Board for a term of 4 years, and 2 shall be designated by the President, by and with the advice and consent of the Senate, to serve as Vice Chairmen of the Board, each for a term of 4 years, 1 of whom shall serve in the absence of the Chairman, as provided in section 244 of this title, and 1 of whom shall be designated Vice Chairman for Supervision. The Vice Chairman for Supervision shall develop policy recommendations for the Board regarding supervision and regulation of depository institution holding companies and other financial firms supervised by the Board, and shall oversee the supervision and regulation of such firms. The Chairman of the Board, subject to its supervision, shall be its active executive officer. Each member of the

inside the board

Board Policies

Adjusting Work-Related Problems

Approved by H. Fay Peters, effective June 30, 2010

Jump to section: Policy Statement

Policy Statement

All employees are to be treated fairly and equitably. Managers and their staffs are encouraged to create and maintain an atmosphere of mutual trust, respect, and open and objective communication. Most work-related problems, complaints, disputes, and differences of opinion can be resolved once they are discussed with the employee's supervisor. If the problem cannot be resolved through discussion, employees are encouraged to follow the procedure described below.

Return to top

Covered Problems

A work-related problem covered under this policy can be any issue that arises in the context of a work situation *and* that is not within the scope of the following management policies: Adverse Action Policy and Procedures, Disciplinary Actions, Sexual Harassment, Reasonable Accommodation, Performance Management Program, Equal Employment Opportunity, Provisional Employment Period, and Provisional Period for Newly Selected Managers and Supervisors. Accordingly, the procedure set forth in this policy may not be used in lieu of appeal procedures provided in other policies that establish an exclusive remedy and may not be used to avoid conditions or limitations set out in such other policies. When a work-related problem is addressed under another management policy, any complaint or appeal under this policy regarding the same work-related problem will be dismissed, and the matter will be addressed under the other applicable policy.

Work-related problems include, but are not limited to, employee complaints or questions regarding unfair treatment on the basis of conduct or reasons that do not adversely affect the employee's performance and that are not covered under existing laws regarding discrimination. Such matters may include allegations of discrimination in employment on the basis of sexual orientation.

Return to top

Definitions

Employee means an individual who works full-time or part-time and is appointed into Board service for a period of more than 90 calendar days.[1] The term *employee* does not include members of the Board or nonregular employees, that is, student aides, worker-trainees, student interns, co-op employees, or individuals who are serving in a temporary term-limited position.

The term *employee* also does not include an *at-will* employee, that is, an individual serving at the pleasure of the Board and who may be discharged from Board service for any reason that is not illegal.

Return to top

Procedure for Addressing a Work-Related Problem

Employee relations specialists in the Employee Relations section (ER) of the Management Division are available to help employees and managers address work-related problems. They ensure that employees are aware of their rights and guide them through the steps outlined in the following procedure. An employee relations specialist may also help resolve cases by gathering facts, consulting with the employee regarding his or her concerns, and recommending a course of action. An employee relations specialist may be consulted at any time before or during the

process.

Step 1. An employee should first discuss any work-related problem (or problems) under this policy with his or her immediate supervisor as soon as possible. Unless unusual circumstances exist, an employee should bring the matter to the attention of the supervisor within 15 working days from the date the employee first became aware of the matter or from the effective date of the action giving rise to the work-related problem. Experience has shown that most problems can be settled once they are brought to the attention of the supervisor and discussed fairly and openly.

Step 2. If the problem is not resolved within 15 working days after it has been brought to the attention of the immediate supervisor, the employee may submit a written description of the problem within five working days to the manager or officer responsible for the functional area. This person may, depending on the organizational structure, be the same person as the immediate supervisor. The manager or officer responsible for the functional area will review the problem and issue a written decision within 15 working days of receipt of the employee's written description of the problem.

Step 3. If the employee is not satisfied with the decision of the manager or officer responsible for the functional area, the employee may appeal to the division director. Any such appeal must be filed within five working days of the employee's receipt of the manager's or officer's decision. The appeal must be submitted in writing to the division director. If the division director is the same person as the manager or officer responsible for the functional area (as described in step 2), the employee may ignore step 3 and proceed to step 4. The division director will issue a written decision within 15 working days of receipt of the employee's appeal.

Step 4. If the employee is not satisfied with the decision of the division director (or of the manager or officer responsible for the functional area if that person is the same person as the division director), the employee may select one of the following two options:

- *Officer responsible for ER (ER Officer).* The employee may appeal the decision of the division director to the ER Officer or to his or her designee. Any such appeal must be filed within five working days of the employee's receipt of the division director's decision and must be submitted in writing. The ER Officer, or his or her designee, will issue a written decision within 15 working days of receipt of the employee's appeal. The decision of the ER Officer is final and binding.

  For employees in the Management Division, this appeal shall be made to a Board officer outside the Management Division, who shall be designated by the chairman, Committee on Board Affairs, rather than to the ER Officer. The decision of the officer appointed by chairman, Committee on Board Affairs, shall be final and binding.

  The decision of the ER Officer or, as appropriate, a Board officer designated by the chairman, Committee on Board Affairs, may be implemented under delegated authority.

- *Mediation.* Within five working days of the employee's receipt of the division director's decision, the employee may request that a mediator be engaged to help bring about a mutually acceptable resolution to the problem. The mediation between the employee and division management will be governed by the procedures described in the Employee Relations Mediation Guidelines.

  If mediation does not resolve the problem, the employee may choose to appeal the decision of the division director to the ER Officer in accordance with the provisions of step 4.1 above. Any such appeal must be made within five working days of the conclusion of the mediation.

Review of Documentation at Each Level

In reviewing an appeal, the reviewing authority at each level has the discretion to conduct whatever investigation he or she deems appropriate, including requesting supplementary information from the employee or from management. The reviewing authority, however, may choose to issue a decision based on a review of the appeal and any documentation that may have been initially presented.

Submission of Documentation

At any stage of the process, the employee may submit additional material. Such material must be submitted, as applicable, by the date the written description of the problem or the date the appeal is due.

Any material submitted to the ER Officer in connection with an appeal will be shared with the employee's management unless the ER Officer does not rely on the information in reaching a decision or if the ER Officer determines that disclosing the

information would create or exacerbate an employee relations issue. Any documentation submitted by the division in connection with an appeal will be shared with the employee except to the extent that doing so infringes on the privacy rights of other employees.

Time Limits

The ER Officer can extend the time limits contained in this policy. No procedural rights or requirements that are not specifically stated in the procedure may be implied.

Return to top

Responsibility

The Management Division has the discretionary authority to administer and interpret this policy. The Board may review, update, and amend this policy at any time.

Return to top

Footnotes

1. Applicants for employment with the Board may invoke the procedures in this policy for claims of unfair treatment on the basis of sexual orientation. Return to text.

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
MANAGEMENT POLICY STATEMENT

Equal Employment Opportunity

Approved by Don Hammond, effective May 13, 2013

Policy Statement

The Board's policy is to provide equal opportunity in employment for all persons. Thus, consistent with applicable law, the Board prohibits discrimination in employment on the basis of race, color, religion, sex, national origin, age, disability, or genetic information, and promotes the full realization of equal employment opportunity (EEO) through a continuing affirmative program. The Board also prohibits discrimination on the basis of any application, membership, or service in the uniformed services. In addition, as a matter of policy and although it is not required by law, the Board prohibits discrimination in employment on the basis of sexual orientation.

The Board strives to comply with the following statutes and any amendments thereof: the Civil Rights Act of 1964 (title VII), section 501 of the Rehabilitation Act of 1973, the Age Discrimination in Employment Act of 1967 (ADEA), the Equal Pay Act of 1963, the Genetic Information Nondiscrimination Act of 2008, and the Uniformed Services Employment and Reemployment Rights Act of 1994 (USERRA). The Board's Rules Regarding Equal Employment Opportunity (the Board's EEO rules), 12 CFR part 268, set forth the policies and procedures relating to the Board's policy to promote equal opportunity. In addition, plans, program objectives, and goals dealing with equal employment opportunity and affirmative action are set forth in the Board's EEO rules as well as in the Affirmative Employment Program Plan adopted by the Board (which is available through the Board's Office of Diversity and Inclusion (ODI)).

Complaint Processing

An employee or applicant for employment who believes that he or she has been discriminated against on the basis of race, color, religion, sex, national origin, disability, age, or genetic information, or subject to retaliation for engaging in protected activity, may raise any such complaint with the Board's ODI (formerly the EEO Office) as provided by the Board's EEO rules. The aggrieved person must initiate contact with an EEO counselor within 45 days of the matter alleged to be discriminatory or, in the case of a personnel action, within 45 days of the effective date of the action.

An employee or applicant for employment who believes that he or she has been discriminated against on the basis of any application, membership, or service in the uniformed services, or

subject to retaliation for engaging in protected activity, may raise any such complaint with the Department of Labor. Because the process for USERRA-related complaints differs from the process for complaints of other forms of discrimination, ODI does not counsel or provide any complaint processing for USERRA-related complaints. These complaints are addressed by the Department of Labor. Additional information on USERRA and filing USERRA complaints is available at the Department of Labor's VETS website.

Complaints by employees and applicants for employment regarding discrimination on the basis of sexual orientation may be raised under the Adjusting Work–Related Problems policy. Because discrimination on the basis of sexual orientation is not covered by federal laws prohibiting discrimination, the Board's EEO rules do not address discrimination on the basis of sexual orientation. In this regard, this policy does not create any right to file a lawsuit or other legal action on the basis of sexual orientation. This policy also does not provide any right to benefits, as those are determined by the terms of the particular benefit plan.

Interaction with Other Policies

Allegations of discrimination on the grounds of race, color, sex, national origin, age, disability, or genetic information, or of retaliation for engaging in protected activity, cannot be simultaneously raised under the Board's EEO rules and the Board's Adjusting Work–Related Problems policy. When an employee presents an allegation of discrimination on the grounds of race, color, sex, religion, national origin, age, disability, or genetic information, the allegation shall be processed under the Board's EEO rules, and any grievance regarding the same matter being processed through the Adjusting Work–Related Problems policy shall terminate.

Responsibility

The Board has assigned direct responsibility for implementation of its EEO policy to supervisors and managers. The ODI director is responsible for coordinating Boardwide implementation of EEO procedures and practices; advising on the Board's policies and practices in connection with federal EEO laws; implementing this and other Board policies related to EEO; coordinating the resolution of EEO complaints; and, if applicable, recommending corrective measures to management. The Human Resources (HR) Function of the Management Division is responsible for addressing complaints filed under the Adjusting Work–Related Problems policy that allege discrimination on the basis of sexual orientation and for addressing any USERRA-related concerns.

This policy will be reviewed and updated as necessary.

Return to top

Management Policies Home

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
MANAGEMENT POLICY STATEMENT

Performance Management Program

Approved by Michell C. Clark, effective February 7, 2014

Policy Statement

The Board's policy is to review the performance of all employees periodically and make employment decisions based on an employee's performance. To this end, the Board has established a Performance Management Program (PMP) that requires a written annual review (annual PMP).[1]

Purpose

The purpose of the PMP process is to (1) continuously improve individual and organizational performance, (2) develop and motivate employees to become top performers and help the Board achieve its mission and purpose, and (3) inform various employment decisions, such as compensation and retention decisions.

Objectives

The PMP process helps the Board achieve its mission and purpose by establishing a set of planned activities for each employee. These activities support the organization’s work needs and emphasize the importance of open lines of communication between employees and their supervisors regarding work performance. The Board encourages employees to develop their skills and grow in their professions; therefore, annual PMPs should outline goals and objectives and discuss performance areas that can be improved. To meet the goals of the PMP process, supervisors are responsible for creating performance standards, monitoring performance, and providing an employee with feedback on his or her performance. Employees share responsibility for initiating communication at any time regarding performance issues and concerns, preparing for each step of the performance-appraisal

process, and implementing the suggestions provided as feedback.

Definitions

For purposes of this policy, the following definitions apply unless otherwise specified.

Employee is an individual who works full-time or part-time and is appointed into Board service for a period of more than 90 calendar days. The term "employee" includes officers but not Board members, student aides, student interns, or co-op employees.

Performance Ratings

An employee's performance is evaluated against five possible levels of performance: Extraordinary, Outstanding, Commendable, Marginal, and Unsatisfactory. An employee receives an evaluation and overall rating each year. The evaluation takes into account an employee's performance on both the technical requirements and the behavioral components of the job and may take into consideration the performance of his or her similarly situated peers. The five rating levels are defined below.

Extraordinary. Performance that substantially and consistently exceeds the Board's high standards and expectations. This rating is reserved for a limited number of employees.

Outstanding. Performance that consistently meets and often exceeds the Board's high standards of the job and the expectations of the position. This rating is reserved for a limited number of employees.

Commendable. Performance that consistently meets the Board's high standards and expectations.

Marginal. Performance that is marginally below the level of acceptability because it does not either fully or consistently satisfy the requirements and expectations of the position.

Unsatisfactory. Performance that is below the level of acceptability because it substantially fails to satisfy the requirements and expectations of the position.

Annual PMP Requirements

1. *Timing.* Supervisors must conduct an annual PMP for each employee they supervise.[2] Annual PMPs of all employees will be completed on the same annual cycle on PMP forms that have been approved by the Human Resources (HR) Function of the Management Division.[3] HR will notify all divisions of the dates the annual PMPs are due.

2. *PMP session.* Supervisors should let each employee know when they will be conducting the annual PMP session. During the PMP session, supervisors are expected to discuss the employee's performance and how well the employee met his or her performance objectives or expectations during the performance period. Supervisors may also review an employee's job responsibilities, performance expectations and/or objectives, behavior, strengths, areas for further improvement, and development needs and activities. The objective of feedback is to recognize effective and ineffective performance and motivate the employee to higher levels of performance. Employeesare

encouraged to provide their views about their performance.

3. *Reviewing managers' responsibilities*. Reviewing managers should review the PMPs completed by their subordinate supervisors (before an employee is given his or her PMP) and ensure that the PMPs adequately reflect employee performance. Reviewing managers should attempt to resolve PMP disagreements between an employee and his or her immediate supervisor.

4. *Change of supervisor or job*. If a supervisor is reassigned from a work unit or leaves the Board, responsibility for the PMPs for employees in the unit will be given to the new supervisor. Similarly, responsibility for the PMP for an employee transferring to a work unit with a different supervisor will be with the new supervisor. In both cases, the prior supervisor should provide the new supervisor and the employee who is transferring or being reassigned with feedback on the employee's performance before the employee's reassignment or transfer.

5. *Signing and finalizing the PMP*. The supervisor and reviewing manager must sign the annual PMP and the employee should acknowledge receipt of the PMP by signing it as well. If the employee declines to sign the PMP, this should be noted on the PMP. A copy of the PMP must be provided to the employee shortly after it is signed by the reviewing manager.

   A PMP is final and effective when both the supervisor and the reviewing manager sign it. Until the PMP is signed by the reviewing manager, an employee may raise a disagreement about the PMP with the supervisor or reviewing manager. (If the employee continues to disagree with the PMP, after it is signed by the reviewing manager the employee may appeal the PMP as explained under the appeal section, below.) If the reviewing manager or supervisor makes any changes to the PMP in connection with a PMP disagreement, these changes should be reflected on the PMP. Any written statements an employee submits in response to the PMP must be attached to the completed PMP.

6. *Submitting the PMP to HR*. Each division must send the original, completed annual PMP to the designated HR staff responsible for the Performance Management Program for HR staff to file in the appropriate system of records consistent with applicable law. Divisions are expected to provide signed PMPs to HR no later than November 30. HR will keep documents related to PMP appeals. Each division must maintain all of the supporting documentation to support the PMP rating consistent with the applicable records-retention schedule.

7. *Consultation with HR*. A division may issue an annual PMP that rates an employee's performance as Marginal or Unsatisfactory only after consulting with the Employee Relations Section, HR.

Other PMP-Related Activities

1. *Objective setting for new employees and employees in new positions.* Supervisors should hold objective-setting sessions with all new employees and employees who are assuming new positions within 90 calendar days of an employee's appointment or assumption of a new position. The objective-setting session is a meeting in which the supervisor, with the employee's input, clarifies the employee's job responsibilities and performance expectations, identifies specific objectives and measurement criteria for the employee's job, and plans how the employee will accomplish the objectives. The supervisor should retain a written record documenting the session.

2. *PMP training for newly appointed employees and newly appointed supervisors.* New employees and newly appointed supervisors must complete PMP training within 90 calendar days of their appointments. If possible, this training should occur before the supervisor issues any PMPs and before the supervisor's initial PMP-objective-setting session with a subordinate employee.

3. *Interim PMPs.* Supervisors may provide their employees with interim PMPs in order to give employees performance feedback between annual PMPs.

4. *Performance feedback*. In addition to interim and annual PMPs, supervisors should routinely provide performance feedback to their employees. As described below, thatperformance feedback may include a performance warning, if warranted.

Use of Annual PMP Ratings

1. *Generally.* The annual PMP rating is used to determine the amount of any merit increase the employee will receive for the year and, when applicable, is considered when determining variable pay or eligibility for other incentive programs. PMP ratings may also be relied on for promotion decisions and employment actions within the Board. In addition, as explained more fully below, a rating of Marginal or Unsatisfactory at any time (including on an interim PMP or performance warning) may lead to an employee's separation from Board employment.

2. *Merit pay and Marginal or Unsatisfactory ratings.* An employee who receives a rating of Marginal or Unsatisfactory on his or her annual PMP is not eligible for a merit increase, salary-structure increase, or any other type of performance-based pay, such as cash awards and variable pay, unless and until the employee receives a rating of higher than Marginal or Unsatisfactory on a subsequent annual PMP. If the employee's salary falls below the minimum of the salary range for his or her grade because he or she receives a Marginal or Unsatisfactory rating, the employee's salary will not be raised to the minimum of the salary range.

3. *Workforce reductions.* An employee's performance on the three most recent annual PMPs is a factor used in determining the retention standing of the employee when the employee is affected by a workforce reduction.

Marginal or Unsatisfactory Performance

1. *Timing.* At any time during the year, if an employee's performance is Marginal or Unsatisfactory, the employee's supervisor can issue the employee notice that his or her performance is Marginal or Unsatisfactory. This could happen through either a formal annual or interim PMP or a less formal performance warning, such as an e-mail or memorandum. Whatever the form, the performance warning must tell the employee why his or her performance has been Marginal or Unsatisfactory and the consequences of failure to improve performance to at least the Commendable level after a period to improve performance.

2. *Consequences of Marginal or Unsatisfactory performance.* The Board may separate an employee who fails to meet the Board's performance standards after the employee is given Marginal or Unsatisfactory performance feedback and a period of time to improve his or her performance.[4] An employee who is subject to the Board's Adverse Action policy and receives feedback that his or her performance is Marginal will generally be given six months to improve. An employee who is subject to the Board's Adverse Action policy and receives feedback that his or her performance is Unsatisfactory will generally be given three months to improve. An employee who is subject to the Board's Provisional Employment policy and receives feedback that his or her performance is Marginal or Unsatisfactory will generally be given a period of three months to improve. If an employee engages in any misconduct during the improvement period, the employee may be separated immediately. If at the end of the improvement period, the employee's performance is still at a Marginal or Unsatisfactory level, the employee may be separated from Board employment.

   In addition, if an employee improves performance to a Commendable level or above, the employee must sustain his or her performance at that level after the improvement period ends. If an employee who is subject to the Board's Provisional Employment Policy does not, during the provisional period, sustain performance at a Commendable level or above, the employee may be separated from service. If an employee who is subject to the Board's Adverse Action policy does not sustain performance, in the areas previously identified for improvement, at a Commendable level or above, for six months after the end of the improvement period, the employee may be separated from service.[5] The Board's Provisional Employment policy and Adverse Action policy describe the procedures applicable to separating most Board employees for poor performance.

3. *Consultation with HR.* A division may issue an employee notice that his or her performance is Marginal or Unsatisfactory only after consulting with the Employee Relations Section, HR.

Appeals

1. *What may be appealed.* An employee (other than a division or office director or the chief operating officer) may appeal (1) his or her most recent annual PMP, which may include an appeal of the overall rating, the rating on an individual element, or adverse comments in the PMP; or (2) any notice that his or her performance is Marginal or

Unsatisfactory. An employee may not appeal interim PMPs or other informal performance feedback (unless the PMP or feedback rates the employee's performance as Marginal or Unsatisfactory) or annual PMPs for prior performance periods. Any appeal must be in writing.

2. *Time period.* An employee wishing to appeal an annual PMP or notice that his or her performance is Marginal or Unsatisfactory must file any such appeal, along with all documentation the employee wishes to provide in support of the appeal, within 15 calendar days after the date on which the reviewing manager signed the PMP or the date on which the supervisor notified the employee that his or her performance was Marginal or Unsatisfactory. The appeal must be filed with the director of the division or office in which the employee works unless the director was the supervisor or reviewing manager for the PMP or other performance warning, in which case the chief human capital officer shall hear the appeal ("appeal officer"). If the chief operating officer was the supervisor or reviewing manager for the PMP or other performance warning, the general counsel shall appoint an appeal officer.

3. *Content of the appeal.* The appeal must specifically set forth those areas with which the employee disagrees. If the employee does not provide sufficient information in the appeal, the employee may be asked to submit additional information.

4. *Appeal determination.*The appeal officer will notify the appropriate supervisor of the appeal promptly after receipt.

   In reviewing the appeal, the appeal officer (or his or her designee) may act based upon the material provided by the employee and may also conduct whatever further investigation he or she deems appropriate, including requesting supplementary information from the employee and his or her supervisor(s).

   Unless an extension of time (explained below) is granted, within 30 calendar days after receipt of the appeal, the appeal officer (or his or her designee) will issue a written decision on the appeal. The decision should be given to the employee in a manner that identifies the date it was delivered to the employee. The appeal officer (or his or her designee) will determine whether the overall performance rating is appropriate and whether any changes should be made to the written documentation. As a result of an appeal, an appeal officer (or his or her designee) may uphold the PMP or notification that the employee's performance is Marginal or Unsatisfactory, raise the overall performance rating, raise the rating in an individual element on an annual PMP, or change language in the documentation. The PMP or the notification that the employee's performance is Marginal or Unsatisfactory may not be modified in a way that is adverse to the employee as a result of an appeal. The appeal officer's decision on an appeal is final and not subject to further review.

   Even if an appeal is pending, the Board may proceed with action under any other

policy, including the Provisional Employment and Adverse Action policies.

5. *Interplay with other appeal processes.*A PMP or notice that the employee's performance is Marginal or Unsatisfactory may not be simultaneously challenged under this policy and through other procedures provided by various Board policies. This means that while PMP or rating-related issues may be raised under employee relations policies, such as the Adverse Action policy, Provisional Employment policy, and the Equal Employment Opportunity (EEO) policy, an appeal under this policy cannot be pursued at the same time as an action or appeal under these other policies. Accordingly, whenever an employee is pursuing other avenues under any other policy, any appeal under this policy will be dismissed, and the PMP issue will be addressed under the other policy.

   If an employee files an appeal under this procedure and the employee wishes to file an EEO complaint regarding the PMP or notice that the employee's performance is Marginal or Unsatisfactory, the employee must contact an EEO counselor and initiate the EEO process within 45 calendar days of the date his or her PMP was signed by the reviewing manager or the date that he or she received notice that his or her performance was Marginal or Unsatisfactory.

   An employee may not pursue a PMP-related disagreement under the Board's Adjusting Work-Related Problems policy. The supervisor or manager involved must refer the employee to the PMP policy.

   An employee's appeal under this procedure does not stay or prevent any action that may be taken under another Board procedure. In this regard, an adverse action or a disciplinary action that is based on the PMP or notice of Marginal or Unsatisfactory performance can be taken even if an appeal is pending. The PMP matter will be addressed under the Board procedure pursuant to which the action is taken against the employee.

6. *Consultation.* At any stage in the appeals process, an employee or manager may contact an Employee Relations specialist for assistance in resolving appeal-related problems.

7. *Extensions of time.* The ER Officer, after consulting with both the affected employee and the employee's division, may extend any of the time frames under this appeal procedure.

References

- Adjusting Work-Related Problems
- Adverse Action
- Cash Compensation Program

- Equal Employment Opportunity
- Personnel Placement Program
- Provisional Employment

Responsibility

The Management Division has the authority to administer and interpret this policy. The Management Division shares the responsibility for implementation of the PMP program with each division (or office). This policy may be reviewed, updated, or amended at any time.

---

1. Whether an employee who has been at the Board for less than 12 months receives a PMP depends on the division's practice. Return to text

2. Some new employees may be an exception (see footnote 1). Return to text

3. If a division demonstrates a sufficient need, HR may permit that division to use specifically tailored PMP forms. Any such form must include objectives and/or expectations; measurement criteria; performance results; strengths; areas for further improvement; and an overall evaluation. Furthermore, all tailored PMP forms must include a description of the performance–rating levels as stated in this policy. Return to text

4. In general, the improvement period will not be extended for time an employee is out on leave unless the employee is out for more than half of the improvement period and the employee showed improvement prior to going out on leave. Return to text

5.If an employee is out of work for any reason this six month period may be extended by the number of days the employee is out of work. Return to text

Return to top

Management Policies Home

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
MANAGEMENT POLICY STATEMENT

Adverse Action

Approved by Michell C. Clark, effective February 7, 2014

Purpose

This policy outlines the general circumstances under which the Board may take an adverse action against an employee and describes the procedures that will be followed when such an action is proposed and taken. Unless an action falls within the definition of an adverse action, the action is not covered by this policy. Actions not covered by this policy may be covered by other Board policies—for example, the Disciplinary Actions policy or the Provisional Employment policy.

Definitions

Adverse action means a discharge, removal, suspension without pay for a period of more than 14 calendar days, or a reduction in grade or base pay against an employee. All other actions do not constitute adverse actions. In addition, adverse actions do not include

- actions the employee voluntarily agrees to or takes on his or her own behalf;
- actions that reduce an employee's variable pay, bonuses, cash awards, or any other type of pay that does not constitute base pay;
- any action taken under the Board's Workforce Reduction policy (including separation or reduction in grade or pay); or
- actions taken to carry out a transfer of function(s) required by law or other actions required by applicable law.

Base pay means the employee's annual rate of basic pay. Base pay does not include variable pay, cash awards, lump-sum merit increases, sign-on bonuses, retention bonuses, shift differential, overtime pay, holiday pay, availability pay, unscheduled-duty pay, premium pay, or any other type of pay that the Board does not treat as base pay.

Days refers to calendar, not working, days unless otherwise noted.

Employee means an individual who works full-time or part-time and is appointed into Board service for a period of more than 90 calendar days. The term *employee* does not include members of the Board or those serving a provisional employment period, student aides, office assistants, student interns, co-op employees, or those serving in a term-limited position.[1] The term employee also does not include an at-will employee, that is, an individual serving at the pleasure of the Board who may be discharged from Board service for any reason that is not unlawful. An individual who provides services to the Board but who is not an employee as defined herein has no rights under this policy.

Officer means an employee who has been appointed by the Board to serve as a member of its official staff.

Grounds for Adverse Actions

Adverse actions are taken to promote the integrity and efficiency of the Board. The circumstances under which an employee's performance may result in an adverse action are described in the Board's Performance Management Program policy. For example, an adverse action may be initiated against an employee on the basis of his or her less-than-commendable performance. An adverse action may also be initiated against an employee on the basis of national security or employment-suitability considerations. When taking an adverse action on the basis of performance, national security, or employment suitability, the Board does not take aggravating and mitigating factors (as explained below) into account.

In addition, the Board may take an adverse action against an employee as a result of his or her misconduct. Whether the Board takes an adverse action against an employee for misconduct depends on the facts of the particular case, including the nature and severity of the misconduct, whether and how the misconduct affects the employee's ability to carry out his or her job responsibilities, and the Board's confidence in the employee's ability to carry out those responsibilities. In deciding whether to pursue an adverse action for misconduct, the Board may consider, as appropriate, aggravating and mitigating factors. Such factors may include whether an offense was intentional, technical, or inadvertent; was committed maliciously or for gain; was frequently repeated; or was notorious (such that it could negatively affect the Board's reputation). The employee's job level, type of employment, supervisory status, previous disciplinary record, performance, and potential for rehabilitation may also be considered. Depending on the seriousness of the offense, one instance of misconduct may be sufficient to separate an employee from Board service.

In certain cases the Board may initiate an adverse action due to an employee's failure to meet certain employment requirements, such as not being legally authorized to work in the United States; not meeting an essential job requirement, such as a law enforcement officer who is not authorized to carry a weapon; not being fit for duty; not passing a background investigation; or not meeting other suitability requirements as explained in the Board's Suitability policy. In cases where the employee fails to meet an employment requirement, the employee will be notified of the problem and be provided with the procedural protections outlined in this policy. However, the employee may not be given any time period to improve performance or remedy the problem, but instead will immediately be separated from Board employment under the procedures outlined herein. In addition, aggravating and mitigating

factors will not be considered in such cases.

Adverse Action Procedures

Proposing an Adverse Action

An officer in the employee's division (the proposing official) must consult with the Employee Relations (ER) Section of the Management Division prior to proposing an action. A division may not inform an employee of a proposed adverse action before consulting ER. After ER has reviewed and commented on the proposal, the proposing official will deliver the proposal to the employee (and such notice will be considered delivered on the date that it was delivered to the employee either in person, by certified mail or Federal Express, or similar method). At the same time, the proposing official will deliver the proposal to the head of the employing division or office (the deciding official). The appendix outlines the individuals who serve as the proposing and deciding officials if an officer is the subject of the adverse action. The employee shall be given an opportunity to respond to the proposal, as further described below.

Content of the proposal and notice to employee. The proposal must state the proposed action, state the specific reasons for the proposed action, and describe the evidence or information on which the proposing official is basing the proposal.[2] In addition, if the proposed action is a result of employee misconduct, the proposal should discuss why the proposed penalty is appropriate in light of any mitigating or aggravating factors. The proposal must (1) attach a copy of this policy; (2) include any material that was relied upon to support the proposed actions, including documents, investigative reports, or extracts and, if such material was derived from witness statements, the statements themselves or information regarding how the employee can access them; and (3) inform the employee

- of the time period to respond to the proposal and that the response may either be in writing, in person (if requested by the employee), or both;
- that an employee relations specialist is available to assist him or her; and
- that he or she is entitled to consult with, and be represented by, a personal representative of the employee's choice and at the employee's expense, at any stage in the adverse action process.

Procedures governing the employee's response to the proposal. An employee will be given 15 calendar days from the date of the proposal to respond to the proposal unless there is reasonable cause to believe that the employee may be guilty of a crime for which a prison sentence can be imposed. In that case, the officer responsible for Employee Relations (ER Officer), or his or her designee, may reduce the response period, but in no event may it be reduced to less than seven calendar days.

At any time, the proposing official may amend a proposed action that has been issued to an employee to include additional information in support of the proposed action, to reference subsequently occurring or discovered supporting evidence, or to add additional bases for the proposed action. The information upon which such amendments are based will be provided to

the employee as stated above. The employee shall be given no less than 15 calendar days to respond to the proposed action, as amended. When there is reasonable cause to believe that an employee may be guilty of a crime for which a prison sentence can be imposed, the ER Officer, or his or her designee, may reduce this time period, but in no event may it be reduced to less than seven calendar days.

An employee's response to the deciding official must be made in writing. The employee's response must specifically state the reasons he or she believes the proposed action is incorrect and may include affidavits or any other relevant documentation. All documentation must be submitted with the employee's response.

An employee may request to meet in person with the deciding official. (An in-person meeting could also include a telephone call or a video conference.) Such requests must be made within seven calendar days of the date of the proposed action and must explain why the employee believes an in-person meeting is necessary. In addition, the employee's meeting request must include the dates and times he or she is available to meet within the 15 calendar-day response period. After receiving the request, the deciding official will inform the employee whether the request for an in person meeting will be granted and, if so, the date and time of the meeting, if applicable. This policy does not provide a right to an in-person meeting with the deciding official.

Employee's status pending a decision. The proposing official, in consultation with the ER Officer, or his or her designee, may place the employee on administrative leave (with pay) from the date the employee is provided with the proposal, or at any time after that date, until the deciding official issues a decision on the proposal. An employee on administrative leave may have his or her access to things such as the Board's buildings and electronic systems restricted, but the employee will continue to receive the regular health and retirement benefits and pay (excluding overtime) he or she would have been paid if the employee had worked during the administrative-leave period.

An employee who is absent from work without pay at the time the adverse action is proposed will not be placed in a pay status while the deciding official's decision is pending, unless the employee requests and qualifies for paid leave or returns to duty. If the employee requests and qualifies for paid leave or returns to duty, the employee will be placed in a pay status from the date the leave request was made or the date the employee returned to duty. In addition, if an employee is absent from work and has applied for, or is receiving, short-term disability (STD) benefits at the time the adverse action is proposed, the employee will be paid in accordance with the Board's normal rules for administering STD claims/benefits while the deciding official's decision is pending. However, if the employee states that he or she is able to return to work and, if required, provides medical documentation to support this statement, the employee will be placed on administrative leave with pay or returned to work while the deciding official's decision is pending. An employee's access to the building may be restricted while the decision is pending.

Deciding Official's Decision on the Proposal

Within 30 calendar days after the employee responds to the proposed action, or not more than 30 calendar days after the time period for the employee's response expires, the deciding

official shall notify the employee, the employee's representative (if any), and the proposing official in writing of his or her decision. The deciding official may, in reaching a decision, conduct whatever investigation he or she deems appropriate, including requesting supplementary information from the employee or the proposing official (or both).

The decision may (1) sustain the proposing official's recommendation either in whole or in part; (2) modify the proposing official's recommendation by substituting a less severe action; or (3) reverse the proposing official's recommendation either in whole or in part. If the deciding official uncovers new and material information to support the proposal, and he or she intends to rely on that information in reaching a decision, the deciding official must provide the employee with that information and allow the employee an opportunity to respond. The employee must have a minimum of 15 calendar days to respond to the new and material information, unless there is reasonable cause to believe that the employee may be guilty of a crime for which a prison sentence can be imposed. In that case, the ER Officer, or his or her designee, may reduce this time period, but in no event may it be reduced to less than seven calendar days.

If the decision is adverse to the employee, the deciding official shall notify the employee of the decision at or before the time the action will be made effective. The deciding official's decision shall be dated and shall inform the employee of the reason (or reasons) for the decision, the effective date of the decision, and his or her right to appeal the decision. Any appeal will not delay the effective date of the adverse action.

Appeal

An employee may appeal the deciding official's decision to the chief operating officer (COO),[3] or if the COO made the initial determination to separate the employee or otherwise must abstain from making the decision, to a neutral and impartial third party designated by the chairman, Committee on Board Affairs (appeal official).[4] The appendix outlines who serves as the appeal official in the case of an officer. As part of an employee's appeal, he or she may request a hearing. The employee must file an appeal with the appeal official no later than 15 calendar days after the date of the deciding official's decision.

Content of the appeal. The appeal must (1) be in writing, (2) state the specific reasons the adverse action is incorrect, and (3) state whether the employee is requesting a hearing.

Hearing. If the employee requests a hearing, the appeal official, will determine the type of hearing and the scope of the hearing that will be provided.[5]

Decision on appeal. The appeal official shall review and consider the entire record. Within 30 calendar days after the date of a timely appeal, the appeal official shall notify the employee, the employee's representative (if any), the proposing official, and the deciding official of his or her decision in writing. The decision may (1) sustain the deciding official's decision either in whole or in part, (2) modify the deciding official's decision by substituting a less severe action, or (3) reverse the deciding official's decision either in whole or in part. In reaching a decision on appeal, the appeal official may only consider the written record before him or her as well as the information presented at the hearing, if any. The decision must explain the basis for the decision. The decision on appeal shall be final and binding upon the employee and the Board.

Time Limits

At any stage of the process, the deciding official or appeal official, as appropriate, may extend the time limits indicated in the adverse action procedures. In situations that require an extension of time, the employee will be informed of such an extension.

Disclosure of Information

Any information the employee submits in response to an adverse action will be shared with the proposing official at each stage in the process unless the information will not be relied on in reaching a decision. Any information the proposing official or the deciding official submits to support the adverse action will be supplied to the employee unless the information will not be relied on in reaching a decision. In appropriate cases, the deciding official or appeal official may require the employee to agree to maintain the confidentiality of information submitted by the proposing official or the deciding official as a pre-condition to receiving such information if disclosure of such information would impinge on the privacy rights of other employees or would otherwise be impermissible under law or Board policy.

Interplay with Other Policies

An employee may not simultaneously challenge an action under this policy and under other applicable Board policies, except for the Board's Equal Employment Opportunity (EEO) policy. Accordingly, subject to that exception, if an adverse action is proposed, all actions under other Board policies that are based on the same set of facts as the proposed adverse action will be terminated. An employee may continue to pursue both an appeal under this Adverse Action policy and an action under the Board's EEO policy. If an employee wishes to challenge an adverse action under the Board's EEO policy, he or she must initiate contact with an EEO counselor within 45 calendar days of the date of the deciding official's decision on the adverse action. The filing of an EEO complaint does not delay the effective date of the adverse action.

Actions Taken Pursuant to National Security

Notwithstanding any other provisions of this policy, to the extent a proposed adverse action is based on information that is classified for national security reasons, the Board will provide an employee with as comprehensive and detailed a written explanation of the basis for the adverse action as the national security interests of the United States and other applicable law permit. In addition, the Board will provide an employee with the information an adverse action is based on only as permitted by national security interests and other applicable law.

Responsibility

The Management Division has the authority to administer and interpret this policy. Divisions are responsible for notifying ER when the division first believes that an employee's behavior or performance could result in an adverse action. This policy may be reviewed, updated, or amended at any time.

Appendix —Proposing and Deciding Officials for Adverse Actions Involving Officers

Adverse Action Against:

1. **Against the chief operating officer (COO) and division/office directors, except those listed under 2, below, and except the inspector general**[6]
   Proposing Official: Chair of the relevant standing committee (or administrator if there is no standing committee)
   Deciding Official: Administrative governor (or if the administrative governor was the proposing official, the Vice Chair)[7]
   Appeal Official: Full Board (excluding the proposing and deciding officials)

2. **Against the director of the Management Division, director of the Division of Financial Management, program director of the Office of Diversity and Inclusion, director of the Division of Information Technology, chief data officer, and any other division or office director that the Board states, in writing, reports to the COO**
   Proposing Official: Chief operating officer
   Deciding Official: Administrative governor
   Appeal Official: Full Board (excluding the deciding official)

3. **Against all other officers (other than the inspector general)**
   Proposing Official: Division/office director
   Deciding Official: Chair of the standing committee/administrator
   Appeal Official: Administrative governor (or if the administrative governor was the deciding official, the Board's Vice Chair)[8]

The COO, division directors, and governors who are required to act as the proposing official, deciding official, or appeal official may consult with the chief human capital officer and the assistant general counsel, as needed.

---

1. Those serving a provisional employment period can be separated from employment at the will of the Board for any reason that is not unlawful, in accordance with the Board's Provisional Employment policy. In addition, student aides, office assistants, student interns, co-op employees, and persons in term limited positions, serve at the will of the Board and may be disciplined or separated for any reason that is not unlawful. Furthermore, a person serving in a term-limited position may automatically be separated at the end of his or her term, unless a decision is made to extend the employee's term.
Return to text

2. If an adverse action is based on the employee's performance under the Board's Performance Management Program, the proposing official need only attach the employee's PMP forms to describe or explain the action.
Return to text

3. The COO may designate the chief human capital officer (CHCO) to decide the appeal instead of the COO. However, if the COO made the initial determination to separate the employee or otherwise must abstain from deciding the appeal, the CHCO also may not hear the appeal.
Return to text

4. The COO must consult with the Legal Division regarding when a neutral and impartial third party must be assigned. A neutral and impartial third party may be any Board officer who was not involved in the initial decision.
Return to text

5. The hearing will provide sufficient process to satisfy due process requirements as determined by the COO or the third party designated by the chairman, Committee on Board Affairs, in consultation with the Legal Division.
Return to text

6. The inspector general may only be removed under the terms and conditions specified under the Inspector General Act.
Return to text

7. If the position of Vice Chair is vacant the administrative governor shall appoint a governor to act in place of the Vice Chair.
Return to text
8. As noted above, if the position of Vice Chair is vacant the administrative governor shall appoint a governor to act in place of the Vice Chair.
Return to text

Return to top

Management Policies Home

inside the board

Board Policies

Delegations of Administrative Authority

Effective December 20, 2013

Jump to section:
Overview

Overview

A 1966 amendment to the Federal Reserve Act authorizes the Board to delegate any of its functions, other than those pertaining to rulemaking or monetary and credit policies, to hearing examiners, members or employees of the Board, or the Federal Reserve Banks. Since 1966, the Board has delegated a large number of functions, mostly in the areas of the Board's management, administration, and bank and financial holding company supervision, including the processing of applications. Only the Chairman may assign responsibility for the performance of functions delegated by the Board.

Section 10(2) of the Federal Reserve Act designates the Chairman as the Board's "active executive officer." In this capacity, the Chairman is responsible for the overall management of the Board in the execution of its objectives, policies, and programs. The Board has delegated to the Chairman the administrative responsibilities delineated in section 1 of this document. This document only deals with the delegations of the Board's internal administrative authority. The Board has delegated non-internal functions as stated in 12 CFR 265. The Board shall review any action taken under these delegations of internal administrative authority upon the vote of one member of the Board in accordance with the procedures set out in 12 CFR 265.3.

The Chairman, who has authority under section 11(k) of the Federal Reserve Act to assign responsibility for performance of delegated functions, has selected one of the Board members to serve as the Board's administrative governor, with authority to oversee day-to-day operations of the organization as outlined in section 2 below. As outlined in other sections of this document, the administrative governor has delegated authority and responsibility for a number of these operations to the chief operating officer (COO) and to the directors of the offices and divisions, and some of these functions have been further delegated. However, the Board has not delegated the authority to approve the Board's budget, strategic plan, or salary structure.

As outlined in section 3 below, the Chairman delegates to the chair of each standing committee (or administrator for the relevant division or office) the authority to supervise all officers (including actions such as approving promotions of officers, adjusting officer salaries and bonuses, and approving any significant changes to duties of existing officers). In exercising delegated authority for setting and adjusting officer salaries and bonuses, the chair of each standing committee (or the administrator for the relevant division or office) must obtain the concurrence of the administrative governor, unless the administrative governor is responsible for taking the action. The Board retains the authority and responsibility for the creation of new officer positions, the initial appointment of officers, and all matters relating to division and office directors (except adverse actions against division or office directors).[1]

The governor or officer to whom any function shown below is delegated may redelegate that function to any other staff in writing, while also retaining the delegated authority, unless expressly stated otherwise. Moreover, individuals who delegate authority have a duty to monitor the work of the individuals who exercise their delegated authority. To assist with this monitoring, those who are delegated functions must report to the Board, or to the appropriate committee, governor, or officer, as needed. No individual authorized to act under these delegation rules, or any further subdelegation, may take action that contravenes (1) prior decisions, findings, or determinations lawfully made by the Board, except for budget actions permitted by the below delegations; (2) an applicable management policy, unless the individual has the authority to modify the applicable policy and has done so in writing (or has consented

to an exception in writing); or (3) a decision made by a higher-level individual without first obtaining the consent of that individual.

The Board also delegates certain administrative authorities to the inspector general. This delegation is made in conjunction with the Director of the Consumer Financial Protection Bureau (CFPB). The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) (Pub. L. 111-203) modified the Inspector General Act by creating one inspector general for both the Board and the CFPB. As a result of this statutory modification, matters (other than appointment of the inspector general) related to management of the Office of Inspector General are handled by both the Board and the CFPB. For this reason, the delegation of administrative authority to the inspector general is from both the Board and the Director of the CFPB.

1. Delegation of Administrative Responsibilities from the Board to the Chairman

1.1 ***Delegation of responsibilities.*** Except as provided under section 16, the Board delegates to the Chairman the responsibility and authority for—

(a) the overall internal management and organization of the Board's resources, including the formulation and implementation of plans, budgets, and funding to ensure effective performance of the Board's functions under law and the formulation, approval, and implementation of management policies such as those governing physical premises; personnel management; financial planning; management and control; information technology; security of personnel, premises, and information; and space accommodations;

(b) the review and presentation to the Board of the operating and capital budgets for the Board;[2]

(c) the disbursement of funds;

(d) the appointment and supervision of non-officer personnel (including the approval of personnel actions, such as pay actions and adverse actions) and taking adverse actions against officers (including division and office directors), the authority to supervise all officers (including actions such as approving promotions of officers, adjusting officer salaries and bonuses, and approving any significant changes to duties of existing officers), except that the Board retains the authority and responsibility for the creation of additional officer positions that increase the total number of Board officer positions, the initial appointment of an individual as an officer, and all matters relating to division and office directors (except adverse actions against them);

(e) the distribution of business activities among staff and organizational units;

(f) the approval of reorganizations within the dollar limitations noted below for substantive changes; and

(g) the abolishment of vacant positions and reduction of the Board's workforce if doing so is consistent with the Board's strategic plan and work requirements.

1.2 ***Limitations on delegation.*** In carrying out these delegated responsibilities, the Chairman shall be governed by the operating budget and the single-year and multiyear capital budgets adopted by the Board, except that the Chairman shall have authority to amend any of the operating and single-year capital budgets or multiyear capital budgets by—

(a) approving, with regard to the operating budget, reallocations among cost centers and budget accounts (as set forth in the budget authorized by the Board) or overexpenditures of budgeted funds, except that no individual reallocation or overexpenditure may exceed $2.0 million and the total of all such changes combined may not exceed 2 percent of the operating budget approved by the Board for the budget period, [3]

(b) approving, with regard to the single-year capital budget, reallocations among cost centers and budget accounts (as set forth in the budget authorized by the Board) or overexpenditures of budgeted funds, except that no individual reallocation or overexpenditure may exceed $2.0 million and the total of all such changes combined may not exceed 10 percent of the single-year capital budget approved by the Board for the budget period;

(c) approving, with regard to the multiyear capital budget, reallocations among cost centers and budget accounts (as set forth in the budget authorized by the Board) or overexpenditures of budgeted funds, except that no individual reallocation or overexpenditure may exceed $2.0 million and the total of all such changes combined may not exceed 10 percent of the multiyear capital budget approved by the Board for the budget period; and

(d) approving permanent new positions that would increase the Board's total position authorization for that budget period by no more than 2 percent of the number

originally authorized by the Board for that budget period, and approving dual-occupancy and temporary positions as long the overall budget limits are not exceeded.

2. Chairman to the Administrative Governor (Chair, Committee on Board Affairs)

2.1 ***Delegation.*** The Chairman redelegates to the administrative governor all administrative responsibilities delegated to the Chairman pursuant to section 1 above (and as limited by section 1 above) with the further limitations noted below. The administrative governor shall have the authority to carry out the day-to-day operations of the Board directly or through appropriate redelegation. All actions taken by the administrative governor and any other person delegated to act under these delegations of authority count against the Chairman's limits with regard to reallocations, overexpenditures, and number of positions, except actions that result in current-year budget savings and/or transfers of functions to achieve operating efficiencies that do not result in increases to the Board's budget.

2.2 ***Limitations on delegation.*** In carrying out these delegated responsibilities, the administrative governor shall not—

(a) make significant budgetary decisions without input from the appropriate standing committee chair or administrator or abolish vacant positions or reduce the Board's workforce without the consent of the appropriate standing committee chair or administrator; or

(b) approve, with regard to the operating budget, single-year capital budget, or multiyear capital budget, any reallocations among cost centers and budget accounts (as set forth in the budget authorized by the Board) or overexpenditures of budgeted funds unless the administrative governor has reason to believe that savings in one or more other budget categories will have the result that the overall operating budget, single-year capital budget, or multiyear capital budget, as the case may be, will not be exceeded; or

(c) take any actions delegated to the chair of each standing committee (or administrator for the relevant division or office) under section 3 unless the administrative governor serves as the chair of the relevant standing committee or administrator for the relevant division or office. In addition, any Board policy pertaining to the separation of officers must give the chairs of the standing committees (or administrators) the sole authority to propose separations of division/office directors in the divisions/offices they oversee (except the COO may propose separations of directors who report directly to the COO) and to make final decisions to separate all other officers in the divisions/offices they oversee.

3. Chairman to the Chair of Each Standing Committee (or Administrator for the Relevant Division or Office)

3.1 ***Delegation.*** The Chairman redelegates to the chair of each standing committee (or administrator for the relevant division or office) the authority to supervise all officers within the relevant division or office (including actions such as approving promotions of officers, adjusting officer salaries and bonuses, and approving any significant changes to duties of existing officers, but not including adverse actions against officers, unless the adverse action was delegated to the governor by the Chairman, administrative governor, or under Board policy).

3.2 ***Limitations on delegation.*** In exercising delegated authority for setting and adjusting officer salaries and bonuses, the chair of each standing committee (or the administrator for the relevant division or office) must obtain the concurrence of the administrative governor unless the administrative governor is responsible for taking the action. The Board retains the authority and responsibility for the creation of new officer positions, the appointment of officers, and all matters relating to division directors (except adverse actions against them).

4. Administrative Governor to the Chief Operating Officer

4.1 ***Delegation.*** The administrative governor redelegates to the COO (as limited above) the responsibility and authority for—

(a) administrative oversight of the Board's operations and resources;

(b) approval, with regard to the operating budget, of reallocations among cost centers and budget accounts (as set forth in the budget authorized by the Board) or overexpenditures of budgeted funds if (1) each reallocation or overexpenditure does not exceed $1.5 million, (2) the total of all such changes combined does not exceed 2 percent of the operating budget approved by the Board for the budget period, and (3) the COO has reason to believe that savings in one or more other budget categories will have the result that the overall operating budget will not be exceeded;

(c) approval, with regard to the single-year or multiyear capital budget, of reallocations among cost centers and budget accounts (as set forth in the budget authorized by the Board) or overexpenditures of budgeted funds if (1) each reallocation or overexpenditure does not exceed $1.5 million, (2) the total of all such changes combined does not exceed 10 percent of the single-year or multiyear capital budget approved by the Board, and (3) the COO has reason to believe that savings in one or more other budget categories will have the result that the overall single-year or multiyear capital budget will not be exceeded;

(d) approval of dual-occupancy and temporary positions as long the overall budget limits are not exceeded;

(e) approval of the reallocation of functions from one cost center to another to promote efficient staff operations, without regard to the dollar or position limitations noted above, if the reallocation does not result in increases to the Board's budget or total authorized position count (funds transferred as a result of such actions do not count against the delegation limits);

(f) approval of the specific financial and position changes proposed to implement more general actions approved previously by the Board or the administrative governor pursuant to these delegations;

(g) approval of actual expenses (as opposed to per diem expenses) in connection with travel of all staff;

(h) approval of all agreements and understandings that obligate the Board to make payments or entitle the Board to receive payments (except assessing civil money penalties) and, in consultation with the Legal Division, settling any actual or potential claims against the Board (and such claim-settlement authority may only be further redelegated to the director of the Management Division);

(i) procurement of goods, services, and real property for use in conducting the operations of the Board as approved in the budget or by an authorized program change request;

(j) formulation, approval, and implementation of Board policies pertaining to administrative oversight of the Board's operations and resources, including policies governing matters such as planning, management, and financial control; personnel management (including policies for adverse actions against officers) within the limits noted below; physical and personnel security (except for policies related to the Chairman's physical protection); access to and handling of classified information; information technology and security; data management and governance; privacy; procurement; allocation, management control, and maintenance of building space required by the Board; and the Board's continuity of operations and business-resumption activities;

(k) approval of all personnel actions of non-officer employees (except that the COO shall have no authority to decide whether to reduce the Board's workforce or abolish positions, except as provided under section 14, or change personnel actions made by a division or office director under his or her delegated authority under section 14.1(e) of these delegations);

(l) performing actions and duties required under the Paperwork Reduction Act; and

(m) approval of changes to benefit-plan documents (other than changes to plans administered by the Office of Employee Benefits), so long as the plan documents relate to benefits available only to Board staff and do not create a new benefit or reduce or eliminate an existing benefit.

4.2 ***Limitations on delegation.*** In exercising delegated authority, the COO must obtain the prior consent of the administrative governor for all changes to Board policies that pertain to personnel issues, such as policies that govern adverse actions, including actions such as separating and disciplining employees (whether at the staff or officer level); performance systems; pay; and benefits (such as leave accrual rates, severance pay, disability benefits, flexible work schedules, and similar benefits). For clarity, the COO is not required to obtain the consent of the administrative governor when taking actions with regard to a specific employee unless Board policy requires such consent. In addition, any Board policy pertaining to the separation of officers must give the chairs of the standing committees (or administrators) the sole authority to propose separations of division/office directors in the divisions/offices they oversee (except the COO may propose separations of directors who report directly to the COO) and to make final decisions to separate all other officers in the divisions/offices they oversee.

5. Chief Operating Officer to Director of the Management Division

5.1 ***Delegation.*** The COO redelegates to the director of the Management Division (as limited above) the responsibility and authority for—

(a) formulation, approval, and implementation of the management policies for personnel management; physical and personnel security (except for the Chairman's physical protection); access to and handling of classified information; allocation, management control, and maintenance of building space required by the Board; and the Board's continuity of operations and business-resumption activities (but such formulation and approval authority may not be further redelegated);

(b) approval of changes to benefit-plan documents (other than changes to plans administered by the Office of Employee Benefits) so long as the plan documents relate to benefits available only to Board staff and do not create a new benefit or reduce or eliminate an existing benefit; and

(c) approval of all personnel actions of non-officer employees.

6. Chief Operating Officer to the Program Director, Office of Diversity and Inclusion

6.1 ***Delegation***. The COO redelegates to the program director, Office of Diversity and Inclusion (as limited above), the responsibility and authority for—

(a) formulation and approval, in consultation with the director of the Management Division or the director of the Division of Financial Management (as appropriate) and the Legal Division, of management policies relating to diversity and inclusion in the Board's workforce and procurement (but such formulation and approval authority may not be further redelegated); and

(b) overseeing the Board's equal employment opportunity function, including processing complaints of discrimination in hiring or employment under federal law.

6.2 ***Reporting responsibilities.*** The program director, Office of Diversity and Inclusion, shall report to the Board on the progress of the Office of Diversity and Inclusion as needed.

7. Chief Operating Officer to the Chief Financial Officer

7.1 ***Delegation.*** The COO redelegates to the chief financial officer (CFO) (as limited above) the responsibility and authority for—

(a) formulation, approval, and implementation of the Board's policies, operations, and resources related to travel, procurement, financial management, financial control, and risk management (but such formulation and approval authority may not be further redelegated);

(b) setting budget targets consistent with the Board's strategic plan and chairing the Board's annual budget and review process, including discussions of enterprise-wide initiatives that are not included in the strategic plan and making recommendations regarding the same to the Board;

(c) approval, with regard to the operating budget, of reallocations among cost centers and budget accounts (as set forth in the budget authorized by the Board) or overexpenditures of budgeted funds if (1) each reallocation or overexpenditure does not exceed $1.5 million, (2) the total of all such changes combined does not exceed 2 percent of the operating budget approved by the Board for the budget period, and (3) the CFO has reason to believe that savings in one or more other budget categories will have the result that the overall operating budget will not be exceeded;

(d) approval, with regard to the single-year or multiyear capital budget, of reallocations among cost centers and budget accounts (as set forth in the budget authorized by the Board) or overexpenditures of budgeted funds if (1) each reallocation or overexpenditure does not exceed $1.5 million, (2) the total of all such changes combined does not exceed 10 percent of the single-year or multiyear capital budget approved by the Board, and (3) the CFO has reason to believe that savings in one or more other budget categories will have the result that the overall single-year or multiyear capital budget will not be exceeded;

(e) approval of the reallocation of functions from one cost center to another to promote efficient staff operations, without regard to the dollar or position limitations noted above, if the reallocation does not result in increases to the Board's budget or total authorized position count (funds transferred as a result of such actions do not count against the delegation limits);

(f) approval of dual-occupancy and temporary positions as long as the overall budget limits are not exceeded;

(g) approval of the specific financial and position changes proposed to implement more general actions approved previously by the Board or the administrative governor pursuant to these delegations;

(h) approval of actual expenses (as opposed to per diem expenses) in connection with

travel of all staff;

(i) approval of all agreements and memorandums that obligate the Board to make payments or entitle the Board to receive payments (except assessing civil money penalties or settling any actual or potential claims against the Board); and

(j) procurement of goods, services, and real property for use in conducting the operations of the Board as approved in the budget or by an authorized program change request.

7.2 ***Limitation on delegation.*** Notwithstanding the authority delegated to the CFO herein, the CFO may not approve dual-occupancy or temporary positions within the Division of Financial Management, and with respect to budget reallocations within the Division of Financial Management, the CFO shall be limited to the same authority granted to division directors under section 14 of these delegations.

7.3 ***Reporting responsibilities.*** The CFO shall report to the Committee on Board Affairs quarterly, in conjunction with budget reports, on all material actions under delegated authority that result in budget or position adjustments.

8. Chief Operating Officer to the Chief Information Officer and Chief Privacy Officer

8.1 ***Delegation.***The COO redelegates to the chief information officer and chief privacy officer (as limited above) the responsibility and authority for—

(a) automation, telecommunications, and other information technology matters;

(b) information security (but not as it relates to handling and access to classified information);

(c) formulation, approval, and implementation of the management policies for information technology and security (but such formulation and approval authority may not be further redelegated); and

(d) formulation, approval, and implementation of all privacy policies, including responsibility for (1) ensuring the Board's implementation of information-privacy protections, which includes the Board's compliance with applicable federal laws, regulations, and policies relating to information privacy, such as the Privacy Act of 1974 (but such formulation and approval authority may not be further redelegated), and (2) providing input into the Board's development and evaluation of legislative, regulatory, and other policy proposals regarding information privacy issues, except that approving and reviewing privacy impact assessments must be coordinated with the chief information officer.

8.2 ***Reporting responsibilities.*** The chief information officer and chief privacy officer shall report to the Committee on Board Affairs as needed.

9. Director of the Management Division to the Deputy Director of the Management Division Responsible for Facility Services

9.1 ***Delegation.*** The director of the Management Division redelegates to the deputy director of the Management Division responsible for facility services, the responsibility and authority—

(a) to allocate, manage, and maintain all Board buildings, grounds, and storage spaces;

(b) for the Board's continuity of operations and business resumption activities; and

(c) for physical and personnel security (except for the Chairman's physical protection) and for implementation of policies related to the access to and handling of classified information.

10. Director of the Management Division to the Deputy Director of the Management Division Responsible for Human Resources

10.1 ***Delegation.*** The director of the Management Division redelegates to the deputy director of the Management Division responsible for human resources (as limited above), except as otherwise provided in written management policies, the responsibility and authority for—

(a) administrative oversight of the Board's operations and resources related to personnel management; and

(b) approval of all personnel actions involving non-officer employees in accordance with Board policies.

10.2 ***Reporting responsibilities.*** The deputy director of the Management Division

responsible for human resources shall inform the director of the Management Division of the pending involuntary removal of any employee Boardwide. The chief human capital officer shall also report to the Committee on Board Affairs quarterly on all material actions related to personnel management.

11. Deputy Director of the Management Division Responsible for Facility Services to the Chief Personnel Security Officer

11.1 ***Delegation.*** The deputy director of the Management Division responsible for facility services redelegates to the chief personnel security officer the responsibility and authority for physical and personnel security (except for the Chairman's physical protection and except for matters pertaining to handling of classified national security information) and for implementation of policies related to access to classified national security information.

12. Chief Financial Officer to the Chief Acquisition Officer

12.1 ***Delegation.*** The CFO redelegates to the chief acquisition officer the responsibility and authority for procurement of goods, services, and real property for use in conducting the operations of the Board as approved in the budget or by an authorized program change request and for approval of all agreements and memorandums that obligate the Board to make payments or entitle the Board to receive payments (except assessing civil money penalties or settling any actual or potential claims against the Board). The chief acquisition officer shall act as the Board's contracting officer with authority to procure goods and services.

13. Deputy Director of the Management Division Responsible for Human Resources to the Chief Human Capital Officer

13.1 ***Delegation.*** The deputy director of the Management Division responsible for human resources redelegates to the chief human capital officer (as limited above), except as otherwise provided in written management policies, the responsibility and authority for—

(a) administrative oversight of the Board's operations and resources related to personnel management; and

(b) approval of all personnel actions involving non-officer employees in accordance with Board policies.

13.2 ***Reporting responsibilities.*** The chief human capital officer shall inform the deputy director of the Management Division responsible for human resources and the director of the Management Division of the pending involuntary removal of any employee Boardwide. The chief human capital officer shall also report as necessary to the Committee on Board Affairs on all material actions related to personnel management.

14. Administrative Governor to the Directors of Offices and Divisions

14.1 ***Delegation***. The administrative governor redelegates to the directors of offices and divisions the responsibility and authority to—

(a) approve, with regard to the division's or office's operating budget, reallocations among cost centers and budget accounts (as set forth in the budget authorized by the Board) or overexpenditures of budgeted funds in a particular cost center or budget account if (1) each reallocation or overexpenditure does not exceed $200,000, (2) the total of all such changes combined does not exceed a cumulative limit of the higher of 1 percent of the division's or office's operating budget approved by the Board for the budget period or $500,000 per budget period, (3) the reallocation does not move funds between personnel services and goods and services accounts, and (4) the director has reason to believe that savings in one or more other budget categories will have the result that the division's or office's overall operating budget will not be exceeded;

(b) approve the reallocation of functions from one cost center to another to promote efficient staff operations (such as a division or office reorganization) if the reallocation does not increase the division's or office's operating budget or total authorized positions (in which case, the funds or positions transferred do not count against the delegation limits);

(c) approve, with regard to the division's or office's single-year capital budget, reallocations among cost centers and budget accounts (as set forth in the budget authorized by the Board) if the total of all such changes combined does not exceed the lesser of 5 percent of the division's or office's single-year capital budget approved by the Board for the budget period or $100,000 for each budget period (if 5 percent of the division's or office's single-year capital budget is less than $10,000, the limit is $10,000);

(d) abolish vacant positions within their office or division if doing so is consistent with the Board's strategic plan and work requirements and if the standing committee chair or administrator for the division or office consents to the abolishment;

(e) approve all personnel actions, in accordance with Board policies, for non-officers within the division/office relating to promotions, salary increases, and performance awards such as cash awards and variable pay;

(f) approve domestic and foreign travel of division staff, including the division director's own travel expenses, and approve the division director's own leave use; and

(g) maintain information security associated with the data and computer facilities under their control in accordance with policies established by the chief information officer.

15. Administrative Governor to the Director of the Office of Board Members

15.1 ***Delegation***. The administrative governor redelegates to the director of the Office of Board Members the responsibility and authority for the Chairman's physical protection and Board policies related thereto (which responsibilities and authorities may not be further redelegated).

16. Board and Director of the Consumer Financial Protection Bureau to the Inspector General

16.1 ***Delegation***.The principles embodied in the Inspector General Act of 1978 and subsequent amendments preclude the Board and the Director of the CFPB from redelegating the responsibility for providing general supervision for the inspector general. To facilitate the operations of the Office of Inspector General (OIG), however, the Board and the Director of the CFPB delegate to the inspector general the responsibility and authority to—

(a) approve, with regard to the office's operating budget, reallocations among cost centers and budget accounts (as set forth in the OIG's authorized budget) or overexpenditures of budgeted funds in a particular cost center or budget account if (1) each reallocation or overexpenditure does not exceed $200,000, (2) the total of all such changes combined does not exceed a cumulative limit of the higher of 1 percent of the office's operating budget approved by the Board and the CFPB for the budget period or $500,000 per budget period, (3) the reallocation does not move funds between personnel services and goods and services accounts, and (4) the inspector general has reason to believe that savings in one or more other budget categories will have the result that the office's overall operating budget will not be exceeded;

(b) approve the reallocation of functions from one cost center to another to promote efficient staff operations (such as an office reorganization) if the reallocation does not increase the office's operating budget or total authorized positions (in which case, the funds or positions transferred do not count against the delegation limits);

(c) approve, with regard to the office's single-year capital budget, reallocations among cost centers and budget accounts (as set forth in the OIG's authorized budget) if the total of all such changes combined does not exceed the lesser of 5 percent of the office's single-year capital budget approved by the Board and the CFPB for the budget period or $100,000 for each budget period (if 5 percent of the office's single-year capital budget is less than $10,000, the limit is $10,000);

(d) abolish positions and create new positions so long as the office's total position authorization for that budget period does not change and so long as no additional funding is required in the current budget period;

(e) approve all personnel actions, in accordance with Board policies, for non-officer Board employees within the office, which relate to promotions, salary increases, and performance awards such as cash awards and variable pay;

(f) approve domestic and foreign travel of Board employees within the office, including the inspector general's own travel expenses, in accordance with Board policies, and approve the inspector general's own leave use;

(g) maintain information security associated with the data and computer facilities under the office's control, in accordance with policies established by the Board; and

(h) procure goods and services directly, within the approved operating and capital budgets, for use in conducting the operations of the office when, in the opinion of the inspector general, operational necessity warrants. In all other cases, normal Board procurement procedures will be used if the office uses the Board to procure the items or services.

Return to top

Footnotes

1. Adverse action has the meaning given to it under the Board's Adverse Action policy but generally means a discharge, removal, or suspension without pay for a period of more than 14 days or a reduction in grade or base pay. Return to text.

2. This delegation does not apply to the Currency Budget, which is covered by section 16 of the Federal Reserve Act (12 USC 411 et seq.) and in the *Federal Reserve Administrative Manual* at 1-049. Return to text.

3. References to the Board's operating, single-year, and multiyear capital budgets do not include the operating or capital budgets of the Office of Inspector General. Return to text.

Return to top

inside the board

Board Policies

Discriminatory Workplace Harassment

Approved by Don Hammond, effective June 24, 2013

Jump to section:
Policy Statement

Policy Statement

The Board's policy is to (1) provide all employees with a work environment that is free from discriminatory harassment, (2) thoroughly and promptly investigate all complaints of discriminatory harassment, and (3) effect appropriate discipline if discriminatory harassment is found to have occurred. Sexual harassment is one form of discriminatory harassment and is addressed more specifically later in this policy.

Return to top

Zero-Tolerance Policy

Discriminatory harassment will not be tolerated. The Board's policy is to prevent any discriminatory harassment even if the behavior does not violate the law—that is, it is not objectively severe or pervasive. Because the Board wishes to prevent all discriminatory harassment and to encourage reporting of discriminatory harassment before it becomes severe or pervasive, the Board has established this policy both to encourage the reporting of discriminatory harassment and to clarify that any employee who engages in discriminatory harassment may face disciplinary action. The Board is committed to investigating any possible discriminatory harassment of which it learns, even if the harassed individual does not file an equal employment opportunity (EEO) complaint.

Return to top

Background

Discriminatory harassment is verbal or physical conduct that demeans or shows hostility or aversion toward an individual because of his or her race, color, religion, sex, gender, national origin, age (40 or older), disability, genetic information, or because of retaliation for engaging in protected activity. Discriminatory harassment is against the law (that is, it violates Title VII of the Civil Rights Act of 1964, Section 501 of the Rehabilitation Act of 1973, the Age Discrimination in Employment Act of 1967, or the Genetic Information Nondiscrimination Act of 2008) when it has the purpose or effect of unreasonably interfering with an individual's work performance or of creating an intimidating, hostile, or offensive working environment. The conduct must be sufficiently severe or pervasive that it alters the conditions of employment and creates an environment that a reasonable person would find to be hostile or abusive. In addition, to constitute illegal harassment, there must be a basis for imputing liability to the Board. Although harassment based on sexual orientation is not a violation of federal law, it constitutes discriminatory harassment for purposes of this policy.

Below are some examples of conduct that might constitute discriminatory harassment. The list is not all-inclusive; in addition, each situation must be considered in light of the specific facts and circumstances to determine if discriminatory harassment occurred. For example, an occasional remark that could be considered offensive by a particularly sensitive individual is unlikely to be considered discriminatory harassment under this policy; a pattern of such remarks, particularly after the individual has objected to them, would more likely be considered to be discriminatory harassment. By contrast, even a single use of an epithet or slur that would be widely considered to be offensive would be likely to be considered discriminatory harassment under this policy. A finding that discriminatory harassment occurred that violates this policy does not mean that illegal discriminatory harassment necessarily occurred.

Examples of Discriminatory Harassment

- Oral or written use of offensive epithets, slurs, or comments aimed at an individual or group that relate to their race, color, religion, sex, gender,

national origin, age (40 or older), disability, genetic information, or sexual orientation.

- Use of offensive gestures or display of graphic pictures or drawings which demean or show hostility or aversion toward an individual or group because of race, color, religion, sex, gender, national origin, age (40 or older), disability, genetic information, or sexual orientation.
- Taunting on the basis of an individual's association with people of a particular race, color, religion, sex, gender, national origin, age (40 or older), disability, genetic information, or sexual orientation.
- Intimidation through violence or threats of force or violence against an individual because of his or her race, color, religion, sex, gender, national origin, age (40 or older), disability, genetic information, or sexual orientation.
- Unfavorable treatment of an individual or group because of their race, color, religion, sex, gender, national origin, age (40 or older), disability, genetic information, or sexual orientation.
- Ridiculing or mocking a person because of his or her race, color, religion, sex, gender, national origin, age (40 or older), disability, genetic information, or sexual orientation.
- Making comments to an individual, or in an individual's hearing, that reflect stereotypes about that individual's race, color, religion, sex, gender, national origin, age (40 or older), disability, genetic information, or sexual orientation.
- Sending unwelcome mail, voicemail or email containing derogatory jokes or comments about an individual or group because of race, color, religion, sex, gender, national origin, age (40 or older), disability, genetic information, or sexual orientation.[1]
- Treating people differently based on their protected characteristics can also be discriminatory harassment. For example, a supervisor who complains about his or her older employees' tardiness but allows workers under age 40 to come to work late without comment may be engaging in discriminatory harassment based on age.

Return to top

Sexual Harassment

Sexual harassment is a specific type of discriminatory harassment. Sexual harassment is defined as unsolicited and unwelcome sexual advances, requests for sexual favors, or other verbal or physical conduct of a sexual nature directed to any person of the same or opposite sex when (1) submission to such conduct is made either explicitly or implicitly a term or condition of an individual's employment, (2) submission to or rejection of such conduct by an individual is used as the basis for employment decisions affecting such individual, or (3) such conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile, or offensive work environment. The courts and the Equal Employment Opportunity Commission (EEOC) have defined two types of illegal sexual harassment: (1) quid pro quo (a Latin phrase meaning giving or providing something in return for something else); and (2) hostile work environment.

Quid Pro Quo Sexual Harassment

Quid pro quo sexual harassment is the easiest to recognize. It occurs when one person seeks sexual favors from another person in return for something of value. The "something of value" offered in return might consist of almost any form of favorable treatment, such as receiving a good performance evaluation or being selected for promotion.

Quid pro quo sexual harassment does ***not*** require that the harasser clearly state what specific favors are expected for what specific return. Rather, as both the courts and the EEOC have recognized, quid pro quo sexual harassment can be ***implied*** from the overall pattern of a person's actions—particularly if he or she occupies a position of authority or power over the other person.

Below are some examples of conduct that might constitute quid pro quo sexual harassment. The list is not all-inclusive; in addition, each situation must be considered in light of the specific facts and circumstances to determine whether sexual harassment occurred. A finding that sexual harassment occurred that violates this policy does not mean that illegal sexual harassment necessarily occurred.

Examples of Quid Pro Quo Sexual Harassment

- When an employee tells her supervisor that some people really don't like to have their necks and shoulders rubbed, he responds by saying, "Those who want to get ahead do."

- A manager pressures a subordinate employee to join her for dinner and dancing. When he declines, she tells him that he can't expect her to mentor him on the job if he's unwilling to spend time together after hours.
- After an employee resists her team leader's repeated suggestion that she travel with him so that they "can get to know each other better," he turns in a project evaluation rating her work "substandard."

Hostile Work Environment Sexual Harassment

Hostile work environment sexual harassment is often harder for employees and managers to recognize. It is usually found where a general pattern of workplace behavior exists that is ***sexually oriented, pervasive,*** and ***severe.*** Those descriptive terms have been defined in actual workplace situations as follows:

Sexually oriented behavior has been found to include

- letters, telephone calls, magazines, pictures, and objects of a sexual nature or content;
- the deliberate touching, brushing, cornering, or pinching of or leaning over a person;
- suggestive looks, comments, gestures, or whistles; or
- sexual jokes, teasing, remarks, and questions.

Pervasive behavior is behavior that is widespread, common, or repeated.

Behavior of a sexual nature is considered *severe* when it would be objectionable to a "reasonable person" within the circumstances.

Below are some examples of conduct that might constitute hostile work environment sexual harassment. The list is not all-inclusive; in addition, each situation must be considered in light of the specific facts and circumstances to determine whether sexual harassment occurred. A finding that sexual harassment occurred that violates this policy does not mean that illegal sexual harassment necessarily occurred.

Examples of Hostile Work Environment Sexual Harassment

- When an employee complains about the vulgar language and jokes that routinely fill the break room, her supervisor tells her to "lighten up and get used to it because that's how boys behave."
- After learning that an employee has separated from her husband and may be getting a divorce soon, a coworker has begun asking her out. After being repeatedly turned down, he has begun calling her at home to ask if she'd like him to "come over and help cure her loneliness."
- A manager calls and sends instant messages to an employee in another division repeatedly asking him to go out with her, even after he tells her he's not interested.

Return to top

Applicability of Policy

This discriminatory harassment policy applies equally to any conduct that constitutes discriminatory harassment, whether sexual harassment or some other form of discriminatory harassment.

Return to top

Responsibility of All Employees with Regard to Discriminatory Harassment, Including Sexual Harassment

It is the responsibility of all employees to refrain from engaging in, condoning, or tolerating discriminatory harassment. It is also employees' responsibility to cooperate with any investigation or inquiry into allegations of discriminatory harassment.

Return to top

Responsibility of All Supervisors and Managers with Regard to Discriminatory Harassment, Including Sexual Harassment

A supervisor or manager who witnesses or receives a report of actions that he or she believes may constitute discriminatory harassment under this policy must report the incident to the officer responsible for Employee Relations, or his or her designee. This is true whether or not the manager or supervisor is in the direct reporting chain of the victim of the alleged discriminatory harassment. After receiving a report, the officer responsible for Employee Relations, or his or her designee, must follow the investigation procedures outlined below, including immediately informing the

program director of the Office of Diversity and Inclusion (formerly called the EEO Office) of the complaint.

Return to top

Procedures for Reporting and Responding to Discriminatory Harassment, Including Sexual Harassment

Any employee who believes he or she has been subjected to discriminatory harassment, or witnessed discriminatory harassment, is encouraged to promptly report the conduct and not remain silent. Employees are encouraged (but not required) to inform the offending person orally or in writing that such conduct is unwelcome and offensive and must stop. If employees do not wish to communicate directly with the offending person, or if such communication has been ineffective, employees are encouraged to report the discriminatory harassment to their supervisor or any of the individuals designated below. When reporting a concern, employees should describe in detail the actions that are perceived to be discriminatorily harassing.

Employees who allege discriminatory harassment or who cooperate in an investigation shall not be subjected to reprisal, recrimination, retaliation, or the threat of such action. Prompt reporting and employees' continued assistance is critical to allow rapid response by management and resolution of the objectionable behavior.

An employee who believes he or she has been subjected to discriminatory harassment always has the option to initiate the EEO complaint process by contacting an EEO counselor within 45 days of the action perceived to be harassing. More detail regarding this process can be found in the "EEO Administrative Complaint Process" section of this policy; in addition, employees may wish to consult the Board's Rules Regarding Equal Opportunity at 12 CFR 268).[4]

Alternatively, an employee who believes he or she has been subjected to discriminatory harassment may report the conduct to any of the following individuals: (1) the offending individual's supervisor or the harassed employee's supervisor; (2) the offending individual's division director or the harassed employee's division director; (3) an
Employee Relations staff member in the Human Resources Function of the Management Division; (4) the officer responsible for Employee Relations, or his or her designee; and (5) for employees in Human Resources, the assistant general counsel for Human Resources in the Legal Division. The names and telephone numbers of the individuals occupying the positions identified in (3), (4), and (5), above are available by calling the Human Resources hotline at extension 3737. An employee who reports discriminatory harassment to any of these individuals will be advised of this policy and that an investigation/inquiry will be opened by Employee Relations as set forth in this policy.

Return to top

Employee Relations Investigation/Inquiry Procedure

Any individual, including an employee of the Office of Diversity and Inclusion, who receives an allegation that he or she believes may constitute discriminatory harassment under this policy must report the allegation to the officer responsible for Employee Relations, or his or her designee. Upon receipt, the officer responsible for Employee Relations or his or her designee must

1. document the allegation received;

2. inform the individual who believes that he or she was subjected to discriminatory harassment that he or she may initiate the EEO complaint process by contacting an EEO counselor in the Office of Diversity and Inclusion within 45 days of the action perceived to be harassing; and

3. inform the program director of the Office of Diversity and Inclusion of the complaint, and ascertain from the program director whether the Office of Diversity and Inclusion will investigate the complaint or whether Employee Relations will.

Depending upon the determination in 3, above, either Employee Relations or the Office of Diversity and Inclusion will

1. investigate the allegation, including documenting the investigation;

2. evaluate the results of the investigation and determine whether discriminatory harassment may have occurred;

3. if discriminatory harassment occurred, determine the appropriate management response, including the proposed action to be taken against the employee who engaged in discriminatory harassment;

4. ensure implementation of (including documenting of) management's response and, if problems are encountered with implementation, immediately report

such problems to the program director of the Office of Diversity and Inclusion;

5. follow up with the victim to ensure management's response effectively addressed (ended) the discriminatory harassment (including documenting the employee's response); and

6. in the unusual event the employee indicates that discriminatory harassment has continued, immediately report the problem to the program director of the Office of Diversity and Inclusion, and consider additional management responses that may more effectively stop the harassing activity (e.g., taking more stringent action against the employee who engaged in discriminatory harassment).

In no case shall the individual being accused of harassment have supervisory authority over the individual who investigates the harassment or over the investigation more generally. Other immediate measures to stop any harassing conduct and prevent further harassment may include granting interim relief to the victim of the harassing conduct before completing an investigation. Examples of such interim relief include making scheduling changes so as to avoid contact between the parties, transferring the alleged harasser, or placing the alleged harasser on administrative leave with pay pending the conclusion of the investigation.

Where an investigation has established that an employee engaged in discriminatory harassment, he or she may be subject to discipline or other appropriate management action, ranging from a letter of reprimand to suspension without pay, to separation for cause, in accordance with the Board's Adverse Action policy or its Disciplinary Actions policy. Oral or written performance feedback may also be considered. Furthermore, the offending employee may also be required to attend training designed to address his or her harassing conduct. Where an investigation has established that a manager condoned harassing conduct, ignored complaints of such conduct or otherwise failed to properly carry out the responsibilities provided under this policy, he or she may be subject to disciplinary action and/or be required to attend training to assist the manager in identifying and preventing discriminatory harassment in the future.

Management will protect the confidentiality of all harassment allegations to the fullest extent possible. However, such information may have to be disclosed to management and employees with a need to know in order to carry out the purpose and intent of this policy. For example, management will need to disclose sufficient facts to the alleged harasser to enable the Board to investigate the allegation of harassment. In addition, information relating to the alleged harassment may have to be disclosed in any litigation involving the Board to which the information may be relevant or necessary.

Return to top

EEO Administrative Complaint Process

An employee subjected to discriminatory harassment may choose to initiate the administrative EEO process with the Board's Office of Diversity and Inclusion by contacting an EEO counselor within 45 days of the action perceived to be harassing. If an employee has reported an incident to Employee Relations in a timely manner and Employee Relations' investigation has not been completed before the 45-day period for filing an EEO complaint, the employee may request in writing that the program director of the Office of Diversity and Inclusion stay, for a specific period of time, the time for filing a complaint. The program director of the Office of Diversity and Inclusion will consider requests that stay the filing deadline for the time it takes to resolve any internal investigation or inquiry and will inform the employee in writing whether the stay has been granted and, if so, for how long.

An employee's right to initiate the EEO process does not diminish in any way management's responsibility to ensure that discriminatory harassment does not occur. Even if an employee chooses not to use the procedures in this policy to report harassing conduct and instead initiates the EEO process with the Office of Diversity and Inclusion, the Human Resources Function of the Management Division may choose to initiate an investigation/inquiry using the procedures in this policy.

The Board forbids retaliation against any employee who reports harassment to an EEO counselor or management official, files an EEO complaint, or otherwise participates in a discriminatory harassment investigation/inquiry.

Return to top

Appeals Process

An employee subject to disciplinary action for conduct that violates this policy may appeal such disciplinary action under procedures set out in the Board's Disciplinary Actions policy or the Adverse Action policy, as appropriate.

Return to top

Responsibility for Policy

The Human Resources Function of the Management Division and the Office of Diversity and Inclusion are responsible for the administration and interpretation of

this policy. Division directors will consult with the Board's Office of Diversity and Inclusion, as necessary, in carrying out their responsibilities under this policy. This policy will be reviewed and updated as necessary.

Return to top

Footnotes

1. Note that the Board's Information Technology Permissible-Use and Privacy policy forbids employees from disseminating material that is offensive or harassing in nature, including material that disparages others on the basis of race, color, religion, sex, gender, national origin, age (40 or older), disability, genetic information, or sexual orientation, even if such dissemination is not "unwelcome." Return to text.

2. While a victim of harassment is free to initiate the EEO process in lieu of using the reporting process described in this policy, a victim of harassment who unreasonably fails to use available, effective complaint mechanisms designed to stop the harassment is less likely to prevail on a claim of discriminatory harassment, including hostile work environment sexual harassment. Return to text.

FRS ALERT
Jan. 27, 2015 - 5:06 p m.

inside the board

Board Policies

Adjusting Work-Related Problems

Approved by H. Fay Peters, effective June 30, 2010

Jump to section: Policy Statement

Policy Statement

All employees are to be treated fairly and equitably. Managers and their staffs are encouraged to create and maintain an atmosphere of mutual trust, respect, and open and objective communication. Most work-related problems, complaints, disputes, and differences of opinion can be resolved once they are discussed with the employee's supervisor. If the problem cannot be resolved through discussion, employees are encouraged to follow the procedure described below.

Return to top

Covered Problems

A work-related problem covered under this policy can be any issue that arises in the context of a work situation *and* that is not within the scope of the following management policies: Adverse Action Policy and Procedures, Disciplinary Actions, Sexual Harassment, Reasonable Accommodation, Performance Management Program, Equal Employment Opportunity, Provisional Employment Period, and Provisional Period for Newly Selected Managers and Supervisors. Accordingly, the procedure set forth in this policy may not be used in lieu of appeal procedures provided in other policies that establish an exclusive remedy and may not be used to avoid conditions or limitations set out in such other policies. When a work-related problem is addressed under another management policy, any complaint or appeal under this policy regarding the same work-related problem will be dismissed, and the matter will be addressed under the other applicable policy.

Work-related problems include, but are not limited to, employee complaints or questions regarding unfair treatment on the basis of conduct or reasons that do not adversely affect the employee's performance and that are not covered under existing laws regarding discrimination. Such matters may include allegations of discrimination in employment on the basis of sexual orientation.

Return to top

Definitions

Employee means an individual who works full-time or part-time and is appointed into Board service for a period of more than 90 calendar days.[1] The term *employee* does not include members of the Board or nonregular employees, that is, student aides, worker-trainees, student interns, co-op employees, or individuals who are serving in a temporary term-limited position.

The term *employee* also does not include an *at-will* employee, that is, an individual serving at the pleasure of the Board and who may be discharged from Board service for any reason that is not illegal.

Return to top

Procedure for Addressing a Work-Related Problem

Employee relations specialists in the Employee Relations section (ER) of the Management Division are available to help employees and managers address work-related problems. They ensure that employees are aware of their rights and guide them through the steps outlined in the following procedure. An employee relations specialist may also help resolve cases by gathering facts, consulting with the employee regarding his or her concerns, and recommending a course of action. An employee relations specialist may be consulted at any time before or during the

process.

Step 1. An employee should first discuss any work-related problem (or problems) under this policy with his or her immediate supervisor as soon as possible. Unless unusual circumstances exist, an employee should bring the matter to the attention of the supervisor within 15 working days from the date the employee first became aware of the matter or from the effective date of the action giving rise to the work-related problem. Experience has shown that most problems can be settled once they are brought to the attention of the supervisor and discussed fairly and openly.

Step 2. If the problem is not resolved within 15 working days after it has been brought to the attention of the immediate supervisor, the employee may submit a written description of the problem within five working days to the manager or officer responsible for the functional area. This person may, depending on the organizational structure, be the same person as the immediate supervisor. The manager or officer responsible for the functional area will review the problem and issue a written decision within 15 working days of receipt of the employee's written description of the problem.

Step 3. If the employee is not satisfied with the decision of the manager or officer responsible for the functional area, the employee may appeal to the division director. Any such appeal must be filed within five working days of the employee's receipt of the manager's or officer's decision. The appeal must be submitted in writing to the division director. If the division director is the same person as the manager or officer responsible for the functional area (as described in step 2), the employee may ignore step 3 and proceed to step 4. The division director will issue a written decision within 15 working days of receipt of the employee's appeal.

Step 4. If the employee is not satisfied with the decision of the division director (or of the manager or officer responsible for the functional area if that person is the same person as the division director), the employee may select one of the following two options:

- *Officer responsible for ER (ER Officer).* The employee may appeal the decision of the division director to the ER Officer or to his or her designee. Any such appeal must be filed within five working days of the employee's receipt of the division director's decision and must be submitted in writing. The ER Officer, or his or her designee, will issue a written decision within 15 working days of receipt of the employee's appeal. The decision of the ER Officer is final and binding.

  For employees in the Management Division, this appeal shall be made to a Board officer outside the Management Division, who shall be designated by the chairman, Committee on Board Affairs, rather than to the ER Officer. The decision of the officer appointed by chairman, Committee on Board Affairs, shall be final and binding.

  The decision of the ER Officer or, as appropriate, a Board officer designated by the chairman, Committee on Board Affairs, may be implemented under delegated authority.

- *Mediation.* Within five working days of the employee's receipt of the division director's decision, the employee may request that a mediator be engaged to help bring about a mutually acceptable resolution to the problem. The mediation between the employee and division management will be governed by the procedures described in the Employee Relations Mediation Guidelines.

  If mediation does not resolve the problem, the employee may choose to appeal the decision of the division director to the ER Officer in accordance with the provisions of step 4.1 above. Any such appeal must be made within five working days of the conclusion of the mediation.

Review of Documentation at Each Level

In reviewing an appeal, the reviewing authority at each level has the discretion to conduct whatever investigation he or she deems appropriate, including requesting supplementary information from the employee or from management. The reviewing authority, however, may choose to issue a decision based on a review of the appeal and any documentation that may have been initially presented.

Submission of Documentation

At any stage of the process, the employee may submit additional material. Such material must be submitted, as applicable, by the date the written description of the problem or the date the appeal is due.

Any material submitted to the ER Officer in connection with an appeal will be shared with the employee's management unless the ER Officer does not rely on the information in reaching a decision or if the ER Officer determines that disclosing the

information would create or exacerbate an employee relations issue. Any documentation submitted by the division in connection with an appeal will be shared with the employee except to the extent that doing so infringes on the privacy rights of other employees.

Time Limits

The ER Officer can extend the time limits contained in this policy. No procedural rights or requirements that are not specifically stated in the procedure may be implied.

Return to top

Responsibility

The Management Division has the discretionary authority to administer and interpret this policy. The Board may review, update, and amend this policy at any time.

Return to top

Footnotes

1. Applicants for employment with the Board may invoke the procedures in this policy for claims of unfair treatment on the basis of sexual orientation. Return to text.

inside the board

Board Policies

Cash Compensation Program

Approved by H. Fay Peters, effective June 30, 2010

Jump to section: Policy Statement

Policy Statement

The Board's Total Rewards Program consists of cash compensation, benefits, work environment, career development opportunities, and intrinsic rewards. As part of *Total Rewards*, the Board's various cash compensation programs are designed to (1) attract, motivate, and retain highly skilled employees; (2) balance external competitiveness and internal fairness; (3) reward employees according to their individual performance and contribution to organizational goals; (4) provide reasonable flexibility in the management of employee pay so as to respond to employment pressures and changing market conditions; and (5) comply with applicable laws and regulations.

Return to top

Definitions

Cash compensation programs: These programs include (1) base salaries and the guidelines used to set and adjust salaries, and (2) additional pay programs, such as cash awards, variable pay plans, sign-on and retention bonuses, project incentives or pay as described in the Overtime and Other Forms of Premium Pay Policy.

Employee: An employee is defined as an individual who works full- or part-time and is appointed into Board service for a period of more than 90 days. The term does not include members of the Board, student aides, worker-trainees, student interns, co-op employees, or those serving in a temporary term-limited position.[1]

Base salary: Base salary means the employee's annual rate of basic pay. Base salary does not include variable pay, cash awards, lump-sum merit increases, sign-on bonuses, retention bonuses, project incentives, shift differential, overtime pay, holiday pay, availability pay, unscheduled duty pay, premium pay, or any other type of pay that the Board does not treat as base salary.

Return to top

Guidelines: Base Salary Programs

New Employee Starting Salaries

The Human Resources (HR) Staffing function, with guidance from the HR Compensation function and in conjunction with input from the Board hiring division, determines starting salaries. Starting salaries are based on one or more of the following factors: (1) the experience and qualifications of the new employee; (2) salary alignment with other staff in the hiring division or job family, as appropriate; (3) market comparisons relevant to the specific position; (4) current salary of the prospective employee; and (5) the business needs of the hiring division. Generally, a new employee's salary may be set anywhere within the salary range, depending upon the employee's qualifications and market conditions. Starting salaries more than 10 percent above the midpoint of the range will be reviewed by HR Compensation.

Return to top

Salary Increases

Annual Merit Increase

Annual merit increases in base salary are based on performance during the past year, as reflected in employee performance evaluations and as outlined in the Board's

Performance Management Program (PMP). Generally, employees hired on or before June 30 of the performance year are eligible to receive annual merit increases based on the formal PMP review.[2] An employee rated marginal or unsatisfactory during his or her most recent annual PMP review (annual PMP) is not eligible for a merit increase. An employee hired after June 30 of the performance year is generally not eligible for a merit increase, but may receive a salary increase up to an amount published annually by the HR Compensation staff. Each division director decides whether or not to grant salary increases in such cases, subject to final sign off by HR after Compensation staff validate that the actions are consistent with policy.

Periodic salary-range adjustments: The Board may adjust salary ranges periodically based on the results of available salary information from custom and/or published surveys. When salary ranges are adjusted, an employee's salary may fall below the minimum of the new salary range. In this case, an employee whose most recent annual PMP was commendable or better is eligible to receive a merit and/or special salary increase to bring his or her salary to at least the minimum of the new salary range. An employee rated marginal or unsatisfactory will not have his or her salary brought to the minimum of the salary range until his or her performance, as reflected on an annual PMP review, reaches the commendable or better level.

Merit increases and the maximum of the salary range: If a merit increase will take an employee's salary above the maximum of the range for his or her grade, the employee will receive a merit increase sufficient to bring his or her salary to the maximum of the range, and will receive the remainder of the increase in the form of a lump-sum merit payment, provided that his or her PMP rating is commendable or better. If an employee's salary is at the maximum of the range, the employee will receive the full amount of the increase in the form of a lump-sum merit payment.[3]

Merit increases and job/supervisor changes: When an employee transfers or changes direct supervisors during the performance period (October 1 through September 30), and is eligible for a merit increase for that year, the increase will be based on his or her annual PMP. An interim (close-out) PMP should be given at the time of the transfer. However, if this does not occur, input from previous supervisor(s) will be sought for the annual PMP.

Promotional Increase

When an employee is promoted to a higher grade level, the employee's salary level should be increased to at least the minimum of the salary range of the new grade. In making a promotion salary increase recommendation, managers should consider the following:

- the employee's education and experience in relation to the minimum qualifications of the position
- the salaries of other employees in similar positions within the division, section or office
- the placement of the recommended salary relative to the new salary range

A division director can approve a recommended salary increase up to 12 percent (15 percent if an employee is promoted multiple grades) for any staff level, subject to final sign off by HR after Compensation staff validate the action is consistent with policy.

Special Salary Adjustment

Special salary adjustments may be necessary when external or internal considerations affect the salary of an individual, the salaries of those employees in a particular job family, or the salaries of a group of employees in general. For example, special adjustments may be needed to retain employees who possess skills for which HR has determined market demand exceeds supply or other significant market factors exist. An employee with a rating of marginal or unsatisfactory on his or her most recent PMP review (annual or interim) is not eligible for a special salary adjustment. Requests by managers for adjustments up to 5 percent (on an annual basis) can be approved by division directors (with subsequent notification to, and automatic sign off by, HR of the adjustments made using a form noted below); requests over 5 percent will be reviewed and approved by HR after Compensation staff review them on a case-by-case basis. In addition, a special salary adjustment for an employee who has already received an adjustment within the past 12 months must be reviewed by HR Compensation staff for approval.

In making special salary adjustments, divisions should consider one or more of the following factors:

- internal equity with other staff salaries
- consistency with the Board's pay-for-performance philosophy
- retention of incumbents with critical knowledge and competencies

- comparative employee performance over time
- job enlargement, such as taking on duties that have a greater scope than originally envisioned
- market averages for the job
- special market pressures that may affect the job, such as skill shortages
- completion of a PhD (by economists)

To process a special salary adjustment, the requesting division director (or the director's designee) must submit a completed *Special Salary Adjustment Request* form and forward it to HR Compensation staff for review or approval, as appropriate. The form must be submitted for inclusion in the employee's records, even in cases where the division director has the authority to approve the adjustment.

Lateral Transfer Equity Adjustment

Generally, salary increases are not granted for cross-divisional lateral transfers (i.e., a transfer to a position at the same grade) at the Board. However, special circumstances, such as ensuring internal equity, may support salary increases in the range of 3 percent to 5 percent. These increases are considered exceptions, and are reviewed and approved by HR Compensation staff on a case-by-case basis.

Return to top

Salary Grade Reductions

A reduction in grade and salary can occur: (1) voluntarily at an employee's request; (2) involuntarily without cause through job abolishment or reclassification; or (3) involuntarily in accordance with the Board's Adverse Action Policy.

Voluntary Reduction

A voluntary reduction in grade level occurs when an employee is reduced in grade as a result of a (1) change in career focus, (2) request to reduce an employee's workload, (3) need to address personal issues, or (4) need to address performance problems (accepting a lower grade level voluntarily in lieu of a formal adverse action).[4]

The employee's grade will be reduced and his or her new salary will be set within a new salary range, if possible. If the current salary is within the range of the new grade level, no decrease in salary will occur. Thereafter, normal salary-administration procedures will apply. If the employee's salary is above the maximum of the range for the lower grade, the employee's salary will be frozen, and no salary increases will occur until the maximum of the range for the new lower grade exceeds the frozen salary level. If, after two years at the new grade, the employee's salary remains above the maximum of the range for the lower grade, the salary will be reduced to the maximum of that grade. If an employee is promoted to a higher grade level within the two-year timeframe, the employee will not normally receive an increase in base salary.

Involuntary Reduction without Cause

An involuntary reduction in grade can occur as a result of (1) the reclassification of a job to a lower grade level, or (2) the abolishment of a position.

An employee will retain his or her current grade and pay for two years from the date of the reclassification decision or from the effective date of the abolishment decision. After two years, the grade will be reduced. If the employee's salary is above the maximum of the new range after the two years, the employee's salary will be frozen, and no salary increases will be granted until the maximum of the range for the reduced grade exceeds the employee's frozen salary. Thereafter, normal salary-administration procedures will apply.

Involuntary Reduction with Cause

An employee's salary and/or grade may be reduced in accordance with the procedures set out in the Board's Adverse Action Policy. The employee's salary and/or grade will be reduced upon the effective date of the action.

Return to top

Guidelines: Additional Pay Programs

In addition to base salary, the Board provides a number of other pay programs, such as sign-on and retention bonuses, cash awards, project incentives, and variable pay.

Sign-on Bonuses

Sign-on bonuses are designed to assist in recruiting new employees for positions that

are under market pressure and, in the absence of such bonuses, would be difficult to fill.

Source of funds. Divisions fund these payments from their individual operating budgets and not through their cash award allocations.

Eligibility and amount.[5,6] In determining the appropriateness of paying sign-on bonuses and the amount, the following factors should be considered:

- the results of recent efforts to recruit candidates for the same or similar positions
- recent turnover rates for the same or similar positions
- current labor market factors that may affect the ability of the Board to recruit candidates for the same or similar positions
- special qualifications required for the position as well as the demand at the Board and in the marketplace for those qualifications
- assessments of internal-equity, base-salary considerations when making hiring offers

Sign-on bonuses may be paid in lump-sum form or paid out in installments. For lump-sum sign-on bonuses, if an employee's employment with the Board is terminated voluntarily or involuntarily within the first year of employment, the pro-rated balance of the bonus must be returned based on the number of months remaining. In cases where sign-on bonuses are awarded, upon voluntary or involuntary termination, the employee forfeits unpaid installments. The terms and conditions of sign-on bonuses are specified in the *Sign-On Bonus Program* receipt form, which must be signed by employees as part of offer packages.

To obtain authorization for payment of sign-on bonuses, a division director (or the director's designee) must complete the *Sign-On Bonus Program* request and receipt form(s), and submit them to the HR Staffing supervisor for approval before an offer is extended.

Retention Bonuses

Retention bonuses are designed to increase the flexibility of cash compensation packages and ensure the availability and continuity of critical skills and knowledge needed to meet business objectives.

Source of funds: Divisions fund these bonuses from their individual operating budgets and not through their cash award allocations.

Eligibility and amount:[7] Division requests for retention bonuses and specific amounts should consider one or more of the following factors:

- criticality of the knowledge, skills, and abilities needed
- current market conditions and practices
- availability of replacements
- critical project completions/requirements
- knowledge transfer
- length of time for which the knowledge, skills, and abilities are needed
- employee performance

Retention bonus amounts may vary. The bonus shall be paid for a specific project or a retention period and, except for the final payment, shall normally not exceed a maximum of one-third of the annual base salary each year (except in the final year of a multi-year retention agreement).

Payment options and conditions. An employee who has received a sign-on bonus may not receive a retention bonus until 12 months have elapsed since either the date of hire or the last installment of the sign-on bonus has been paid to him or her.

Retention bonus agreements. Guidelines for administering retention bonuses are as follows:

- *Length of agreements:* A retention arrangement should not normally extend for more than three years, and may be distributed monthly, quarterly, multi-year, or in one lump sum payment.
- *Maximum annual payout:* No more than 40 percent of the bonus awarded shall be paid before the conclusion of the specified project or retention period.

- *Employee acknowledgment:* The employee must acknowledge and sign an understanding of both the bonus percentages and the project benchmarks or retention period.
- *Future retention agreement:* If it is necessary to retain the employee beyond the designated retention period, new retention arrangements may be established.
- *Employment termination:* Any employee who terminates employment before the conclusion of the retention period shall forfeit any unpaid bonus amounts.
- *Performance expectation:* The commitment to pay a retention bonus is based upon the *continued satisfactory performance* of the intended recipient, meaning the employee must continue to meet established standards of the job, maintain productivity requirements, and perform all assigned responsibilities. The employee must also receive a performance rating of commendable or higher, and must not have been subject to disciplinary action. The Board will withhold all unpaid retention bonus payments if the recipient's performance does not meet expectations.
- *Change in circumstances:* A retention agreement should include provisions that cover payment of the unpaid retention bonus if the Board finds that circumstances occur affecting the criticality of the criteria listed above before the end of the agreed upon project or retention period or if an employee transfers to another position within the Board.

Except for the economist retention program (in which the division director or division director's designee approves the retention bonus), the director of the Management Division must approve all requests for retention bonuses. To obtain authorization for payment of a retention bonus, the requesting division director (or the director's designee) must submit the *Retention Bonus Plan* request and receipt forms to the HR Compensation staff to validate that the terms of the retention bonus have been met and to sign off on the payment. Terms and conditions for a retention bonus are specified on the *Retention Bonus Plan* receipt form and signed by the employee.

Cash Awards

There are two types of cash awards: (1) project-based, and (2) performance-based. Cash awards may be provided to individual employees or to groups of employees (for example, a project team).

Source of funds. The Board provides the funding for cash awards in each division's budget, and divisions may not exceed the allocation of funds for cash awards.

Eligibility. Any employee, except one who receives--or is eligible to receive--a variable pay award at any time during the relevant performance period, may be nominated for a cash award. To be eligible to receive a cash award, the employee must *not* have been subject to any type of written disciplinary action during the performance period or received (if eligible) a PMP rating below commendable.[8]

The division director (or the director's designee) can approve an employee's cash award, based on whether the employee:

- initiated, recommended, or accomplished actions that achieved important Board goals, improved productivity, realized significant cost reductions, or improved the productivity or quality of Board services;
- responded to unforeseen circumstances or events in an exemplary fashion;
- resolved, or made significant progress toward resolving, significant operational problems;
- made a unique and significant contribution that resulted in a section or group meeting its objectives when factors such as new laws or regulations, severe staff turnover, or a dramatic increase in work volume presented additional challenges;
- made outstanding contributions, on behalf of the Board, to a profession or organization, and those contributions enhanced the Board's image and or strengthened its external relations; or
- performed at a high level for a sustained period.

To process a project-based cash award at any time during the year or performance-based cash award at any time other than at year-end, the division director (or the director's designee) must complete the *Cash Award Nomination* form and submit it to HR Compensation staff, who will then validate and sign off on awards that satisfy one or more of the above criteria.

For end-of-year cash awards for sustained high performance, divisions need only state

the employee's name, determine the proposed amount of the award, and indicate the appropriate award criteria. HR Compensation will provide divisions annually with instructions required for end-of-year processing and will sign off on awards after validating they meet eligibility criteria.

Amount. Cash awards may be made in any amount up to an annual maximum of 30 percent of an employee's base salary. If an employee receives more than one award within the same calendar year, then the total of all cash awards received (including targeted cash awards and/or project incentives) for that year must not exceed 30 percent of the employee's base salary.

Targeted Cash Awards

Targeted cash awards allow divisions to reward employees outside the normal cash award program subject to one or more of the eligibility criteria below.

Source of funds. The Board provides the funding for targeted cash awards, and funding is separate and apart from the normal cash award allocation.

Eligibility. Any employee, except one who receives--or is eligible to receive--a variable pay award at any time during the relevant performance period, is eligible to be nominated for a targeted cash award. The employee must *not* have been subject to any type of written disciplinary action during the performance period for which the targeted cash award is issued or received (if eligible) a PMP rating below commendable.

The division director (or the director's designee) approves an employee's recommended targeted cash award, based on the award satisfying at least one or more of the following criteria:

- It addresses external compensation market pressures.
- It recognizes significant specific project-based achievements by the employee.
- It recognizes and helps to retain specific critical skills of the employee.

To obtain authorization for targeted cash awards, the division director (or the director's designee) must complete the *Targeted Cash Award Nomination* form and submit it to HR Compensation for sign off after validating the awards meet eligibility criteria.

Amount. The total of all cash awards may be made in any amount up to an annual maximum of 30 percent of an employee's base salary. If an employee receives cash awards, targeted cash awards, and/or project incentives within the same calendar year, then the total of all awards for that year must not exceed 30 percent of the employee's base salary.

Project Incentives

The establishment of project incentive plans provides means to recognize Boardwide or System initiatives (e.g., Y2K, Basel II) to motivate, reward and encourage individual employees or project teams to achieve project milestones and goals necessary to meet business objectives. Divisions should work with HR to design project incentives that complement merit increases and cash awards, taking into account *total reward* objectives for employees.

Source of funds. The division should fund project incentive plans through requests for additional funds from the Board using the normal budget adjustment process and with the review of the director of Management Division and approval of the chair of the Committee on Board Affairs.

Eligibility. Divisions may pay project incentives to individual employees or project teams that serve as contributors to the successful completion of a project plan. Staff receiving variable pay are eligible to receive project incentives.

Amount. Project incentive amounts may vary. In determining whether an incentive payout and payout amount is appropriate, the division director (or the director's designee) should consider one or more of the following factors:

- the impact of project completion on the Board's mission, objectives, and operations
- the complexity and scope of the project
- the extent to which the performance is above and beyond expectations
- the special skills and qualifications required for the project

Project incentive agreements. Guidelines for administering project incentive plans are

as follows:

- *Maximum annual payout.* Project incentives shall be paid for a specific project and shall not exceed a maximum of 30 percent of an employee's annual base salary each year. If an employee receives cash awards, targeted cash awards, and/or project incentives within the same calendar year, then the total of all awards for that year must not exceed 30 percent of the employee's base salary in that year.
- *Additional payout condition.* No more than 40 percent of the project incentive awarded shall be paid before the conclusion of the specified project.
- *Employee acknowledgment.* The employee must acknowledge and sign an understanding of both the potential bonus amount and the expectations, with the latter including project benchmarks and deliverables.
- *Employment termination.* Any employee who terminates employment before the conclusion of the incentive period shall forfeit any unpaid incentive money.
- *Performance expectations.* Payment of a project incentive is contingent upon *continued satisfactory performance* by the intended recipient. In other words, the employee must continue to meet specific project milestones and established job standards; maintain productivity requirements; perform all assigned responsibilities; possess a current performance rating of commendable or higher; and not have been subject to any type of written disciplinary action during the performance period. The Board will withhold all unpaid incentive payments if the recipient's performance does not meet expectations.
- *Changes in circumstances.* The incentive agreement should include provisions that cover payment of the unpaid project incentive if the Board finds that circumstances change regarding (1) the project's relative importance and/or priority, or (2) the employee's involvement in the project.

To obtain authorization for payment of a project incentive, the requesting division's director (or the director's designee) must submit the *Project Incentive Plan* request and receipt forms to the HR Compensation staff to validate the terms of the plan have been met and to sign off on the payment. Terms and conditions for a Project Incentive Plan are specified on the *Project Incentive Plan* receipt form and signed by the employee.

Variable Pay

Variable pay is generally targeted toward employees appointed as Official Staff of the Board (officers) and employees in designated job families that: (1) are critical to the execution of the Board's core mission; (2) require skills that are in high demand in the marketplace; (3) offer salaries well below prevailing market levels; and (4) experience recruiting difficulties and high rates of turnover. HR Compensation staff reviews new variable pay requests for additional job families, and makes a recommendation to the chair of the Committee on Board Affairs, who makes the final determination. Employees who receive variable pay are not eligible to participate in the Board's cash award and targeted cash award programs; however, they may participate in the merit pay program.[9] Participation in other programs (i.e., a retention bonus plan) is restricted to situations where a compelling business case exists, and requires approval from the director of the Management Division unless otherwise provided for in this policy.

Source of funds. Each year, the Board determines whether to allocate funds to the variable pay program for the following year. Whether variable pay is funded, and the level at which it is funded, is based on (1) market conditions and (2) the Board's experience in retaining and recruiting staff into officer positions and specific job families. If variable pay is funded, the funding level is expressed as a percentage of the total annual salaries of eligible employees (broken out by salary liability for officers and non-officers) in each division. Divisions may not exceed the allocation of funds for variable pay.

Officers

Officer eligibility.[10] To be eligible to participate in the officer variable pay program, an employee must occupy an officer position (and not be in the Personnel Placement Program),[11] have a current performance rating of commendable or higher, and *not* have been subject to any type of written disciplinary action during the performance period.[12] The amount of a division director's variable pay award will be determined by the division's respective oversight governor, in consultation with the chief human capital officer (CHCO), and with the concurrence of the chair of the Committee on Board Affairs. The Board of Governors approves the amount of a division director's

variable pay award. For all other officers, the respective division director recommends variable pay amounts with the concurrence of the division's respective oversight governor and, when needed to ensure consistency and/or fairness in recommendations, in consultation with the CHCO. The chair of the Committee on Board Affairs reviews and approves officer variable pay awards (other than those for directors).

Maximum payout amount. The total of variable pay awards for the performance period must not exceed 30 percent of an officer's base salary. In addition, the total of variable pay awards and base salary cannot exceed the total cash compensation cap.[13] To receive payment, an eligible officer must be an active employee as of the date variable pay is distributed.

Officer variable pay awards are based on one or more of the following:

- the officer's performance rating under the Board's Performance Management Program
- an assessment of whether the officer has knowledge or skills uniquely valuable in carrying out the Board's work
- an assessment of whether the officer has skills that command a substantial salary premium in the external job market
- an evaluation of the awards necessary to relieve salary compression (and in some cases inversion) between officers and senior professional staff in each division

Non-Officers

Non-officer eligibility. To be eligible for variable pay, an employee must not be in the Personnel Placement Program,[14] have a current performance rating of commendable or higher, and *not* have been subject to adverse or disciplinary action during the performance period. In addition, the employee must occupy a position in the grade FR-27 to FR-29 range and be in a job family approved for variable pay.

Amount of variable pay awards for non-officers. The amount of a non-officer's variable pay award is based on performance and division director approval.

Maximum payout amount. The total of a variable pay award and project incentive plan award for the performance period must not exceed 30 percent of the non-officer's base salary. In addition, the total of variable pay awards, qualified project incentive plan awards, and base salary may not exceed the Board's total cash compensation cap. Variable pay will only be paid out to non-officers who occupy positions eligible for variable pay at the time variable pay is distributed.[15]

Non-Monetary Awards

At the discretion of each division director, a portion of a division's cash award budget may be used to fund de minimis, non-monetary awards to employees. A de minimis award is any property or service that has so little value that accounting for it would be unreasonable or administratively impracticable. Examples of such awards include movie tickets, meals, and keepsakes (such as mugs, plaques, key chains, and t-shirts). These awards may not be issued as cash or cash equivalents, such as gift certificates. The fair market value of de minimis awards must not exceed $75 per employee per year. Divisions that wish to offer de minimis, non-monetary awards to employees should consult their HR Compensation Specialist to designate an appropriate funding level, and discuss administrative procedures that will apply to granting the awards. A non-monetary award is not included in an employee's salary for any purpose.

Return to top

Exceptions for Employees in the Management Division

When the Management Division is requesting an exception to any portion of this policy for one of its employees, it shall make a request to the chairman, Committee on Board Affairs or his or her designee. The decision of the officer appointed by the chairman, Committee on Board Affairs, shall be final.

Return to top

Responsibility

The Human Resources function administers this policy. Unless otherwise noted in this policy, exceptions to this policy must be approved by the Board's CHCO in consultation with the deputy director for the Management Division.[16] The Board reserves the right to amend this policy at any time.

Return to top

Footnotes

1. A term-limited appointment is limited to a set period after which time the appointment expires and Board employment ends. Return to text.

2. Economists and research assistants generally become eligible to participate in the annual merit process in the December following their completion of one year of employment. An economist or research assistant may be eligible earlier, depending upon the hire date; eligibility is specified at the time of the job offer. Worker-trainees, student interns, co-op employees, and student aides are not eligible for merit increases, but may receive a salary increase up to an amount published annually by HR Compensation staff. Return to text.

3. Employees who have taken a voluntary or involuntary reduction in grade and are at or above the maximum of their salary range are not eligible to receive lump sum merit payments. Return to text.

4. Exceptions to these provisions may be granted on a case-by-case basis for employees who initiate a voluntary grade reduction as part of a change in career focus. Return to text.

5. The chairman of the Committee on Board Affairs approves, when needed, any changes to the maximum sign-on bonus amount permitted. Return to text.

6. Sign-on bonuses and retention bonuses for economists are administered in accordance with the program approved by the Board in February 2001. Return to text.

7. Sign-on bonuses and retention bonuses for economists are administered in accordance with the program approved by the Board in February 2001. Return to text.

8. New hires that have not received PMP rating and are not subject to disciplinary action are eligible to receive cash awards. Return to text.

9. Officers and staff who are eligible and/or receive variable pay may participate in project incentive plans only when the funding is from outside the division's normal cash award allocation. Return to text.

10. Taking an approved leave of absence, whether paid or unpaid, may affect eligibility for an award. If an employee takes such leave, its length and nature may be considered in determining the amount of a variable pay award. Return to text.

11. Refer to the Personnel Placement Program Policy. Return to text.

12. Variable pay awards for economists are administered in accordance with the program approved by the Board in February 2001. Return to text.

13. On an annual basis, the Board reviews the total cash compensation cap. Return to text.

14. Refer to the Personnel Placement Program Policy. Return to text.

15. Taking an approved leave of absence, whether paid or unpaid, may affect eligibility for an award. If an employee takes such leave, its length and nature may be considered in determining the amount of the variable pay award. Return to text.

16. Exceptions to the policy requested by the Management Division must be approved with the concurrence of the chairman, Committee on Board Affairs. Return to text.

Return to top

inside the board

Board Policies

Vacant-Position Posting

Approved by Don Hammond, effective December 20, 2012

Jump to section: Policy Statement

Policy Statement

The Board's policy is (1) to hire the best qualified candidates from the pool of internal and external applicants for vacant positions[1] and (2) to promote, through its posting procedures, employee awareness of available career opportunities. The Board generally provides employees the first opportunity to apply for open positions; if employees meet the minimum qualifications and apply during the initial posting period, they will be interviewed by the hiring division. This policy is also intended to promote an open process by providing feedback to employees when they are not selected for a position.

Return to top

Postings

Human Resources (HR) will post notices about vacant positions in the FR and Wage Employee grade levels, with the following exceptions: (1) the positions are filled through the Personnel Placement Program; (2) an employee is reassigned to a vacancy at the same grade and with the same career-ladder potential (for example, a dual-occupancy position or positions that result from a division reorganization); (3) the positions are temporary (365 calendar days or less); (4) the positions are reserved for cooperative education programs and internships; (5) the positions are used to rotate candidates for a specific developmental program; (6) the positions are filled by employees returning from leave, regular military service, long-term disability leave, special assignments, or officially approved leaves of absence; and (7) the positions are filled through the required transfer of disabled employees, pursuant to the requirements of the Rehabilitation Act. In response to organizational needs, the HR officer responsible for Talent Acquisition may make other exceptions on the basis of a division director's written recommendation.

Return to top

Eligibility

To be eligible to apply for a posted vacant position, employees must (1) be rated Commendable or above on their most recent annual or interim Performance Management Program evaluation (if they have had one), (2) have served at least six months in their current position (except for worker-trainees, co-op employees, and interns), and (3) not have been subject to disciplinary action (suspension and above) within the immediately preceding six months. With the concurrence of the current supervisor and hiring manager and with HR approval, employees who do not satisfy the above eligibility requirements may, under certain circumstances, be allowed to apply for a vacancy.

Return to top

Posting Requirements

1. The Board will post vacant-position notices internally until the position is filled.

2. Divisions may post positions at the same grade (or a different grade in the career ladder) as that held by the previous incumbent, depending on the specific job family and the needs of the hiring division.

3. The Board will ensure that internal candidates who meet the minimum qualifications *and* who apply during the first 5 business days of the posting

process have an opportunity to interview. Divisions may, at their discretion, extend this internal posting period to 10 days. The hiring manager, or his or her designee, will interview all internal applicants who meet the minimum qualifications for the position and who apply during the initial 5- or 10-day internal posting period. (These interviews may precede, coincide, or follow external interviews.)

4. HR will forward to the hiring manager the applications of all internal candidates who meet the minimum qualifications and who apply for the position *after* the initial 5- or 10-day posting period, as well as the applications of qualified external candidates. The hiring manager will decide which candidates to interview from among the internal candidates who applied after the posting period and the external candidates and schedule interviews accordingly.

5. Posting a position externally does not prevent an internal candidate from being selected for the position.

6. Hiring managers will complete a candidate evaluation form for all internal applicants who are interviewed but not selected for a position.

Return to top

Responsibility

The Management Division is responsible for the administration of this policy and will review and update the policy as necessary. Exceptions to this policy can be approved by the HR officer for Talent Acquisition. The Board reserves the right to amend this policy at any time.

Return to top

Footnotes

1. *Vacant position* means an existing, funded, unoccupied position that a division seeks to fill. Return to text.

inside the board

Board Policies

Reasonable Accommodation

Approved by Don Hammond, effective October 21, 2013

Jump to section: Policy Statement

Policy Statement

The Board complies with the reasonable-accommodation requirements of the Rehabilitation Act of 1973, the federal government's equivalent of the Americans with Disabilities Act, as well as the Board's Rules Regarding Equal Opportunity (12 CFR § 268). Accordingly, this policy establishes the procedures for providing (1) qualified individuals with disabilities reasonable accommodations to enable them to perform the essential functions of their jobs, (2) employees with disabilities reasonable accommodations to ensure they enjoy the equal benefits and privileges of employment, and (3) job applicants with disabilities reasonable accommodations to assist them in applying for jobs at the Board.

Return to top

Definitions

Disability. With respect to an individual, a disability is a physical or mental impairment that substantially limits one or more of such individual's "major life activities." Major life activities include activities such as walking, seeing, hearing, speaking, performing manual tasks, eating, sleeping, standing, lifting, bending, breathing, learning, reading, concentrating, thinking, communicating, and working, as well as the operation of major bodily functions such as functions of the immune system, normal cell growth, and digestive, bowel, bladder, neurological, brain, respiratory, circulatory, endocrine, and reproductive functions. An impairment that is episodic or in remission may constitute a disability if it would substantially limit a major life activity when active.

Equal benefits and privileges of employment. Those benefits, such as cafeteria service, fitness center access, or employee benefit plans, that are available (under the conditions and limitations established by the Board) to the Board's similarly situated employees without disabilities.

Essential functions. Those job duties that are so fundamental to the position that the individual holds or desires that he or she cannot do the job without performing them. A function can be *essential* if, among other things, the position exists specifically to perform that function, there are a limited number of other employees who could perform the function, or the function is specialized and the individual is hired based on his or her ability to perform it. Determination of the essential functions of a position must be evaluated on a case-by-case basis so that it reflects the job as actually performed and not simply the components of a generic position description.

Genetic information. This means genetic information as defined by the Genetic Information Nondiscrimination Act of 2008 (GINA) and includes such information as an employee's or family member's genetic tests; an employee's family medical history (or manifestation of a disease or disorder in a family member); an employee's or family member's request for genetic services (as defined by GINA); an employee's or family member's participation in clinical research that includes genetic services; or genetic information of a fetus carried by an employee or an employee's family member or an embryo lawfully held by an employee or family member receiving assistive reproductive services. Genetic information does not include information about the sex, age, race, or ethnicity of an employee or family member.

Qualified. An individual with a disability, as defined in 12 CFR 268, is qualified for a position if (1) he or she satisfies the requisite skill, experience, education, and other job-related requirements of the position and (2) he or she can perform the essential functions of the position, with or without reasonable accommodation.

Reasonable accommodation. Any change in the work environment or in the way things are customarily done that would not create an undue hardship for the Board and would enable (1) a qualified individual with a disability to perform the essential functions of his or her job, (2) an employee with a disability to enjoy the equal benefits

and privileges of employment, and/or (3) an individual with a disability to apply for a job at the Board.

Undue hardship. If a specific type of accommodation causes significant difficulty or expense, then the Board does not have to provide that particular accommodation. Determination of undue hardship is always made on a case-by-case basis, considering factors that include the nature and cost of the accommodation needed and the impact of the accommodation on the operations of the Board.

Return to top

Requesting Accommodations Generally

An employee can request either an informal accommodation or a formal reasonable accommodation, but only a request for a formal reasonable accommodation gives rise to the rights and obligations under the Rehabilitation Act. An informal accommodation is an accommodation the Board may make in the ordinary course of its business, such as an ergonomic equipment adjustment, whether or not the employee is disabled under the Rehabilitation Act. A formal reasonable accommodation is an accommodation the Board would make as a result of its legal obligation to provide reasonable accommodations to qualified individuals with disabilities under the Rehabilitation Act.

An employee does not need to use special words, such as "reasonable accommodation," "disability," or "Rehabilitation Act," when requesting an informal accommodation or formal reasonable accommodation. However, in order for the Board to know whether an employee is making an informal request versus a formal request for a reasonable accommodation under the Rehabilitation Act, the employee must state in the request whether the accommodation is due to a medical condition. If the employee does not state that the accommodation is due to a medical condition, the Board will assume the employee is making an informal accommodation request. Informal accommodation requests do not receive the same procedural protections as formal reasonable accommodation requests under the Rehabilitation Act.

Return to top

Informal Accommodation Requests

The Board has an informal policy of making minor changes in office furniture and equipment (such as computers) and other similar adjustments to increase the comfort of employees who may not necessarily suffer from a disability or other medical condition.[1]

As noted above, informal accommodation requests will not receive the same procedural protections and considerations as formal reasonable accommodation requests under the Rehabilitation Act. Informal accommodation requests, which, in most cases, require no showing of medical necessity but do require a reason for the request, should be submitted to the employee's division administrator. The division administrator, in consultation with the division director, will decide whether to approve an informal accommodation request.[2]

Return to top

Formal Reasonable-Accommodation Requests

Timing and Content of the Request

Timing. Individuals may request formal reasonable accommodations, orally or in writing, whenever they choose, even if they have not previously disclosed the existence of a disability.

Content. As noted above, a request for a reasonable accommodation need not use special words, such as "reasonable accommodation," "disability," or "Rehabilitation Act." However, the employee must state in his or her request that the request is due to a medical condition if the employee would like for the request to receive the procedural and other protections afforded under the Rehabilitation Act and this policy.

Information Reporting Form for Reasonable-Accommodation Requests

The Board employee who receives the request for accommodation under the Rehabilitation Act must fill out the applicable portions of the Reasonable-Accommodation Information Reporting Form (the reporting form) and forward it to Employee Life, Human Resources (HR) Function, Management Division. The employee filling out the form may obtain assistance from the requester, but should in any event submit the form to Employee Life no more than five business days after the request was made. If additional information is needed to complete the form, the Employee Life staff member who receives the request will contact the requester to obtain the information and/or note why the missing information could not be obtained.

How to Submit a Request for a Reasonable Accommodation

Employees. Employees seeking a reasonable accommodation must request an accommodation from one of the following: (1) their immediate supervisor, (2) their second-level manager, (3) their division director, (4) the Office of Diversity and Inclusion, or (5) Employee Life.

Job applicants. A job applicant seeking a reasonable accommodation to apply for a job must request an accommodation from one of the following: (1) a recruiting specialist; (2) the Talent Acquisition Office, HR; (3) the Office of Diversity and Inclusion; (4) the manager in charge of the particular vacancy; or (5) a Board representative with whom the applicant has had substantial contact during the job-application process--for example, an interviewer.

Representatives of employees or applicants. An individual representing an employee or applicant, such as a family member, attorney, or health professional, may request a reasonable accommodation on the employee's or applicant's behalf. The request must follow the processes outlined above depending upon for whom (employee or applicant) the accommodation is requested. Board staff, where possible, should confirm with the employee or applicant that he or she, in fact, desires the requested accommodation.

Return to top

Processing Requests

Medical Information

Unless a disability and/or need for accommodation is obvious or already known, appropriate medical information will be needed, after a request is made, to make a determination on the employee's request for an accommodation. A disability is considered *obvious* if it is apparent to all observers that it substantially limits one or more of the requester's major life activities and there is no need for detailed medical documentation explaining the condition. For example, an employee's total blindness should be obvious and there would be no need to submit medical documentation to establish that a disability exists and that it substantially limits a major life activity. In addition, assuming the accommodation requested is designed to assist with blindness generally, there would be no need for the employee to submit medical documentation to support the need for the accommodation.

In all other cases, the extent and type of information required will vary depending on the nature of the disability and the accommodation requested. However, the Board will need to know the following information to make a determination under this policy: (1) the nature of the medical problem at issue; (2) the major life activity or activities that are substantially limited and how they are substantially limited; (3) the actual or expected duration of the medical problem; and (4) how the requested accommodation will address the individual's limitations and assist the individual in performing the essential functions of his or her job, enjoying equal benefits and privileges of employment, or applying for a job.

The Board has the right to request relevant supplemental medical information if the information submitted does not clearly explain and address all issues outlined above. The individual will be given a reasonable period to submit any necessary documentation. The Board has the right to have a medical expert of its choosing (and at its expense) review any medical documentation submitted. Failure to provide requested medical information may result in a denial of the request for an accommodation.

Under limited circumstances, the Board may require an individual requesting an accommodation to undergo a medical examination. If the individual has provided insufficient documentation from his or her health-care professional to substantiate the disability and/or need for the accommodation, the Board will explain why the documentation is insufficient and allow the individual an opportunity to provide the missing information in a timely manner. If, after an opportunity to submit additional information, the medical documentation is still insufficient, the Board may require the individual to be examined by a health-care professional of the Board's choice to substantiate the disability and/or need for the accommodation in order to continue to process the request for a reasonable accommodation.

Documentation is insufficient if, for example, (1) it does not establish the existence of a disability and explain the need for the reasonable accommodation requested, (2) it is from a health-care professional who does not have the expertise to give an opinion about the medical condition and the limitations imposed by it, (3) the information does not specify the functional limitations due to the disability, or (4) other factors indicate that the information provided is not credible or may be fraudulent. If the individual fails to provide sufficient documentation and refuses to be examined by a health-care professional of the Board's choice and at the Board's expense, the Board does not have to provide a reasonable accommodation until sufficient documentation is provided.

The scope of any medical examination must be limited to determining the existence of a disability and the functional limitations that require a reasonable accommodation.

Genetic Information Nondiscrimination Act of 2008

GINA prohibits employers from requesting or requiring genetic information of an individual, except as specifically allowed by this law. In accordance with GINA, when the Board requests medical information or conducts medical examinations, the Board will not seek to collect genetic information, and it will inform employees and health care providers responding to Board inquiries or working on the Board's behalf not to share genetic information with the Board.

Time Frame for Responding to a Request

The time limit for responding to a request for accommodation begins when the oral or written request is received by the appropriate Board representative as outlined above. Unless extenuating circumstances are involved, the chief human capital officer (CHCO) will respond to the request no later than 30 days after the request for accommodation was received. However, if the Board requests medical or other information, the period for responding will be extended by the number of days that the Board waited for a response to its request. If extenuating circumstances exist and the 30-day period must be extended, the CHCO will notify the individual of the delay, state the reason (or reasons) for the delay, and inform the individual of the date on which a decision is expected to be made. The Board will make reasonable accommodations prior to the expiration of the 30-day period if circumstances permit such expedited action. In addition, the period for processing a request may be expedited if, for example, the accommodation is needed to enable an individual to apply for a job or attend a Board activity that is scheduled to occur prior to the end of the 30-day processing period.

Interactive Process

Where the existence of a disability, the need for accommodation, or the specific requested accommodation is not clear, or when the Board believes the requested accommodation is not reasonable or that another reasonable accommodation exists, Employee Life must, with the assistance of any other relevant parties, discuss the requested accommodation with the requester to determine whether a mutually acceptable, effective reasonable accommodation exists. A requester should cooperate with these efforts to the extent possible, as failing to do so may result in the denial of the request for reasonable accommodation.

Return to top

Decisionmaking Process

Requests Involving Job Performance

The Board representative (or representatives) who receives an accommodation request involving job performance should advise Employee Life of the request by forwarding part I of the reporting form to Employee Life no later than five days after receipt of the request. Employee Life will promptly work with the employing division, as appropriate, to respond to the request. Absent extenuating circumstances, the CHCO will make a final determination as to how to respond to the request within 30 days of the date on which the Board received the request.

Requests by Job Applicants

The Board representative (or representatives) who receives a request for accommodation by a job applicant should advise Employee Life of the request by forwarding part I of the reporting form to Employee Life no later than five days after receipt of the request. Employee Life will promptly work with the manager in charge of the vacancy and other divisions, as appropriate, to resolve the request. Absent extenuating circumstances, the CHCO will make a final determination as to how to respond to the request within 30 days of the date on which the Board received the request.

Requests Involving Equal Benefits and Privileges of Employment

The Board representative (or representatives) who receives an accommodation request involving equal benefits and privileges of employment should advise Employee Life of the request by forwarding part I of the reporting form to Employee Life no later than five days after receipt of the request. Employee Life will promptly work with the other divisions, as appropriate, to resolve the request. Absent extenuating circumstances, the CHCO will make a final determination as to how to respond to the request within 30 days of the date on which the Board received the request.

Return to top

Types of Accommodations

The Board will consider a range of possible reasonable accommodations. The Board retains discretion to choose among any reasonable accommodation options that address the employee's disability, and is not required to provide the reasonable accommodation favored by the requester. Reassignment will be considered as a reasonable accommodation if the Board determines that no other reasonable

accommodation will permit the employee with a disability to perform the essential functions of his or her current position or if the only effective accommodation would cause undue hardship. In considering whether there are positions available for reassignment, Employee Life will work with the individual requesting the accommodation to identify (1) all vacant positions within the agency for which the employee may be qualified, with or without reasonable accommodation, and (2) all positions that HR knows will become vacant within a reasonable amount of time and for which the employee may be qualified. For example, if HR knows that a position for which the individual is qualified will become vacant in a week, that position should be considered for reassignment. Employee Life will first focus on positions that are equivalent to the employee's current job in terms of pay, status, and other relevant factors. If there is no vacant equivalent position, Employee Life will consider vacant lower-level positions for which the employee is qualified. If the Board is considering reassignment as an accommodation, the Board may consult with the affected employee as necessary to determine whether there are limitations on the search the employee would like the Board to conduct.

Return to top

Granted Requests

If the request for accommodation is granted, the accommodation will be provided at the same time as the response on the request for accommodation is given to the employee. If the accommodation will take longer to provide, the employee will be informed and told when the accommodation will be provided. Management's decision to provide a requested accommodation does not constitute an admission by the Board that the individual is disabled under the Rehabilitation Act.

Return to top

Denied Requests

A denial of a request for accommodation shall be in writing and shall identify the requester, the individual who made the decision, the specific accommodation requested, and the specific reasons for denying the request. Where the decision maker has denied a specific requested accommodation but offered a different one in its place (which was not agreed to during the interactive process), the denial notice should explain both the reasons for the denial of the requested accommodation and the reasons why the decision maker believes the offered accommodation will be effective. (If a requester agrees to an alternative accommodation during the interactive process, the request for accommodation will be deemed granted.) The written notice of denial must inform the individual of the right to initiate the EEO process under the Board's rules, by contacting an EEO counselor within 45 days of the denial of the request. The denial notice must also identify procedures that are available for informal dispute resolution.

Return to top

Appeal and Informal Dispute Resolution

If an individual wishes to appeal HR's decision, the individual must appeal to the director of the Management Division within 10 days of the date of HR's decision. Individuals may present additional information to support their request. The director will issue a decision on the appeal within 10 days unless extenuating circumstances exist. In addition, an individual who wishes to request informal dispute resolution should contact employee relations, which will arrange such dispute resolution.[3] The individual must request informal dispute resolution within 10 days of HR's decision or, if that decision is appealed, within 10 days of the director's decision on appeal. An appeal or a request for informal dispute resolution stays the time for an employee to initiate the EEO process by contacting an EEO counselor. Once a decision on the appeal is issued, or informal dispute resolution is closed by the Board or the employee, or a decision is made and communicated to the employee that informal dispute resolution is not appropriate, the period to request EEO counseling begins for the employee who chooses to use that process.

Return to top

Confidentiality

Under the Rehabilitation Act and GINA, medical information and genetic information obtained in connection with the reasonable-accommodation process must be kept confidential. This means that all medical information, including information about functional limitations and reasonable-accommodation needs, that the Board obtains in connection with a request for reasonable accommodation must be kept in files separate from the individual's personnel file. It also means that any Board employee who obtains or receives such information is bound by these confidentiality requirements. In addition, all records will be maintained in accordance with the Privacy Act. In certain circumstances, medical information may have to be disclosed to those individuals with a need for the information. For example, information may be disclosed to

- a supervisor and manager who needs to be told about necessary restrictions on the work or duties of the employee and/or necessary accommodations;
- first aid and safety personnel if the disability might require emergency medical treatment or assistance in vacating the employee's office in the event of an emergency;
- government officials, if necessary, to investigate the Board's compliance with applicable laws;
- individuals who need the information in connection with processing a reasonable-accommodation request, a workers' compensation claim, or other insurance benefit;
- the Board's attorneys, if necessary, to advise the Board on legal issues arising under this policy; and
- individuals named in a court order or other legal process, if such disclosure is required by a court order or legal process.

Return to top

Responsibility

The Management Division is responsible for administering this policy. The Management Division is solely responsible for maintaining all reporting forms, including information on the disposition of requests, and for reviewing information as necessary to ensure compliance with the Rehabilitation Act. This policy will be posted in all Board facilities and on the Board's internal website. Copies of this policy are available from HR. This policy is subject to change and will be reviewed and updated as necessary.

Return to top

Appendix A--Reasonable-Accommodation Information Reporting Form

Appendix B--Denial of Reasonable-Accommodation Request

Appendix C--Selected Reasonable-Accommodation Resources

1. U.S. Equal Employment Opportunity Commission (EEOC), 800-669-4000 (voice), 800-669-6820 (TTY), http://www.eeoc.gov

   The EEOC has many free documents on the title I employment provisions of the Americans with Disabilities Act (ADA), including both the statute, 42 USC 12101 et seq., and the regulations, 29 CFR 1630. In addition, the EEOC has published a great deal of basic information about reasonable accommodation and undue hardship. The three main sources of interpretive information are (1) the interpretive guidance accompanying the title I regulations (also known as the appendix to the regulations) (29 CFR 1630, appendix, and sections 1630.2(o) and (p) and 1630.9); (2) the *Enforcement Guidance on Reasonable Accommodation and Undue Hardship Under the Americans with Disabilities Act* (8 FEP Manual 405:7601 (1999)); and (3) *A Technical Assistance Manual on the Employment Provisions (Title I) of the Americans with Disabilities Act* (8 FEP Manual (BNA) 405:6981, 6998-7018 (1992) (the technical assistance manual)). The technical assistance manual includes a 200-page resource directory, including federal and state agencies, and disability organizations that can provide assistance in identifying and locating reasonable accommodations.

   The EEOC also has discussed issues involving reasonable accommodation in the following guidances and documents:

   - *Enforcement Guidance: Pre-Employment Disability-Related Questions and Medical Examinations* (5, 6-8, 20, 21-22, 8 FEP Manual (BNA) 405:7191, 7192-94, 7201 (1995))
   - *Enforcement Guidance: Workers' Compensation and the ADA* (15-20, 8 FEP Manual (BNA) 405:7391, 7398-7401 (1996))
   - *Enforcement Guidance: The Americans with Disabilities Act and Psychiatric Disabilities* (19-28, 8 FEP Manual (BNA) 405:7461, 7470-76 (1997))
   - Fact Sheet on the Family and Medical Leave Act, the Americans with Disabilities Act,Act, the Americans with Disabilities Act, and Title VII of the Civil Rights Act of 1964 (6-9, 8 FEP Manual (BNA) 405:7371, 7374-76 (1996))
   - *Enforcement Guidance: Disability-Related Inquiries and Medical Examinations of Employees Under the Americans with Disabilities Act* (20, 22, 23, 24-5, 8 FEP Manual (BNA) 405:7701, 7711, 7712-14, 7715-16 (2000))

   Finally, the EEOC has a poster that employers and labor unions may use to fulfill the ADA's posting requirement.

All of the above-listed documents, with the exception of the technical assistance manual and the poster, are also available through the Internet at www.eeoc.gov. All of these documents provide guidance that applies to federal agencies through the Rehabilitation Act of 1973 (29 USC 791).

2. Job Accommodation Network (JAN), 800-526-7234 (voice), 877-781-9403 (TTY), http://askjan.org

   A service of the President's Committee on Employment of People with Disabilities, JAN can provide information, free of charge, about many types of reasonable accommodations.

3. ADA Disability and Business Technical Assistance Centers (DBTACs), 800-949-4232 (voice/TTY), http://adata.org

   The DBTACs consist of 10 federally funded regional centers that provide information, training, and technical assistance on the ADA. Each center works with local business, disability, governmental, rehabilitation, and other professional networks to provide current ADA information and assistance, and places special emphasis on meeting the needs of small businesses. The DBTACs can make referrals to local sources of expertise in reasonable accommodations.

4. Registry of Interpreters for the Deaf, (703) 938-0030 (voice), (703) 939-0459 (TTY), http://www.rid.org

   The registry offers information on locating and using interpreters and transliteration services.

5. RESNA Technical Assistance Project, (703) 524-6686, http://www.resna.org

   RESNA, the Rehabilitation Engineering and Assistive Technology Society of North America, can refer individuals to projects in all 50 states and the six territories offering technical assistance on technology-related services for individuals with disabilities. Services may include --
   - information and referral centers to help determine what devices may assist a person with a disability (including access to large databases containing information on thousands of commercially available assistive technology products);
   - centers where individuals can try out devices and equipment;
   - assistance in obtaining funding for and repairing devices; and
   - equipment exchange and recycling programs.

Return to top

Footnotes

1. For example, an employee may be able to type more comfortably if he or she uses a certain type of keyboard tray. If practicable, the Board may provide the employee with the requested tray. Return to text.

2. Management's decision to provide an informal adjustment does not constitute a determination that the employee is disabled, as defined by the Rehabilitation Act, or that an adjustment or other type of accommodation is legally required. Return to text.

3. Informal dispute resolution can include mediation, team building, climate assessments, job coaching, etc. Return to text.

inside the board

Board Policies

Time Off in Connection with Administrative EEO Complaints

Approved by Stephen Malphrus, effective November 27, 2002

Jump to section:
Policy Statement

Policy Statement

Section 268.605 of the Board's Rules Regarding Equal Opportunity (12 CFR 268) provides that an individual bringing an equal employment opportunity (EEO) complaint (the complainant) against the Board is entitled to a representative of his or her choice during precomplaint counseling and at all stages of the complaint process. Both the complainant and the representative, if they are Board employees who are otherwise on duty and if the complaint is against the Board, are entitled to a reasonable amount of administrative leave (also called *official time*) to present the complaint and respond to Board requests for information (section 268.605(b)). Former employees of the Board who initiate the EEO process concerning claims relating to their prior employment are employees within the meaning of section 268.605, and their representatives, if they are current Board employees, are entitled to administrative leave.

Return to top

Guidelines

Generally, administrative leave is granted for the following purposes:

- *Meetings or hearings.* Complainants and their representatives are entitled to administrative leave for the duration of meetings or hearings with Board or Equal Employment Opportunity Commission (EEOC) officials.
- *Preparation for meetings or hearings.* Complainants and their representatives are to be given a *reasonable* amount of administrative leave to prepare for the meetings or hearings described in item 1.
- *Preparation of responses and documents.* Complainants and their representatives are to be given a reasonable amount of administrative leave to respond to Board and EEOC requests for information, to prepare the formal EEO complaint, and to prepare any appeals to the EEOC.

Reasonable Amount of Administrative Leave

As used in this policy, *reasonable amount of administrative leave* is defined as whatever is appropriate, under the particular circumstances of the complaint, to allow the complainant and the representative to make a complete presentation of relevant information associated with the complaint and to respond to Board requests for information. The actual number of hours to which a complainant and representative are entitled will vary, depending on the nature and complexity of the complaint and considering the mission of the Board and the Board's need to have its employees available to perform their normal duties on a regular basis. The complainant and the Board should mutually agree on the amount of administrative leave to be used before the complainant uses such time. Time spent commuting to and from home is not included in administrative-leave computations because all employees are required to commute to and from their Board employment on their own time.

Meeting and hearing time. For meetings or hearings (see item 1 above), *reasonable* is defined as the duration of the meeting or hearing. During the processing of a typical complaint, complainants and their representatives spend most of the time in meetings and hearings with Board officials or with EEOC administrative judges. Whatever time is spent in such meetings and hearings is automatically deemed reasonable. Both the complainant and the representative are to be granted official time for the duration of these meetings or hearings. If a complainant or representative has already worked a full week and must attend a meeting or hearing on a day when he or she would normally be off, that complainant or representative is entitled to administrative leave, which may require that the Board pay overtime in accordance with the applicable Board policy.

Preparation time. With respect to items 2 and 3 above, since presentation of a complaint involves preparation for meetings and hearings, as well as attendance at such meetings, conferences, and hearings, complainants and their representatives are also afforded a reasonable amount of administrative leave, as defined above, to prepare for meetings and hearings. In addition, the complainant and the representative are to be afforded a reasonable amount of administrative leave to prepare the formal complaint and any appeals that may be filed with the EEOC, even though no meetings or hearings are involved. However, because matters raised in a complaint will be investigated by investigators appointed by the Board or EEOC personnel, the regulation does not envision that the complainant and representative will need large amounts of administrative leave for preparation. Consequently, *reasonable*, with respect to preparation time (as opposed to time actually spent in meetings and hearings), is generally defined in terms of hours, not days, weeks, or months. Again, however, what is reasonable will depend on the individual circumstances of each complaint.

Aggregate Time Spent on EEO Matters by EEO Representatives

As a federal employer, the Board is entitled to expect its employees to spend most of their time doing the work for which they are employed. Therefore, the Board may restrict the overall hours of administrative leave afforded to a representative, for both preparation purposes and for attendance at meetings and hearings, to a certain percentage of that representative's duty hours in any given month, quarter, or year. These overall restrictions would depend on the nature of the representative's position, the relationship of that position to the Board's mission, and the degree of hardship imposed on the Board's mission by the representative's absence from his or her normal duties. The amount of time to be afforded to an employee for representational activities will vary with the circumstances.

Scheduling of Meetings

It is expected that the Board will, to the extent practical, schedule meetings during the complainant's normal working hours and that Board officials shall provide administrative leave for the complainant and the representatives to attend such meetings and hearings.

If meetings, conferences, and hearings must be scheduled outside of the complainant's or representative's normal work hours, the Board should adjust or rearrange the complainant's or representative's work schedule to coincide with the meetings or hearings, or grant administrative leave to allow an approximately equivalent time off during normal hours of work. In any individual circumstance, the Board has the discretion to select the appropriate method for making the complainant or representative available.

When a Board employee is called as a witness in connection with an EEO complaint, he or she must be in a paid-work status if his or her presence is authorized or required by EEOCor Board officials in connection with the complaint.

Return to top

Procedures for Requesting Administrative Leave

An employee seeking administrative leave in connection with an EEO complaint in the administrative process, whether he or she is an EEO complainant or a representative, must request such leave from the supervisor who is authorized to approve his or her other leave requests. Requests need to be made before the use of any administrative leave. The employee must provide sufficiently detailed information to permit the supervisor to determine what constitutes a *reasonable* amount of administrative leave. For example, if an employee is requesting administrative leave to attend a meeting or hearing, the employee must identify the entity who called the meeting (that is, the Board, an investigator, or an EEOC administrative judge) and provide an estimate of the duration of the meeting. The employee would then be entitled to administrative leave for the duration of the meeting or hearing. After the leave is granted, the supervisor should confirm the actual duration of the meeting or hearing and adjust the amount of administrative leave granted to reflect the actual duration of the meeting or hearing.

Similarly, if an employee is requesting administrative leave for preparation time, the employee must identify the reason the time is needed (for example, to prepare for a meeting or hearing with Board or EEOC officials, to respond to a Board or an EEOC information request, to prepare a formal complaint, or to prepare an appeal to the EEOC) and provide an estimate of the amount of preparation time required.

Supervisors who have questions about how much administrative leave should be granted in a specific instance should contact the Legal Division attorney (or attorneys) assigned to provide assistance with respect to questions on administrative leave for EEO purposes. The Legal Division attorney will consult with the EEO programs director and will work with the supervisor to advise him or her on what constitutes an appropriate amount of administrative leave in that specific instance.

Any reasons for the denial of official time should be fully documented and made part of the complaint file. If a supervisor denies a request for administrative leave, either

in whole or in part, he or she must prepare a written statement noting the reasons for the denial. The supervisor must immediately send the written statement to the EEO Programs Office for inclusion in the employee's EEO complaint file. If administrative leave is denied before a formal complaint is filed, the Board shall provide the complainant with a written explanation for the denial, which it will include in the complaint file if the complainant subsequently files a complaint.

Return to top

Annual Leave or Leave Without Pay in Connection with an EEO Complaint

If the employee believes that additional leave is required beyond any administrative leave that has been determined to be *reasonable* for the purposes set out above, the employee may use annual leave or leave without pay in accordance with the Board's policies.

Return to top

Leave for a Civil Action

Following the administrative process, an employee may file an EEO complaint in federal court as a lawsuit under title VII of the Civil Rights Act of 1964 (and related statutes). Once a complaint is no longer in the administrative EEO process, such as when the employee is preparing to file or has filed his or her EEO complaint as a lawsuit in federal court, this policy on administrative leave in connection with administrative EEO complaints no longer applies. There is no entitlement to administrative leave in connection with title VII litigation in a U.S. district court, a U.S. court of appeals, or before the U.S. Supreme Court. In those cases, Board policies governing annual leave or leave without pay are applicable. However, when an employee-litigant appears as a witness in a court case in which the government is a party, he or she is eligible for court leave for the time involved in giving testimony, as further described in the Board's Leave Policy.

Return to top

Applicability

This policy is issued pursuant to the Board's Rules RegardingEqual Opportunity and is consistent with guidance that is provided to federal agencies by the EEOC. In the case of a conflict between this policy and the Board's rules, the Board's rules shall apply.

Return to top

Reference

Leave Policy

Return to top

Responsibility

The EEO Programs Office, in consultation with the Legal Division, is responsible for administering this policy. This policy is subject to change and will be reviewed and updated as necessary.

Return to top

inside the board

EEO training begins October 27

Sheila Clark, Off ce of Divers ty and Inclusion

Published: October 27, 2014

In compliance with the training requirements of the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (NO FEAR Act), the Board is implementing web-based training beginning October 27. The training is designed to increase awareness and knowledge of equal opportunity federal laws and their application within the workplace.

The training consists of the following modules: discrimination-free workplace, workplace harassment, lawful hiring (managers), and disability discrimination and accommodation. Please allow ample time to complete the training; it takes about 1 to 1.5 hours to complete.

If you begin the training and then are unable to complete it in one sitting, you may exit at any time and resume from where you left off. At the end of each module, you must record your completion by clicking "**I Agree**" on the certificate screen. After doing so, print the certificate for your records.

Please note the following:

- Employees should complete the training in Firefox. If your default browser is Internet Explorer, you should cut and paste the link https://federalres.elt-inc.com into Firefox. If you attempt to access the training in IE, you will receive a certificate error message.
- The username for the training is **FR** combined with you **employee ID** (e.g., **FR000001**), and the password is **welcome** (lowercase).
- A notification will be sent to employees hired after September 30 to take the training at a later date.

All Board employees must complete the training by Friday, December 12.

If you have any questions regarding the training, please contact LaWanda Musgrove at 452-2083.

inside the board

Employee Relations

Jump to section: How To Find Us

Video: Allison Dichoso

The Board's Employee Relations (ER) function exists to maintain effective working relationships between employees and management. The ER staff takes a proactive approach, anticipating the impact of policy changes at the Board that will affect staff. The ER staff reinforces the employee/management relationship by providing assistance in three major areas

- counseling dispute resolution,
- policy assistance, and
- the facilitation of formal employee relations cases.

How to Find Us

Employee Relations is located at 1850 K Street in suite 3301

FRB Shuttle schedule

Return to top

What We Do

- Who We Are & What We Do (PDF)
- We identify emerging employee relations issues and trends that may affect employee morale; bring them to the attention of management in advance of any impact.
- We systematically gauge employee morale and assess the quality of Human Resources programs and services through various outreach mechanisms.
- We resolve workplace issues by providing consultation and counseling for management and employees.
- We develop and implement employee relations policies that are responsive to Board needs.
- We administer the grievance and disciplinary actions policies.

Return to top

Additional Employee Services

- Employee Assistance Program
- External Consultant Services (PDF)
- Mediation Guidelines (PDF)

Return to top

Articles

- Five Things You Didn't Know About Employee Relations, according to Allison Dichoso, Supervisor...

Return to top

Staff

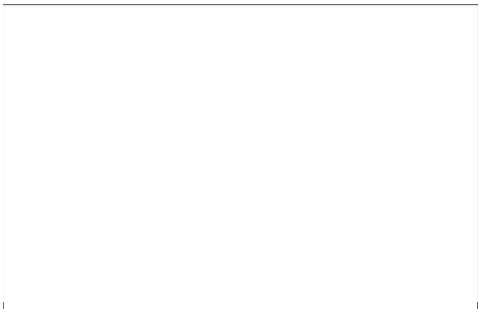
Click on the staff member's name to access contact information.

Name/Email	Title
Allison Dichoso	Employee Relations Supervisor
Keisha Hargo	Sr. Employee Relations Specialist
Kevin May	Sr. Employee Relations Specialist

Return to top

inside the board

Development and Learning



Introduction by Sioux Thompson

Our goal is to improve organizational performance and employee productivity at the Board.

Development and Learning Staff

Click on the staff member's name to access contact information

Contact	Title
Sioux Thompson	Manager
Ethel Bulluck	Learning and Development Supervisor
Annita Cox	Organizational Development and Training Specialist
Jamie Richards	Training Coordinator
Joi Randall	OD&L Intern
Stephanie Thompson-Brown	Sr. Training Specialist
Henry Vicks	Training Specialist

inside the board

Development and Learning

Assessments

Assessment tools are designed to increase employees' awareness of their behavioral tendencies in relation to how they interact with others. The tools can be used to help target training needs as well as help employees make good decisions.

Employee and Managerial Assessment Tools

- **Myers-Briggs (MBTI)** – Scores obtained from the Myers-Briggs Type Indicator (MBTI) indicate a person's individual mind patterns and learning process implications on each of eight polarities and four personality dimensions. This is helpful in the workplace, as the scores can provide insight into a person's working style.
- **NMap (New Manager Assimilation Process)** –The purpose of the New Manager Assimilation Process is to ramp up the integration of a newly appointed manager/leader with his or her direct reports. This process is a valuable step to ensure that a team quickly becomes productive after a management change.
- **DISC Profile** – This four-quadrant behavioral personality profile test is designed to help people gain insight into their behavioral style based on their personality and the situation they find themselves in. The DISC Profile can help build productive teams and develop effective management and leadership.
- **360-Degree Feedback** – A 360, or multi-rater, assessment gathers information from several different groups of people about an employee's effectiveness. A 360 assessment for managers might seek feedback from (1) the people that manager reports to, (2) peers, and (3) people who report to that manager.

inside the board

Development and Learning

Career Planning

We can help you understand the career planning process and help identify appropriate short- and long-term career options.

We start by identifying your interests along with any skill gaps. If there are any gaps, we can help you develop a plan and direct you to the tools necessary to be successful. Then we can help match your talents and skills with your interests. Ultimately, your increased knowledge and skills will add more value to the Board.

We provide the following:

- Skill and value assessments
- Individual career path development
- Job search guidance
- Résumé writing guidance
- Personal brand/marketing guidance
- Networking guidance
- Interview guidance
- Development plan guidance

inside the board

Development and Learning

Consulting

From organization-wide interventions to coaching work teams, our seasoned Organizational Development team can accurately diagnose and recommend the appropriate course of action.

Following is a sample of the types of interventions available:

- **Leadership development**: Expertise is shared in leadership assessment, training, coaching, and other development activities.
- **Process management**: We help create heightened awareness of work processes, which enables individuals and teams to think more systematically about how to improve them. It also helps teams learn the important skill of mapping work processes so that their improvement will increase the departments' effectiveness.
- **Learning solutions**: We provide creative solutions to your training needs, including traditional classroom instruction, facilitation, blended learning, and e-learning.
- **Strategic planning**: We help individuals and teams understand various strategic planning models and assist in implementing them. We assist with identifying the current state of the organization, envisioning the desired future, defining goals, developing action plans to meet goals, and monitoring progress.
- **Change management**: We help plan how change can occur, build a shared commitment to change, and implement needed changes.
- **Team development**: Team development can improve the diagnosis and problem-solving abilities of individuals and other work groups whose difficulties are teamwork-related.
- **Needs assessment design: surveys, evaluations, and focus groups**: The needs assessment process can provide vital information about your teams' services, employees, growth opportunities, and customer attitudes.

inside the board

Development and Learning

Training & Classes

We offer classroom, e-learning, blended learning, and virtual instruction within the Federal Reserve System—all a search away using FedLearn. Each division requires that you get approval from your manager before enrolling in training. This is to ensure that there are adequate resources in the office and that course fees (if applicable) have been approved.

Currently offered professional development courses

We can assist you with the following:

- Information about internal offerings and how they align with development and performance goals
- Referrals to external educational offerings or vendors for department, team, or individual-specific training or coaching needs
- Requests/suggestions you may have for new offerings
- Teambuilding
- Customized training/targeted training
- Writing classes
- e-learning options

What is FedLearn?

FedLearn is our enterprise learning management system. It is a web-based product that provides an infrastructure to manage and deliver training for Fed employees.

Review courses on FedLearn.

FEDLEARN

FedLearn classes and other resources for a successful PMP

View IT Training Opportunities

- Roving Training -- see the calendar for details
- IT Training

inside the board

Office of Diversity and Inclusion

Equal Employment Opportunity

Back to Equal Employment Opportunity

EEO Complaint Process and How It Works

Chairman's Letter

The Board's policy is to provide equal opportunity in employment for all persons. Thus, consistent with applicable law, the Board prohibits discrimination in employment on the basis of race, color, religion, sex, national origin, age, disability, or genetic information and promotes the full realization of equal employment opportunity (EEO) through a continuing affirmative program. In addition, as a matter of policy and although it is not required by law, the Board prohibits discrimination in employment on the basis of sexual orientation.

The Board is committed to complying with the following statutes and any amendments thereof: Civil Rights Act of 1964 (Title VII), section 501 of the Rehabilitation Act of 1973, the Age Discrimination in Employment Act of 1967, the Equal Pay Act of 1963, the Genetic Information Nondiscrimination Act of 2008, and the Uniformed Services Employment and Reemployment Rights Act of 1994. The Board's plan, program objectives, and goals dealing with equal employment opportunity are set forth in the Board's Rules Regarding Equal Opportunity, 12 CFR 268, and in the Annual EEO Program Status Report adopted by the Board. Both of these documents are available from the Board's Office of Diversity and Inclusion.

As an essential part of the Board's policy, no one will be subject to retaliation or reprisal for participating in any stage of the administrative or judicial proceedings provided for in the Board's Rules Regarding Equal Opportunity.
The Board has a zero-tolerance policy for discriminatory harassment, which includes sexual harassment. The Board is committed to preventing any discriminatory harassment.

The Board calls on senior management to comply fully with its policy of a work environment that is free from discrimination, hostility, intimidation, reprisal, and harassment. Each manager, at every level, must ensure that the Board's commitment to equality of opportunity is honored.

The following is an overview of the Board's EEO complaint process. For a comprehensive review of the Board's EEO program, employees and applicants for employment are encouraged to review the Board's Rules Regarding Equal Opportunity.

Sincerely,
Janet L. Yellen, Chair

Return to top

Equal Employment Opportunity (EEO) Designations

The Board designates members of its staff to help carry out the functions described in the Board's Rules Regarding Equal Opportunity.

EEO Counselors

Johanna C. Bruce, M-3304, ext. ext. 2787
Penny Thompson, M-3310, ext. 2077
Daniel Aranda, M-3303, ext. 3367

EEO counselors are available to counsel any Board employee or applicant who feels

that he or she has been discriminated against because of race, religion, color, national origin, sex, age, disability, genetic information, or sexual orientation, or has been subjected to retaliation for engaging in protected activity.

Return to top

Receipt of Complaints

The following individual is designated to receive formal complaints of discrimination:

Sheila Clark, Program Director

Office of Diversity and Inclusion
Board of Governors of the Federal Reserve System
Stop 156, Room M-3408
20th Street & Constitution Avenue, NW
Washington, DC 20551
Voice: (202) 452-2883

Return to top

Approaches to Solving Complaints

If you believe that you have been discriminated against because of your race, religion, color, national origin, sex, age, disability, genetic information, or sexual orientation, or have been subjected to retaliation for engaging in protected activity, you should contact an EEO counselor.

If you believe that you are a victim of discriminatory harassment, which includes sexual harassment, you may contact an EEO counselor. You may also seek relief by reporting such conduct through the established channels designated in the Board's Discriminatory Workplace Harassment Policy. In this regard, an employee may report discriminatory harassment to (1) the offending individual's supervisor or the harassed employee's supervisor; (2) the offending individual's division director or the harassed employee's division director; (3) the Office of Diversity and Inclusion program director, (4) an employee relations specialist in the Human Resources Function of the Management Division; (5) the officer responsible for Employee Relations, or his or her designee; (6) for employees in Human Resources, the assistant general for Human Resources in the Legal Division.

Return to top

The EEO Complaint Process

The following steps summarize the Board's EEO complaint process for employees and applicants who feel they have been discriminated against because of their race, religion, color, national origin, sex, age, disability, genetic information, or sexual orientation, or have been subjected to retaliation for engaging in protected activity. There are time limits for the filing and resolution of an EEO complaint. Failure of the employee or applicant to meet the time requirements stated for any stage of the complaint process may result in the dismissal of the complaint or the loss of administrative and judicial rights. These steps also apply to complaints of retaliation and equal pay (sex-based wage discrimination).

- You must contact an EEO counselor within 45 calendar days of the date of the matter alleged to be discriminatory or, in the case of a personnel action, within 45 calendar days of the effective date of the action.
- Unless you agree to an extension of time, the EEO counselor has 30 calendar days to inquire into your informal complaint, to attempt a resolution of the matter, and to advise you how to file a formal complaint if the matter is not resolved.
- In the event the Board's alternative dispute resolution process is offered to you and you agree to participate in mediation, the informal complaint processing period will be 90 days. Mediation will be offered on a case-by-case basis, when the program director deems a complaint appropriate for mediation.
- If the EEO counselor cannot resolve your complaint or if your complaint is in mediation and it is not resolved by the 90th day, the EEO counselor will issue you in writing a notice of your right to file a formal complaint with the Board. Should you choose to file a formal complaint, you must do so within 15 calendar days after your receipt of this notice.
- If you file a formal complaint, the Office of Diversity and Inclusion will review that complaint and determine the issues accepted for investigation. The Office of Diversity and Inclusion will then assign an EEO investigator to

investigate the issues accepted in your complaint.

- At the conclusion of the investigation, the program director will provide you with the investigative report.
- You will have 30 calendar days from receipt of the investigative report to request a hearing and a decision from an Equal Employment Opportunity Commission (EEOC) administrative judge or to request a final Board decision without a hearing.
- You may request a hearing before an EEOC administrative judge any time after 180 days have elapsed since the filing of your formal complaint.
- All requests for a hearing before an EEOC administrative judge must be made by submitting a written request to:

EEOC

131 M Street, NE – Fourth Floor, Suite 4NW02F
Washington, DC 20507

You are required to send a copy of your request for a hearing to:

Sheila Clark, Program Director

Office of Diversity and Inclusion
Stop 156, Room M-3408
20th Street & Constitution Avenue,
NW Washington, DC 20551

- If you request a final Board decision without a hearing, the Board will have 60 calendar days to render its final decision.
- If you request a hearing before an EEOC administrative judge, the EEOC will appoint an EEOC administrative judge to hold the hearing. The administrative judge will make findings of fact and conclusions of law and will issue a decision. The Board will have 40 calendar days from the date of its receipt of the administrative judge's decision to issue a final order informing you whether it will implement the decision. If the Board does not implement the administrative judge's decision, the Board can file an appeal with the EEOC simultaneously with the issuance of the Board's final order.
- As a complainant, you may appeal the Board's dismissal, or its final decision on your formal complaint, to the EEOC within 30 calendar days of your receipt of the Board's dismissal or final decision.
- As a complainant, you may file a civil action in U.S. district court within 90 calendar days of the Board's final decision or the EEOC's decision on appeal. In addition, you may file a civil action in U.S. district court after 180 calendar days have passed since the filing of your formal complaint or since the filing of your appeal with the EEOC.

Return to top

Important Points to Remember

- *You have the right to be represented at any stage in the presentation of your complaint by a person of your own choosing. This representative may be a Board employee and need not be an attorney. The Board does not, however, provide attorneys. The Board may determine to award attorney fees to a complainant—but only for the services of an attorney—when a finding of discrimination has been entered or when such an award is deemed appropriate under the applicable regulations. Attorney fees are not available for services performed at the administrative level for Age Discrimination in Employment Act (ADEA) or Equal Pay Act (EPA) complaints.*
- *Any person considering filing an EEO complaint must first meet with an EEO counselor within 45 days of the alleged discriminatory act.*
- *Copies of the Board's EEO rules and the Board's internal policy statements on EEO as well as further details on the EEO complaint process, including the Mediation Program for EEO Complaints, are available from the Office of Diversity and Inclusion.*
- *For a work-related problem in which you do not believe discrimination is a*

factor, you should first seek a resolution through your supervisor and other division management. If that effort fails, you may wish to contact an employee relations specialist in Human Resources.

- *If a complaint is determined to be appropriate for mediation, mediation can be offered (prior to the hearing) at both the informal and formal complaint processing stages.*

Return to top

Office of Diversity and Inclusion

You may contact any representative of the Office of Diversity and Inclusion in person, in writing, by e-mail, or by phone for advice or information on all aspects of equal employment opportunity.

Return to top

inside the board

Talent Acquisition

Jump to section: Getting Started

Video: Debra York

The Management Division's Talent Acquisition section assists divisions in attracting, selecting, and hiring a well-qualified and diverse workforce. Section staff recruits for full-time, temporary, worker trainee, intern, youth aids, and cooperative education positions.

Getting started

When you contact the Talent Acquisition section with a position need, the recruiter will arrange for a strategy session with you to discuss the qualifications you are looking for. Please consider the following when you have a position vacancy:

- Obtain a copy of an existing job description for the position from your division's administrative office and review it for accuracy. Your recruiter can help you develop language that can be used in the description and when posting the job internally and externally.
- All positions are posted internally for five business days. All internal job applicants who meet the minimum qualifications for a position must be interviewed by the hiring manager.

Return to top

Are You Hiring?

Peoplefluent is an applicant tracking system designed to manage the recruiting and hiring process through an external website. It assists with evaluating candidate qualifi cations, tracking new hires, and maintaining metrics. Click on the image to access PeopleClick job aid.

Return to top

Services

Sourcing. Talent Acquisition uses many sources to provide a diverse applicant pool. Our recruiters will help you find highly qualified applicants by posting on various job boards, such as Monster, DICE, LinkedIn, USAJOBS, and more. The staff also search for passive candidates by using these websites. (Passive candidates are those individuals who post profiles or resumes on websites, but who are not actively searching for new positions.)

Prescreening. Ensuring that job candidates have the right skills before coming in for a formal interview saves time. Talent Acquisition will work with hiring managers to develop a list of specific questions to identify or narrow a candidate's work experience and will contact candidates for writing samples or other materials.

Candidate coordination. Talent Acquisition will work with hiring managers to develop interview schedules and to arrange for travel assistance for candidates. The staff will also discuss benefits and salary with candidates and will mail information packets to all candidates who are offered positions.

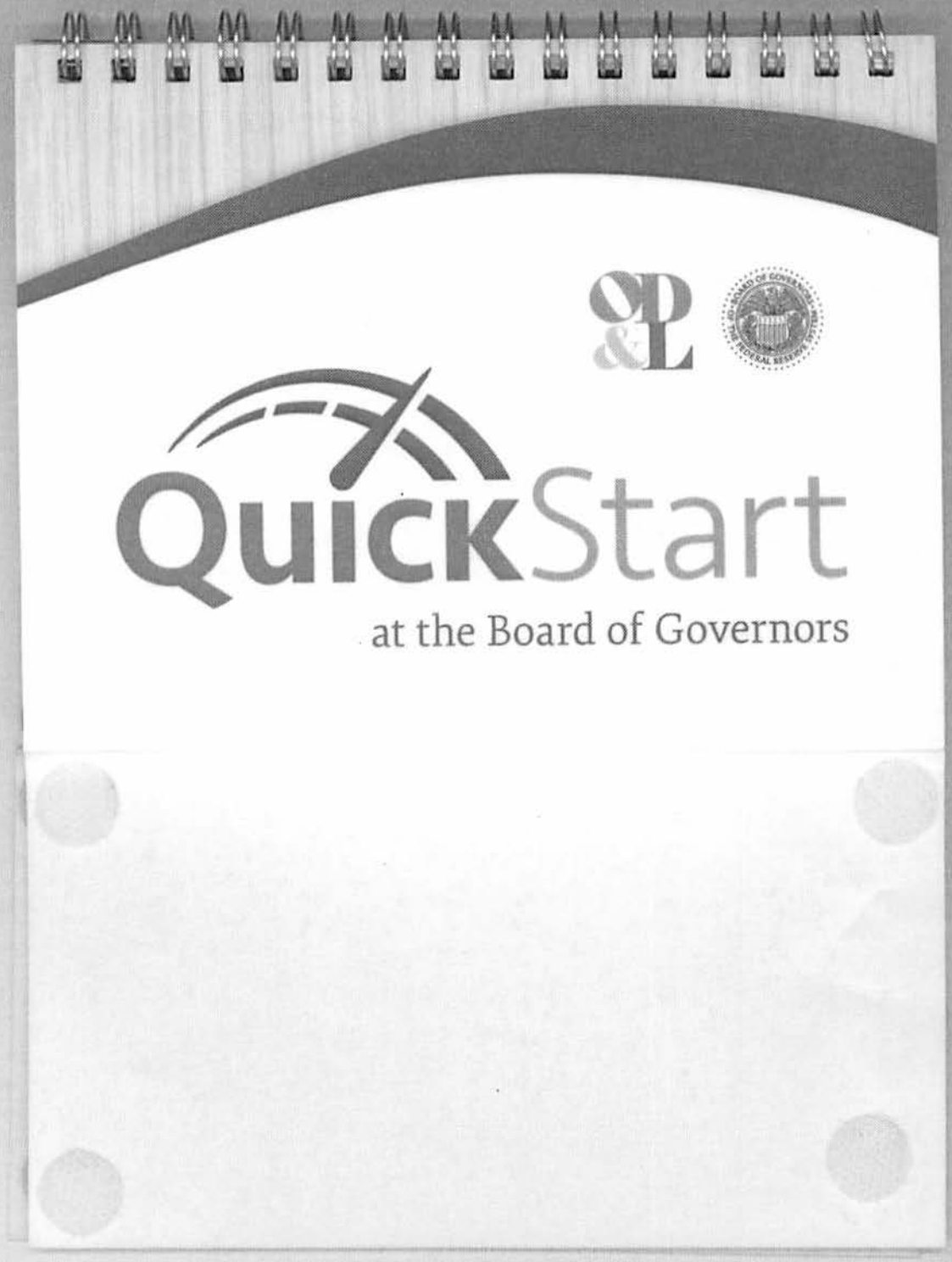
Process management. Recruiters in the Talent Acquisition section understand Board policies. No matter what type of employee you wish to hire, the staff will guide you through the process.

Return to top

Staff

Click on the staff member's name to access contact information.

Name	Title	Responsibilities
Debra York	Supervisor	Officer recruitment, FFIEC
Gioia Wallace	Sr. Recruiting Specialist (Lead)	R&S, OFS, MA, IF, DCCA
Terri Sawyer	Sr. Recruiting Specialist	RBOPS, Legal
Traci Leaphart	Sr. Recruiting Specialist	BDM, OSEC, OIG, Interns, Co-ops, Office Assistants
Yamah Tabibi	Recruiting Specialist	IT, College Outreach
Eileen Ajayi	Recruiting Specialist	BS&R, Temporary Employee (Agency)
Selena Taneja	Recruiting Specialist	MGT, DFM
Bruce Brumbaugh	Recruiting Specialist	COO, BSR, MGT
Fritz Leopold	Recruiting Specialist	BDM, OSEC, OIG, Interns,


QuickStart
at the Board of Governors

at the Board of Governors

QuickStart

01: Exploring Your Role as Manager

Six Roles of a Manager

QuickStart
for managers
at the Board of Governors

Results Master: Focuses on **delivery of outcomes**. The delivery of the "task," "product," or "services" through your team's efforts.

Connector: Aligns, connects, and translates to ensure a shared vision. Builds a robust network of peers and stakeholders, both internally and externally. Maintains productive relationships up, down, and across the organization.

Team Leader: Focuses on **team development** to achieve high performance; this role looks at how the team works together and sets an effective climate for team success.

Change Agent: Initiates and leads change in alignment with organization goals, objectives and initiatives.

Strategist: Takes in the broader view of the organization and external changes impacting the team; **orchestrates strategies** to ensure team's outcomes remain relevant and valuable. Sets the agenda to take actions required to be successful.

Coach: Supports **employees to grow and develop**. Enables employees to increase skills, capabilities and knowledge through developmental opportunities, experiences, and stretch projects.

Enablers and De-Railers

Approaches That *Enable* Success	Approaches That *De-Rail* Success
Engagement and enablement of staff in your section	Micromanagement through controlling and directive behaviors
Openness to and awareness of changing conditions and ability to respond adaptably	Resistance to change
Decision-making informed by timeliness and data required of the situation	Desire for and demand of perfection
Relationships that span across divisions and functions	Over-focus on section or individual results
Perspective that is balanced between strategic thinking and short-term reactive thinking	Focus on short-term priorities

QuickStart for managers at the Board of Governors

Connection – Connecting the work employees do to larger organization outcomes and success. Here is how:

1. Share the big picture.
2. Help employees find meaning and purpose in their work.
3. Support and celebrate progress.

Growth – Encouraging employees to develop their full potential and abilities. Here is how:

1. Know your employees.
2. Provide diverse development opportunities.
3. Use questions to develop employee insight.

Ownership – Fostering employee commitment and accountability for work outcomes and results. Here is how:

1. Empower employees through delegation.
2. Hold employees accountable.
3. Create opportunities for input and suggestions.

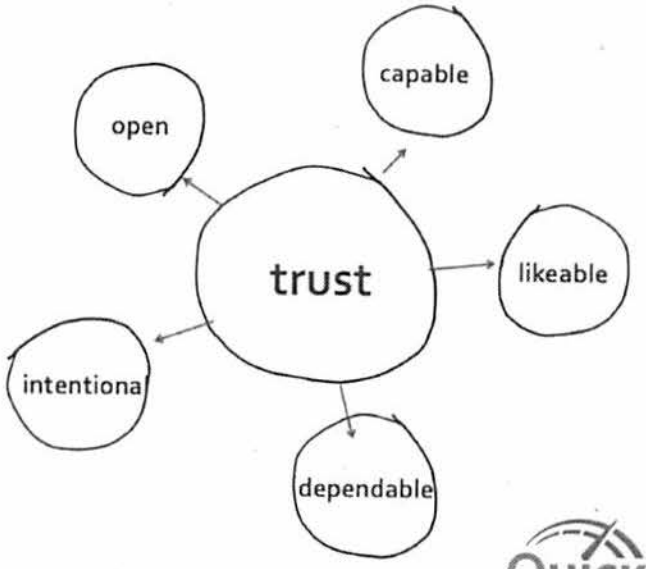
Trust – Increasing trust and openness so employees feel safe talking honestly about difficult issues. Here is how:

1. Develop supportive relationships with your employees.
2. Demonstrate openness to ideas of all team members.
3. Create fairness through consistency and dependability.

QuickStart for managers at the Board of Governors

02: Motivating and Engaging Others

Trust Model



QuickStart for managers at the Board of Governors

Trust, (n). One in which confidence is placed.

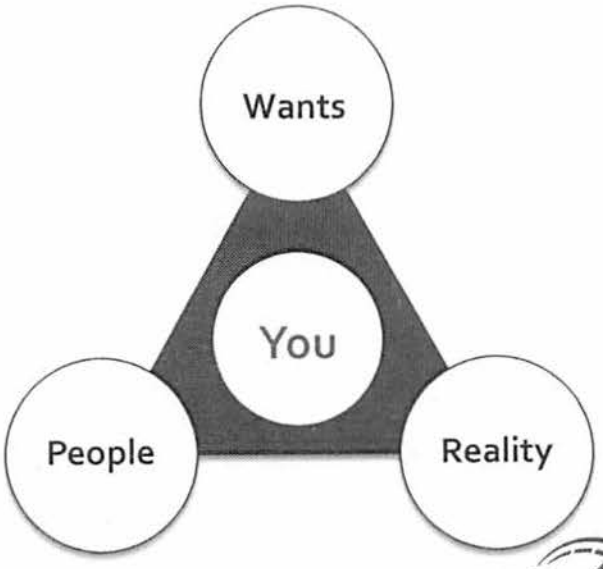
It is the underpinning of every effective relationship and is foundational to organization success. Yet, it is a hidden and an over looked element. Trust is built on one's personal character and competence.

Cultivate Trust

1. **Listen first:** Seek to understand.
2. **Give credit to team members:** Provide them opportunities to be recognized in wider arenas.
3. **Create transparency:** Be open and authentic.
4. **Confront reality:** Take issues head-on, even the 'un-discussable'.

QuickStart for managers at the Board of Governors

Triangle of Influence



Reference: Bellman (1992)

QuickStart for managers at the Board of Governors

WHAT: An influence approach to get things done within organizations by leveraging collective power, building shared understanding, and creating alignment on desired outcomes that are shared.

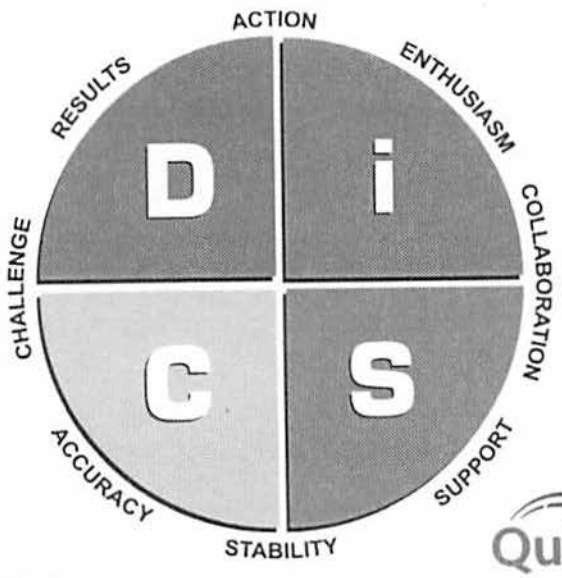
Three focus areas:

People – Who are the people involved in or that care about the situation?

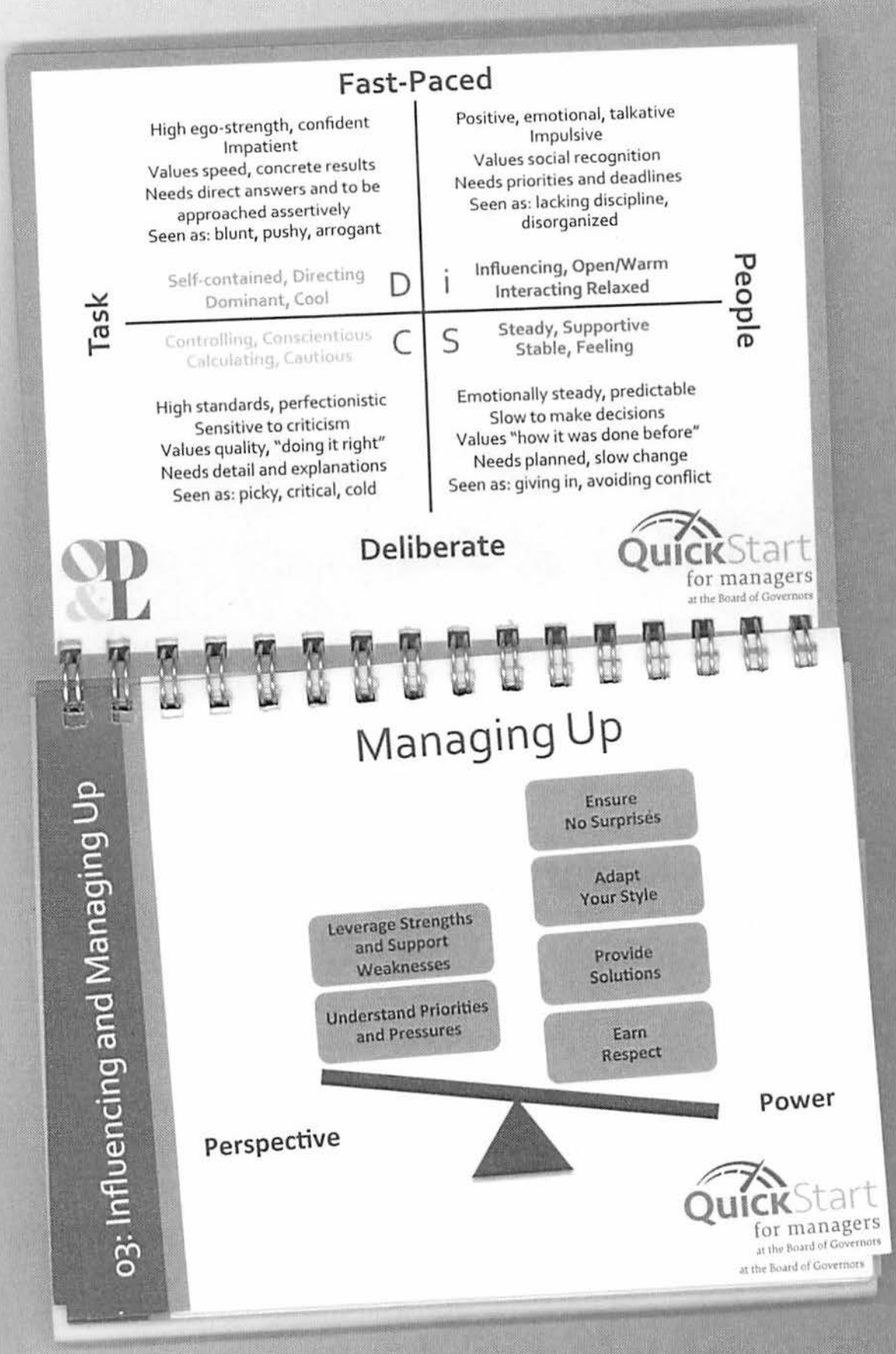
Reality – What is the current situation? How do you and others see the situation as it currently exists?

Wants – What is the preferred state? What do you and others want in the situation?

DiSC Model



Credit: DiscProfile.com
Reference: Marston (1928)


Fast-Paced
High ego-strength, confident
Impatient
Values speed, concrete results
Needs direct answers and to be approached assertively
Seen as: blunt, pushy, arrogant
Positive, emotional, talkative
Impulsive
Values social recognition
Needs priorities and deadlines
Seen as: lacking discipline, disorganized
Task
Self-contained, Directing
Dominant, Cool
D
i
Influencing, Open/Warm
Interacting Relaxed
People
Controlling, Conscientious
Calculating, Cautious
C
S
Steady, Supportive
Stable, Feeling
High standards, perfectionistic
Sensitive to criticism
Values quality, "doing it right"
Needs detail and explanations
Seen as: picky, critical, cold
Emotionally steady, predictable
Slow to make decisions
Values "how it was done before"
Needs planned, slow change
Seen as: giving in, avoiding conflict
Deliberate
QuickStart for managers
at the Board of Governors
03: Influencing and Managing Up
Managing Up
Ensure No Surprises
Adapt Your Style
Provide Solutions
Earn Respect
Leverage Strengths and Support Weaknesses
Understand Priorities and Pressures
Power
Perspective
QuickStart for managers
at the Board of Governors

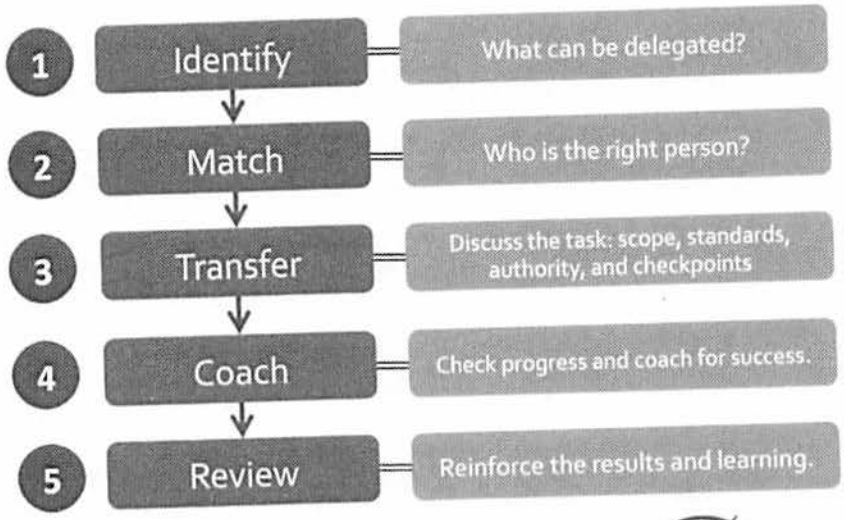
10 Principles to Managing Up

1. A productive relationship with your boss is a core determinant to your success.
2. Know your boss' DiSC Style. Adapt your style as necessary.
3. Do not compete with your boss. You will lose. Negotiate.
4. Always make your boss look good. Keep them well-informed to ensure a "no surprise" policy.
5. Trust is a two way street.
6. Know if your work is progressing your boss' priorities.
7. Under-promise and over-deliver.

QuickStart for managers at the Board of Governors

04: Managing for Results

The Five-Step Delegation Process



QuickStart for managers at the Board of Governors

1. Identify

- Can someone else do the task?
- Can doing the task develop an employee?
- How frequent is the task?
- Is there time to delegate?
- How critical is the task?

2. Match

- Who is interested?
- Who is capable and reliable?
- Who has the required skills?
- Who has the time?
- Who will grow from the task?
- Who are you overusing/overlooking?

3. Transfer

- What is expected?
- How will success be measured?
- What resources will be available?
- Clarify decision making authority.
- What checkpoints are expected?

4. Coach

- High Competence/High Commitment – **Empower**
- High Competence/Variable Commitment – **Support**
- Some Competence/Some Commitment – **Coach**
- Low Competence/High Commitment – **Direct**

5. Review Results

- Review results
- Celebrate successes
- Integrate learning

QuickStart for managers at the Board of Governors

Accountability Initiative Framework

Level 1:	Employee waits until told what to do
Level 2:	Employee asks you what to do
	Low to No Initiative
	Productive Initiative
Level 3:	Employee suggests what to do, and then moves with your approval
Level 4:	Employee decides what to do, and informs you right away
Level 5:	Employee does it and keeps you updated regularly

Reference: Oncken & Wass (1999)

QuickStart for managers at the Board of Governors

Avoid the Tendency to "Take Back Work"

Ensure employees know to:

1. Come with solutions
2. Have an agreed level of accountability to progress work

Authority	Control	Initiative
• Delegate enough authority to: • Keep work going • Allow employee initiative • Allow oversight/guidance to ensure success • Fuel of delegation	• Employee responsible for outcome • Employee responsible for the results of their actions • Consistent feedback mechanisms are necessary	• Allow: • Freedom for employees to do things their way • Managers focus on results not the process

QuickStart for managers at the Board of Governors

Defensive Triggers

Reference: Rock (2008)

QuickStart for managers at the Board of Governors

Principles for Dealing with Emotional Reactions

Remember:

1. The reaction is not about you.
2. Emotions can block the conversation.
3. Emotions can amplify if dismissed or avoided.
4. Enabling expression of emotions can diminish intensity.

Avoiding Defensive Triggers

Status - relative importance as compared to others. Provide growth opportunities; pay attention to employee improvement.

Certainty - the brain craves certainty so that prediction is possible. Provide clear expectations or ensure consistent decision making.

Autonomy - the perception of exerting control over one's environment. Provide options and opportunity for input.

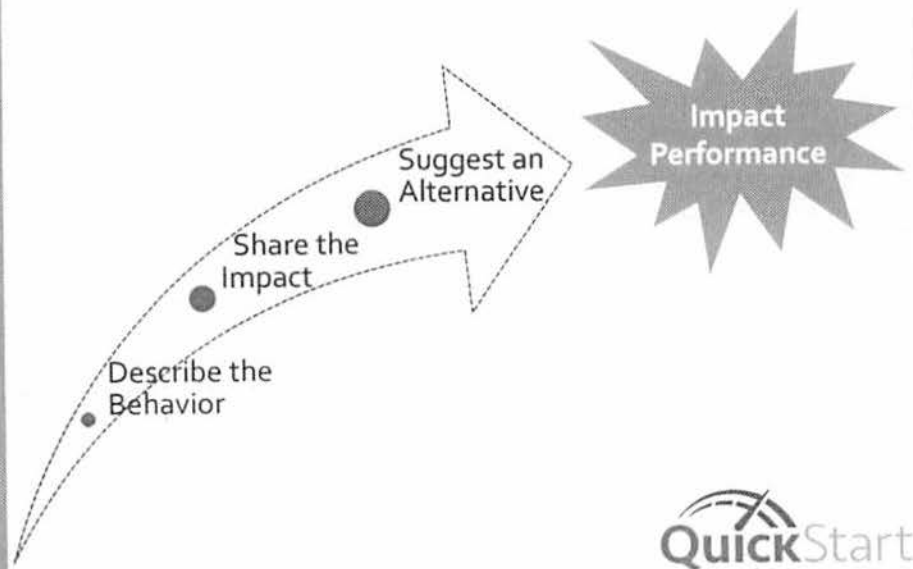
Relatedness - one's inclusion in groups and relationships. Create opportunity to connection with or mentor other employees.

Fairness - perceived equity. Increase transparency and communication.

QuickStart for managers at the Board of Governors

05: Providing High-Impact Feedback

Three-Step Feedback Approach



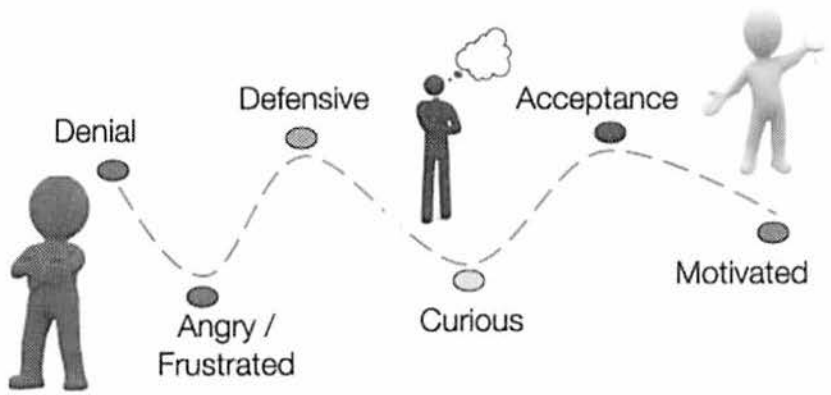
QuickStart for managers at the Board of Governors

What	Why	How
Describe the Behavior	Ensures the feedback is fact-based and non-judging De-personalizes the feedback	"When you..." Describe the behavior Be specific
Share the Impact	Increases their awareness of their impact Provides the reason why change is important	"I felt... confused, frustrated, disappointed" Impact for organization, team, or yourself
Suggest an Alternative	Allows choice of how they handle it in the future Demonstrates respect and provides autonomy	"Next time I suggest..." "Next time I'd prefer..." "How could you handle this differently in the future?"

QuickStart for managers at the Board of Governors

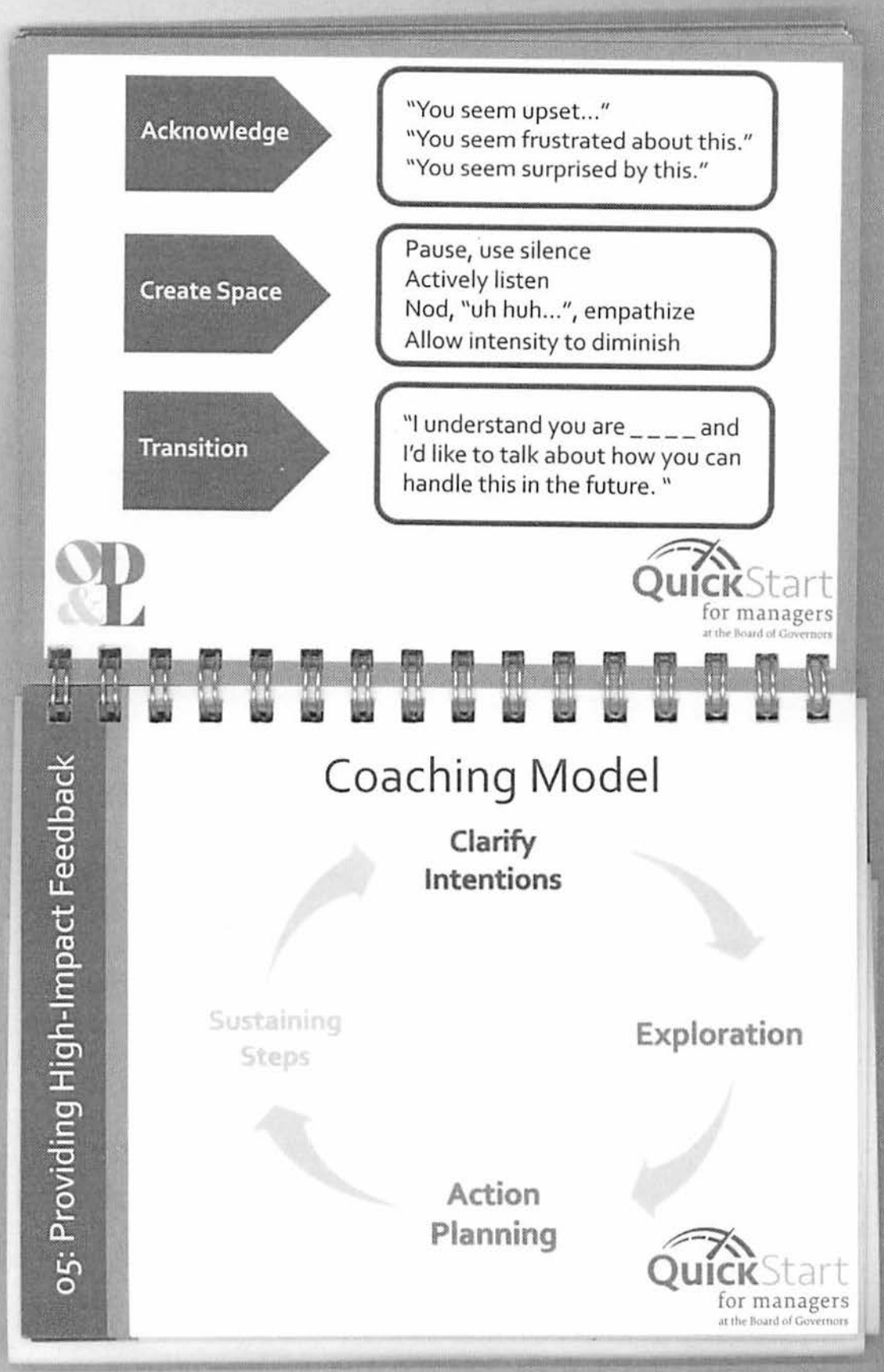
05: Providing High-Impact Feedback

ACT Model



Acknowledge Create Space Transition

QuickStart for managers at the Board of Governors


Acknowledge
"You seem upset..."
"You seem frustrated about this."
"You seem surprised by this."
Create Space
Pause, use silence
Actively listen
Nod, "uh huh...", empathize
Allow intensity to diminish
Transition
"I understand you are _ _ _ _ and I'd like to talk about how you can handle this in the future. "
QuickStart for managers at the Board of Governors
05: Providing High-Impact Feedback
Coaching Model
Clarify Intentions
Exploration
Action Planning
Sustaining Steps
QuickStart for managers at the Board of Governors

Clarify Intentions

- Build shared understanding
- Desired outcomes
- Why is this important

Exploration

- Identify what is working well
- Envision success
- Explore opportunities and options

Sustaining Steps

- Specific next steps or actions
- Success measures
- Support and follow-up

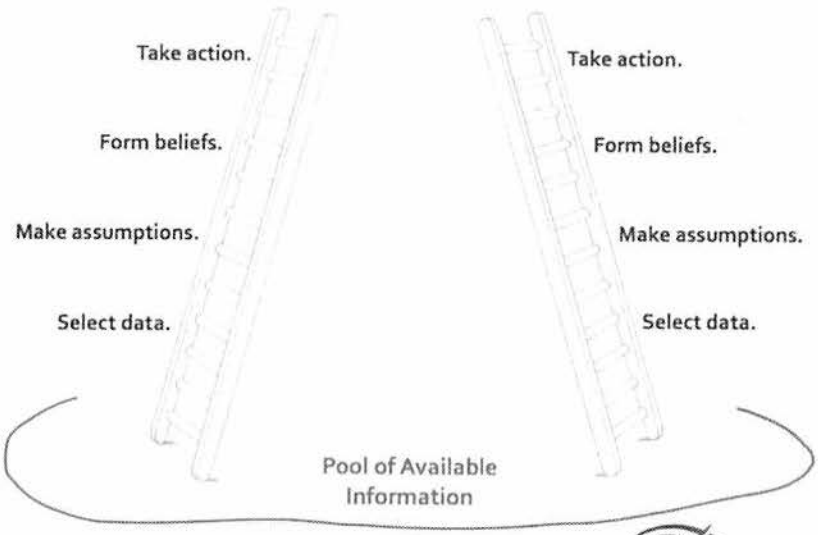
Action Planning

- What will you do differently
- How will you do it differently
- Support required

QuickStart for managers at the Board of Governors

06: Navigating Conflict

Ladder of Inference



Reference: Argyris (1990)

QuickStart for managers at the Board of Governors

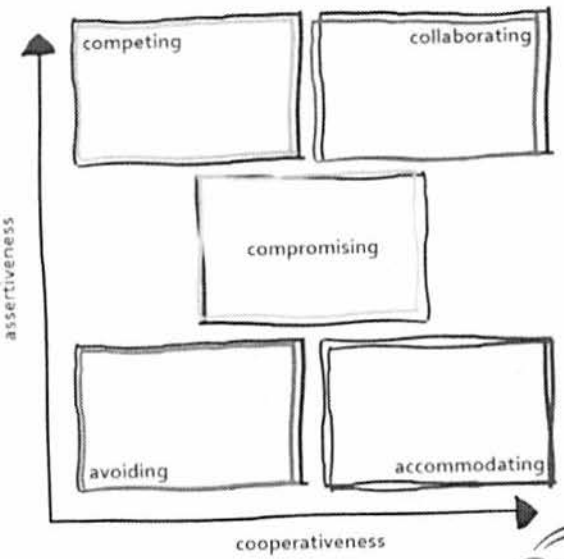
Climbing Down the Ladder (Reframing Beliefs)

1. **Stop.** Practice waiting before acting, especially when the urge to act arises.
2. **Reflect.** What beliefs have you formed about the person or situation? What information/data are using to support your beliefs?
3. **Investigate.** Inquire about others' beliefs and the data they used to form their beliefs.
4. **Advocate.** Express your beliefs and how you came to them.
5. **Reframe.** Use relevant data to reframe your beliefs, if necessary.
6. **Act.** Consider the consequences of your actions and proceed.

QuickStart for managers at the Board of Governors

06: Navigating Conflict

Five Conflict-Handling Modes



Reference: Thomas & Kilmann (1974)

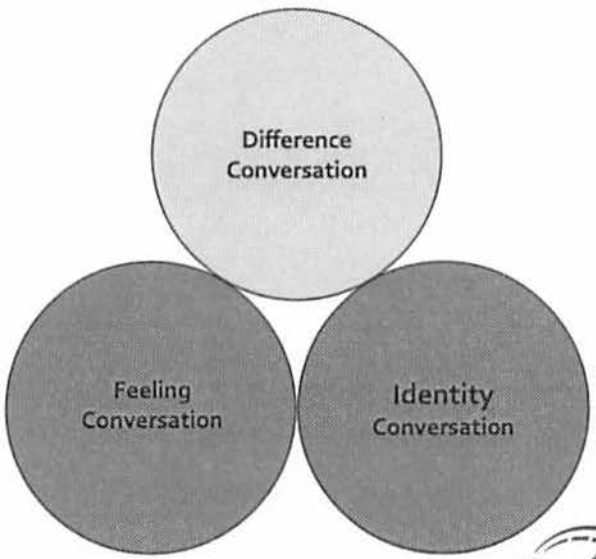
QuickStart for managers at the Board of Governors

Mode	Involves	Useful When
Competing	Asserting your opinions Standing your ground Stating your opinion clearly	Standing up for vital issues Taking quick action Protecting yourself
Accommodating	Forgoing your desires Selflessness Yielding	Goodwill & building relationships Keeping peace Providing customer service
Avoiding	Side-stepping Withdrawing Leaving	Reducing tensions Freeing time Allowing others ownership
Collaborating	Listening and empathizing Balanced advocacy and inquiry Identifying concerns & interests	Gaining commitment Integrating solutions Improving relationships
Compromising	Making concessions Negotiating Finding a middle ground	Resolving small issues Creating temporary solutions Dealing with time constraints

QuickStart for managers at the Board of Governors

06: Navigating Conflict

Difficult Conversations Model



QuickStart for managers at the Board of Governors

Keys to the Difference Conversation

1. Clearly state the assessment of performance
2. Give specific examples of behavior/performance
3. Understand the employee's view of their performance
4. Identify and clarify where the differences lie
5. Establish a plan for moving forward

Keys to the Feelings Conversation

1. Recognize that you can not control their reaction – do not try to
2. Listen to, empathize, and acknowledge their feelings
3. Summarize feelings and the desired outcome to minimize venting
4. Shift the conversation towards the future

Keys to the Identity Conversation

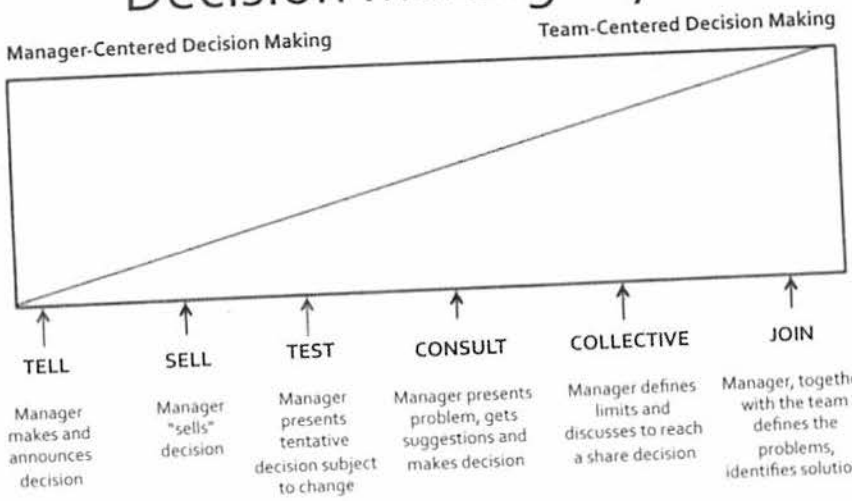
1. Measure success by how clearly and with how much care you speak
2. Separate your self-image from the employee's reaction
3. Help the employee understand the different perceptions
4. Share that you care and want to be helpful in moving forward

High-Performance Team Conditions

QuickStart for managers at the Board of Governors

Compelling Goals • Is there a common understanding of team purpose? • Is there high-level of commitment to this purpose?	**Effective Leadership** • Does the leader provide a vision of what needs to be accomplished and why it is important? • Does the leader obtain appropriate input on key decisions?
Clear Roles • Do individuals have a clear understanding of what is expected from them? • Do individuals understand how their role contributes to the team's success?	**Cooperative Relationships** • Do individuals feel supported in their roles? • Are individuals sensitive to both individual needs and the best interest of teams?
Enabling Principles • Does the team have a clear set of priorities? • Are action plans aligned in an effective manner?	**Mutual Accountability** • Are members committed to doing their best? • Do all members share in the responsibility to deliver?

Decision Making Styles



QuickStart for managers at the Board of Governors

Reference: Tannenbaum & Schmidt (1973)

Approach	Use when...
Tell	Time is limited and urgency is high You have already made the decision
Sell	You have largely made the decision but need to persuade others of your point of view
Test	You want to give the team an opportunity to check the logic of the decision and test it for flaws or gaps You have an idea of what to do, but only a small amount of time to get feedback from a few people (rather than the whole team)
Consult	You have ample time You want to solicit significant participation from team members
Collect	You are open the decision that the team reaches You want to ensure that everyone is involved in the decision process and has an equal say
Join	Manager defines the limits and allows the group to make a decision

References

Argyris, C. (2000). *Overcoming organizational defenses: Facilitating organizational learning*. New York: Prentice Hall.

Bellman G. (1992). *Getting things done when you are not in charge*. New York: Simond Schuster.

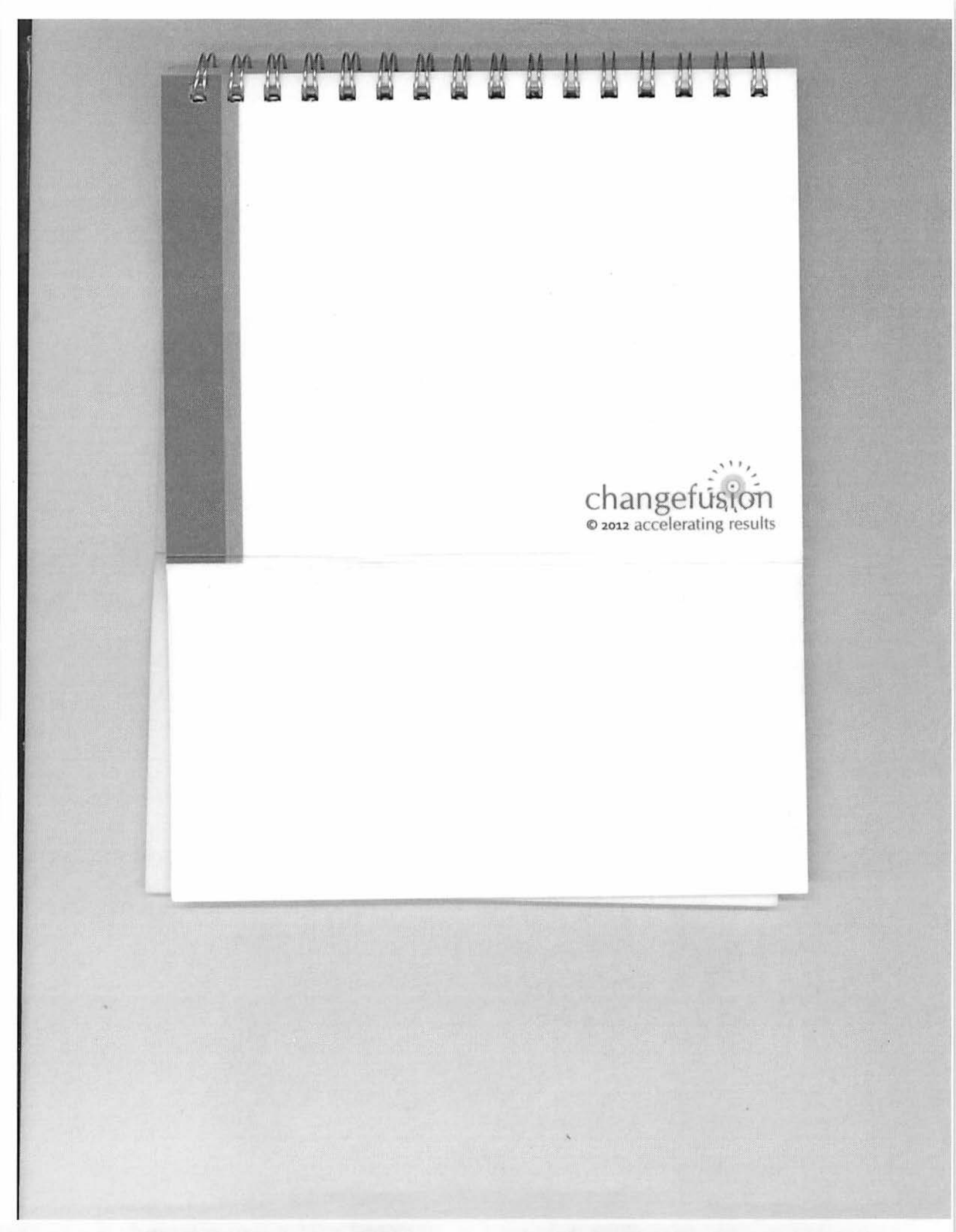
Marston, W.M. (1928). *Emotions of normal people*. Trubner & Co.

Oncken, W., & Wass, D. L. (1999). Management time: Who's got the monkey?. *Harvard Business Review*, 6.

Rock, D. (2008). SCARF: A brain-based model for collaborating with and influencing. *NeuroLeadership Journal*, 1-9.

Tannenbaum, R., & Schmidt W.H. (1973). How to choose a leadership pattern. *Harvard Business Review*, 3.

Thomas, K. W., & Kilmann, R. H. (1974). Thoman kilmann conflict mode instrument. New York: Xycom.


changefusion
© 2012 accelerating results

Management Division • Human Resources

New Employee

PRE-INFORMATION SHEET

Please complete the following information using a local address. This information must be captured in the employee database by 10:00am each Monday.

Hire Date: _____

Name: _____

Street Address: _____ Apt: _____

City: _____

State: _____ Zip Code: _____

Date of Birth: _____

New Employee Data

Board of Governors
of the Federal Reserve System

Personal Data

Name (last, first, initial) | Prefix (Mr., Mrs., Ms., Dr., etc.) | Social Security Number

Home Address/Phone

Address

City | County | State | ZIP | Country

Phone Number (include area code)

Mailing Address (if different from home address)

Address

City | County | State | ZIP | Country

Other Phone Numbers

Type | Number (include area code) | Type | Number (include area code)

Gender
☐ Male ☐ Female

Marital Status
☐ Married ☐ Divorced ☐ Separated ☐ Single ☐ Widowed

Marital Status Date

Birthdate | Birthplace

Citizenship Status
☐ Permanent Resident (Greencard)
☐ Alien Temporary (check one) ☐ H-1B ☐ J-1 ☐ F-1 ☐ Other _____
☐ U.S. Citizen (Native) (born in U.S. or a U.S. territory)
☐ U.S. Citizen (Naturalized) (Born outside the U.S.)

If not a U.S. citizen, list country of citizenship _____

Ethnic Group
☐ Asian ☐ Black ☐ Hispanic ☐ Native Amercian (specify group) _____ ☐ White ☐ Other

Military Status
☐ Active Reserve ☐ Inactive Reserve ☐ Disabled ☐ No Military Service ☐ Other Veteran ☐ Retired ☐ Vietnam Veteran

Education (attach transcript)

Degree | Graduated ☐ Yes ☐ No | Major | Year Earned or Expected

School | State | Country

Degree | Graduated ☐ Yes ☐ No | Major | Year Earned or Expected

School | State | Country

Degree | Graduated ☐ Yes ☐ No | Major | Year Earned or Expected

School | State | Country

Languages (other than English)

Language | Native ☐ Yes ☐ No | Able to Translate ☐ Yes ☐ No

Speaking Proficiency ☐ Low ☐ Moderate ☐ High | Reading Proficiency ☐ Low ☐ Moderate ☐ High | Writing Proficiency ☐ Low ☐ Moderate ☐ High

Language | Native ☐ Yes ☐ No | Able to Translate ☐ Yes ☐ No

Speaking Proficiency ☐ Low ☐ Moderate ☐ High | Reading Proficiency ☐ Low ☐ Moderate ☐ High | Writing Proficiency ☐ Low ☐ Moderate ☐ High

Relatives Employed at the Board

Name (last, first, initial) | Relationship to Employee

Name (last, first, initial) | Relationship to Employee

Name (last, first, initial) | Relationship to Employee

Primary Emergency Contact

Contact Name (last, first, initial) | Relationship to Employee

Home Address/Phone

Same address/phone as employee ☐ Yes ☐ No

Address Line 1

City | County | State | ZIP | Country

Home Phone (include area code) | Work Phone (include area code) | Other Phone (include area code) | Other Phone (type)

Secondary Emergency Contact

Contact Name (last, first, initial) | Relationship to Employee

Home Address/Phone

Same address/phone as employee ☐ Yes ☐ No

Address Line 1

City | County | State | ZIP | Country

Home Phone (include area code) | Work Phone (include area code) | Other Phone (include area code) | Other Phone (type)

Employment Data (HRM Use Only)

Company Seniority Date | Service Date | Date Last Increase | Business Title

Room No | Mail Stop | Work Phone

Original Hire Date | High School/GED Date

FRB initials (input) | Date | FRB initials (verification) | Date

Purpose: (b) (5)

Source: Board's ItB

Prepared By: Kimberly Perteet, SR Auditor

Reviewed by: Anna Saez, Manager

inside the board

3Cs Conversations
Contributions. Competencies. Capabilities

About the 3Cs Process

The 3Cs Conversations, our performance management process, is designed to align staff to the work of the Board, provide greater accountability, support the growth of our staff, improve the value of time everyone spends, and increase fairness of the process.

This process is not solely about new forms or steps in the process:

- It is about the partnership between manager and employee (manager is defined as anyone who supervises someone else - (e.g. officer, manager, chief, supervisor))
- It is about the conversations managers and employees have
- And, most importantly, it is about the approach to the conversations; an approach that increases focused action, encourages learning, and reduces defensive reactions for both managers and employees

The 3Cs Conversations Framework aligns and connects the Board's work. At the heart of this process are collaborative, forward-focused, ongoing, and two-way conversations between managers and employees about the work (**what** needs to be accomplished—the tasks and results—also known as contribution) and behaviors (**how** the work is approached and how one builds relationships along the way—also known as competencies).

The framework incorporates both formal conversations and informal, ongoing conversations. Taken together, all of these conversations are designed to support and direct employees' performance to achieve the Board's mission.

Characteristics of the conversation approach:

- **Collaborative** conversations are those conversations in which employees and managers jointly and cooperatively determine work, define performance, and create conditions for employee success.
- **Forward-focused** conversations use questions to focus on developing solutions for the future.
- **Ongoing** means there will be both formal, scheduled conversations and spontaneous, ad-hoc conversations. The ongoing nature of the conversations will ensure continual adjustment and support and adaptation of expectations as work expectations change.
- **Two-way** conversations means that both the manager and the employee are active, engaged participants in the conversation.)

What are the core changes to performance management for year 2014-2015?

There are changes to the overall standardized process, the objective setting approach, Board- wide competencies, and the definition of performance.

Below, these core changes are explained in greater detail.

1. Overall standardized process: We will operationalize a Board standard conversation approach to performance management. Specifically, this means we will:

- Introduce a set of foundational conversations, the 3Cs Conversations.
- Adopt a conversation approach that is collaborative, ongoing, two-way, forward-focused, and generative.
- Clarify role expectations of managers at the Board. This dual role combines technical expertise and managerial expertise, the ability to engage employees in contributing their best ability.
- Provide a toolkit for managers on how to improve performance via short ongoing conversations.
- Implement a new semi-automated form.

2. Objective setting approach (what): The 3Cs Conversations will increase clarity of what is expected from employees by establishing performance objectives (what) to align and guide work for the year and against which performance is assessed. Specifically, this will include three steps.

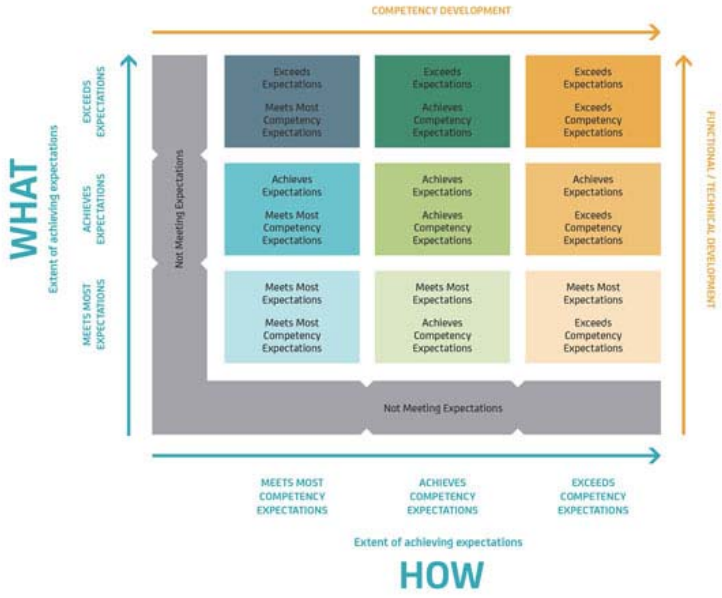
- Set organizational priorities. Division and/or section outcomes set annually by leadership.
- Align staff. Run Align & Connect Conversations to communicate division and/or section outcomes.
- Ensure individual accountability. Run Start-Up Agreement Conversations to finalize objectives that were drafted by employees; objectives will be specific, measurable, actionable, and realistic.

3. Boardwide competencies or expected behaviors (how): Introduce Boardwide expected behaviors/competencies. Everyone will have "how" behaviors/competencies incorporated into their work discussions.

- Divisions will be able to add specific critical competencies relative to their unique goals and objectives.
- Competencies will be graduated across three levels: Employee (Individual Contributor), Manager, and Officer.
- The six Boardwide competencies are:
    - Decision quality
    - Learning agility
    - Perspective and strategic agility
    - Relationships
    - Communication
    - Drive for excellence

4. Successful performance will be defined by both the "what" (objectives) and the "how" (competency demonstration).
The rating will be based on a both "what" the employee has accomplished and "how" the employee accomplished the work. See Diagram 1: Learning Review Matrix

Diagram 1: Learning Review Matrix



5. 3Cs process timeline

Additional Materials

- Focus Group infographic: 2013 Summary (PDF)